v3.0

ASUS Control Center

User Guide

E23345
September 2024

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 of 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

Contents

Contents

Contents

Chapter 3: Deployment

Contents

Chapter 4: Centralized

Contents

Chapter 5: Report

Contents

Chapter 6: Notification

Contents

Chapter 7: Account Management

Chapter 8: Options

Contents

Contents

Chapter 9: License

Appendix

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

Getting Started

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

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.

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		√	√
Monitor (Overview)	System Overview		Partial functions unavailable	√
	VM Overview		-	√
Monitor (one node)	Host Information		-	√
	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	-	√
	Subscription Report		-	√
Account	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:

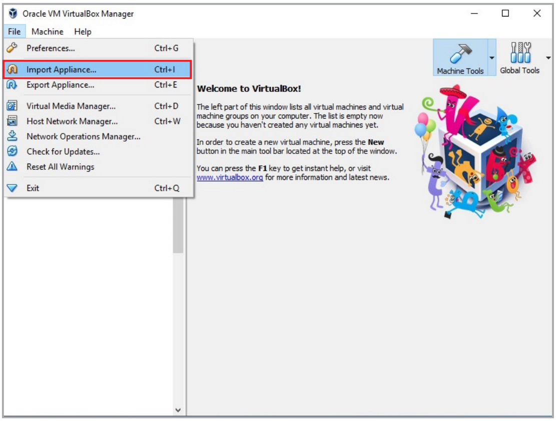
1.2.1 Installing the hypervisor and importing the OVA file

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.

- 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.


Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+W
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Machine Tools
Global Tools

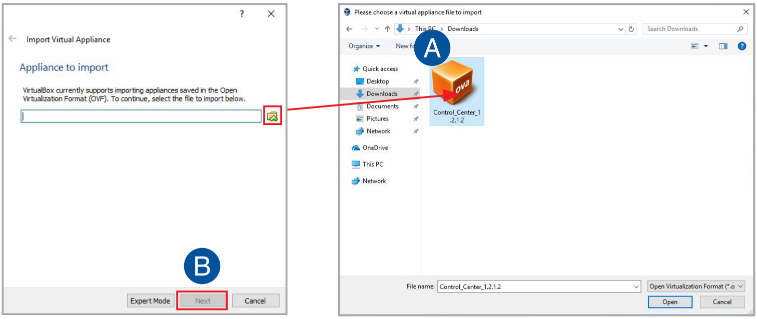
Welcome to VirtualBox!

The left part of this window lists all virtual machines and virtual machine groups on your computer. The list is empty now because you haven't created any virtual machines yet.

In order to create a new virtual machine, press the **New** button in the main tool bar located at the top of the window.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

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



Import Virtual Appliance

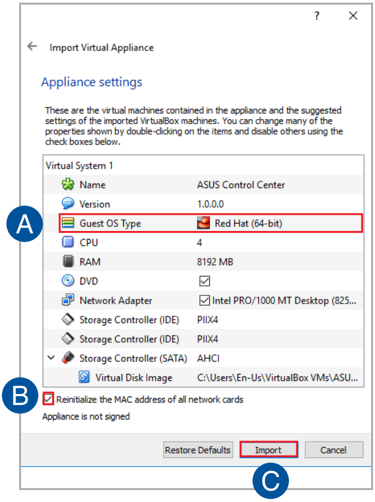
Appliance to import

VirtualBox currently supports importing appliances saved in the Open Virtualization Format (OVF). To continue, select the file to import below.

Please choose a virtual appliance file to import

File name: Control_Center_1.2.1.2

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).



Import Virtual Appliance

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Virtual System 1	
Name	ASUS Control Center
Version	1.0.0.0
Guest OS Type	Red Hat (64-bit)
CPU	4
RAM	8192 MB
DVD	☑
Network Adapter	☑ Intel PRO/1000 MT Desktop (825...
Storage Controller (IDE)	PIIX4
Storage Controller (IDE)	PIIX4
Storage Controller (SATA)	AHCI
Virtual Disk Image	C:\Users\En-Us\VirtualBox VMs\ASU...

☑ Reinitialize the MAC address of all network cards

Appliance is not signed

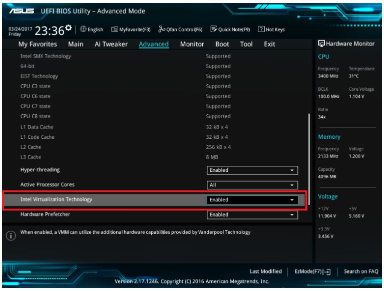
6. Wait for the OVA file to be imported. This may take a few minutes.
7. Select the VM on the list, then click **Start** on the toolbar to start the VM.

The minimum requirements for VM is as follows:

- 4 vCPU
- 8 GB RAM
- 100GB HDD

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

- VT-x: **BIOS** > **Advanced** > **Intel Virtualization Technology** > **Enabled**



Intel SMX Technology	Supported
64-bit	Supported
EIST Technology	Supported
CPU C3 state	Supported
CPU C6 state	Supported
CPU C7 state	Supported
CPU C8 state	Supported
L1 Data Cache	32 kB x 4
L1 Code Cache	32 kB x 4
L2 Cache	256 kB x 4
L3 Cache	8 MB
Hyper-threading	Enabled
Active Processor Cores	All
Intel Virtualization Technology	Enabled
Hardware Prefetcher	Enabled

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology

Hardware Monitor

CPU

Frequency	Temperature
3400 MHz	31°C
BCLK	Core Voltage
100.0 MHz	1.104 V
Ratio	
34x	

Memory

Frequency	Voltage
2133 MHz	1.200 V
Capacity	
4096 MB	

Voltage

+12V	+5V
11.904 V	5.160 V
+3.3V	
3.456 V	

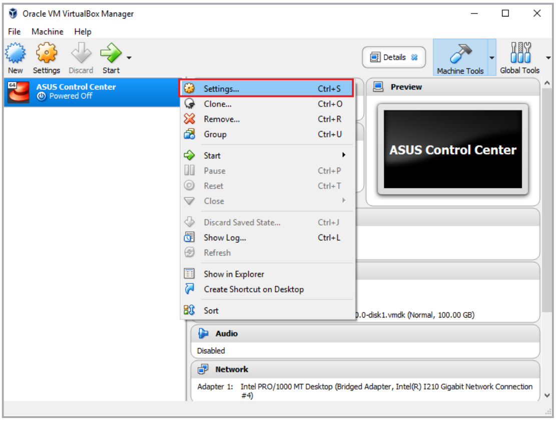
Version 2.17.1246. Copyright (C) 2016 American Megatrends, Inc.

- Network Card: 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:

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



0.0-disk1.vmdk (Normal, 100.00 GB)

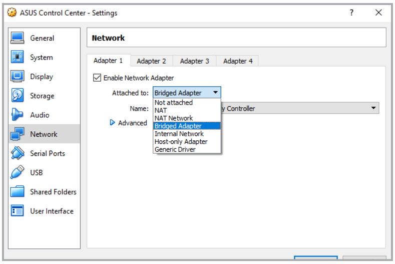
Audio

Disabled

Network

Adapter 1: Intel PRO/1000 MT Desktop (Bridged Adapter, Intel(R) I210 Gigabit Network Connection #4)

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



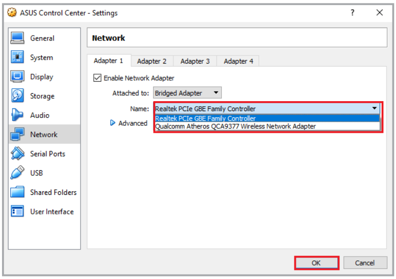
☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: y Controller

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

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**.



☑ Enable Network Adapter

Attached to: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

1.3 Initialize settings

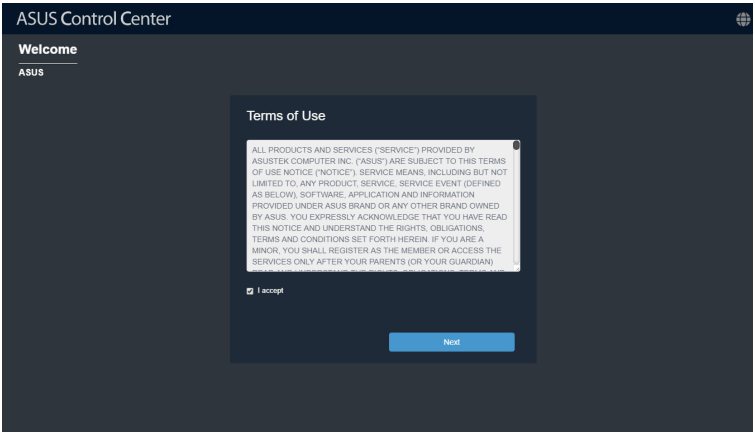
Once your ASUS Control Center is installed successfully, you will need to initialize the ASUS Control Center settings such as time zone, account and password, and network settings.

1.3.1 Initialize startup settings

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

The information entered in this section is for reference only.

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

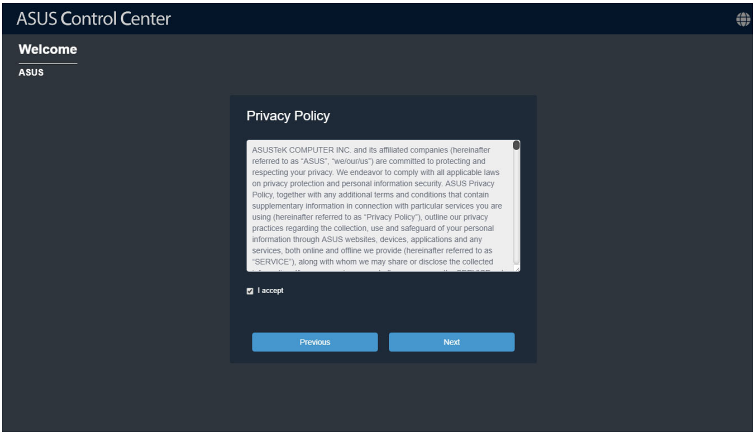


Terms of Use

ALL PRODUCTS AND SERVICES (“SERVICE”) PROVIDED BY ASUSTEK COMPUTER INC. (“ASUS”) ARE SUBJECT TO THIS TERMS OF USE NOTICE (“NOTICE”). SERVICE MEANS, INCLUDING BUT NOT LIMITED TO, ANY PRODUCT, SERVICE, SERVICE EVENT (DEFINED AS BELOW), SOFTWARE, APPLICATION AND INFORMATION PROVIDED UNDER ASUS BRAND OR ANY OTHER BRAND OWNED BY ASUS. YOU EXPRESSLY ACKNOWLEDGE THAT YOU HAVE READ THIS NOTICE AND UNDERSTAND THE RIGHTS, OBLIGATIONS, TERMS AND CONDITIONS SET FORTH HEREIN. IF YOU ARE A MINOR, YOU SHALL REGISTER AS THE MEMBER OR ACCESS THE SERVICES ONLY AFTER YOUR PARENTS (OR YOUR GUARDIAN)

☑ I accept

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



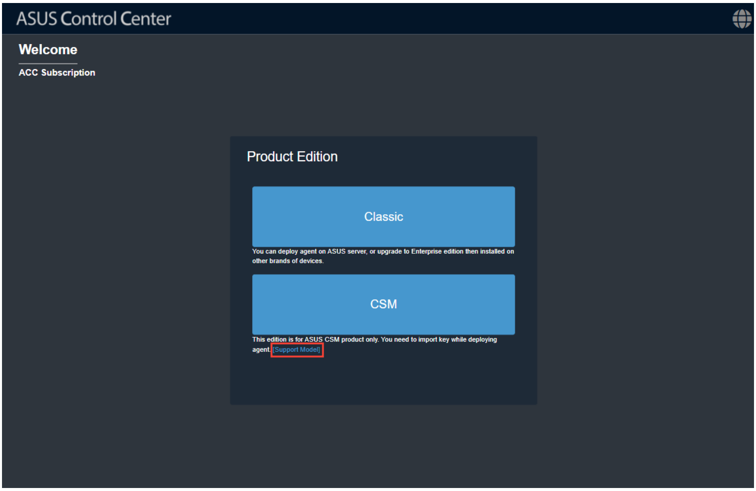
Privacy Policy

ASUSTeK COMPUTER INC. and its affiliated companies (hereinafter referred to as "ASUS", "we/our/us") are committed to protecting and respecting your privacy. We endeavor to comply with all applicable laws on privacy protection and personal information security. ASUS Privacy Policy, together with any additional terms and conditions that contain supplementary information in connection with particular services you are using (hereinafter referred to as "Privacy Policy"), outline our privacy practices regarding the collection, use and safeguard of your personal information through ASUS websites, devices, applications and any services, both online and offline we provide (hereinafter referred to as "SERVICE"), along with whom we may share or disclose the collected

☑ I accept

3. Select the edition of your ASUS Control Center.

A full list of CSM supported models will be displayed when you select the **Support Model** hyperlink under the **CSM** button. Ensure to check whether your system supports CSM edition if you select **CSM**.



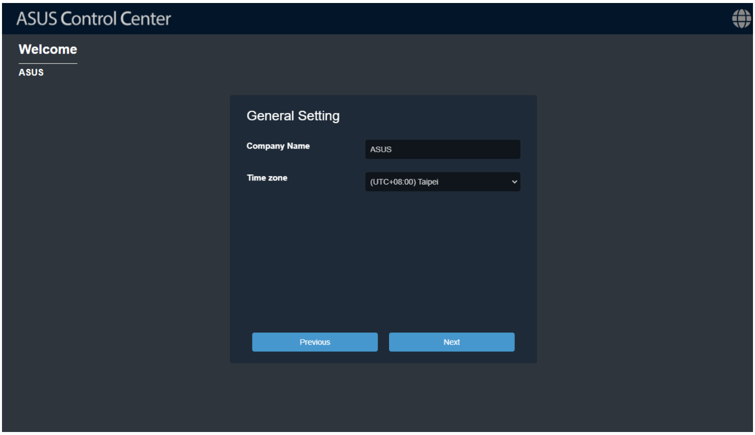
Product Edition

You can deploy agent on ASUS server, or upgrade to Enterprise edition then installed on other brands of devices.

This edition is for ASUS CSM product only. You need to import key while deploying agent.[Support Model]

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

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.



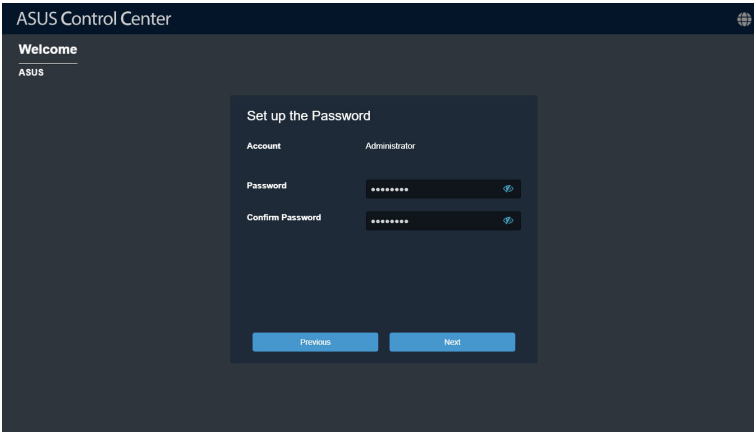
General Setting

Company Name: ASUS

Time zone: (UTC+08:00) Taipei

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

- 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.



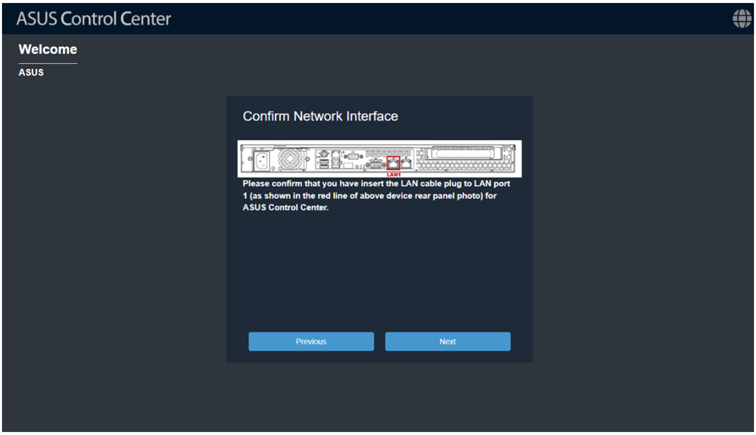
Set up the Password

Account: Administrator

Password: ••••••••

Confirm Password: ••••••••

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

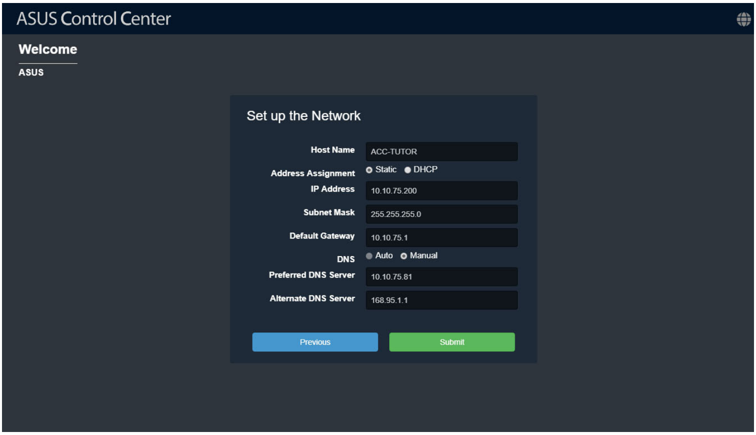


Confirm Network Interface

Please confirm that you have insert the LAN cable plug to LAN port 1 (as shown in the red line of above device rear panel photo) for ASUS Control Center.

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

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.

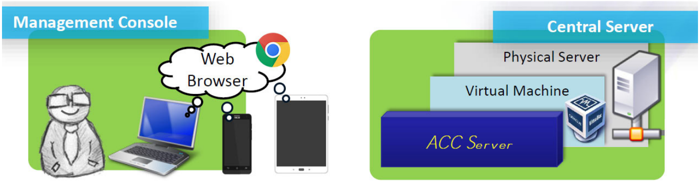


Set up the Network

Host Name: ACC-TUTOR
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

1.3.2 Logging into ASUS Control Center

The Host Name: **ACC-TUTOR**, and IP Address: **10.10.75.200** used in this section are for reference only.



To log into ASUS Control Center:

1. Open a web browser and key in the main server URL (include the Host Name or IP) to enter ASUS Control Center web console. Please refer to the table below for the main server URL format and examples:

Transfer Protocol	URL Template	Example 1 (Host Name)	Example 2 (IP)
HTTP	http://HostName(IP)/ACC	http://ACC-TUTOR/ACC	http://10.10.75.200/ACC
HTTPS (secure)	https://HostName(IP)/ACC	https://ACC-TUTOR/ACC	https://10.10.75.200/ACC

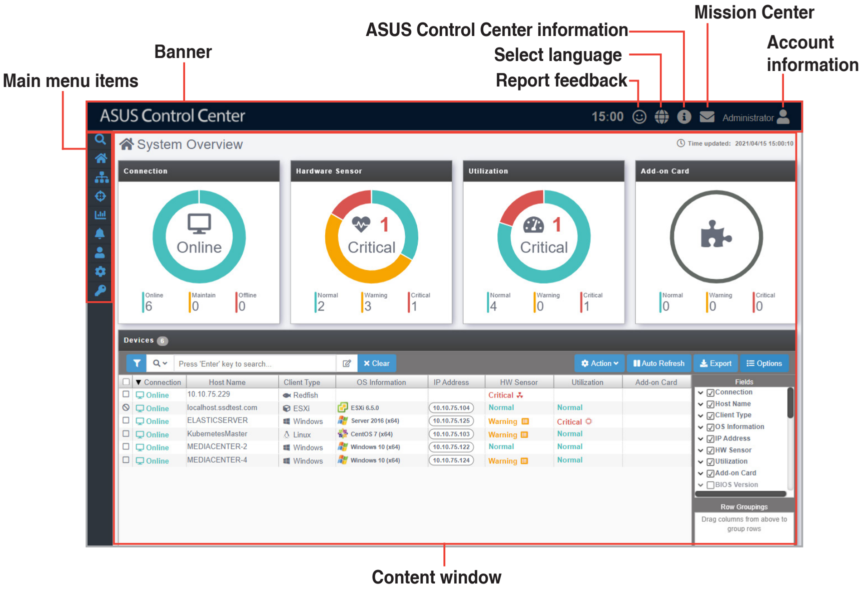
- The *ACC* in the URL is case sensitive, ensure to use all caps when entering *ACC* to the URL.
- The export files and import files functions are disabled when using the ACC through VM. For optimal experience, we recommend using an Internet browser installed on the host system to enter the main server URL when using the functions mentioned in this guide.

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

Refer to the **Account Management** chapter for more information on MFA.

1.4 ASUS Control Center layout

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



☐	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
☐	Online	10.10.75.229	Redfish			Critical		
⃠	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
☐	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
☐	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
☐	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
☐	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

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.

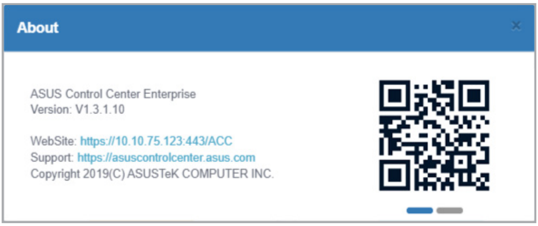
Multiple Language

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 ℹ 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.

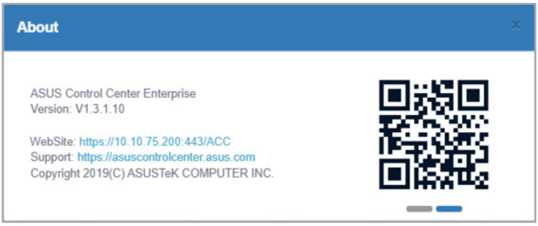
For more information on setting the network configurations for all network cards, please refer to the **Network Configuration** section.



About

ASUS Control Center Enterprise
Version: V1.3.1.10

WebSite: https://10.10.75.123:443/ACC
Support: https://asuscontrolcenter.asus.com
Copyright 2019(C) ASUSTeK COMPUTER INC.



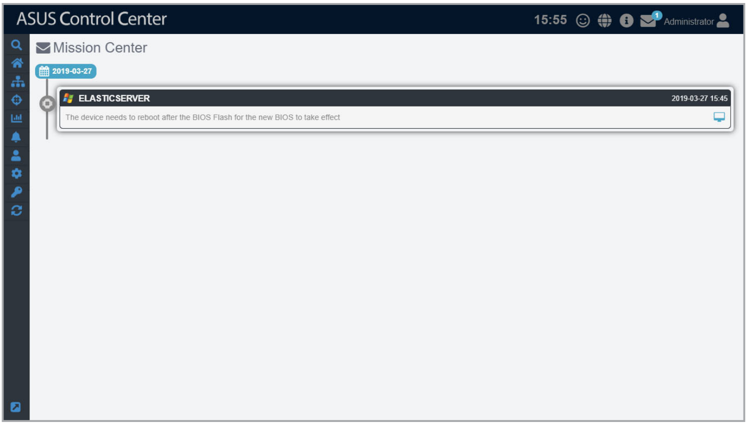
About

ASUS Control Center Enterprise
Version: V1.3.1.10

WebSite: https://10.10.75.200:443/ACC
Support: https://asuscontrolcenter.asus.com
Copyright 2019(C) ASUSTeK COMPUTER INC.

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.



ELASTICSERVER 2019-03-27 15:45

The device needs to reboot after the BIOS Flash for the new BIOS to take effect

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.

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

1.4.2 Menu

The menu bar on the left of the screen has the following menu items:

Main Menu	Submenu	Description
Monitor	**System Overview**	Displays activity alerts and event logs to monitor server components in real time. You can also access the various functions, such as BMC settings, BIOS settings and more of a single device from the System Overview.
	VM Overview	Displays the status and information of the hosts, and all VMs on the host device. You can also perform some functions on the vSpheres such as power controls.
Deployment	**Agent Management**	To remotely deploy Windows or Linux agents, or install these agents manually for effective monitoring. You can also remove agents from Windows and Linux OS managed devices.
	Agentless Management	Add agentless vSphere to be monitored automatically periodically, or remove the vSphere from managed devices.
Centralized	**Metadata Management**	Customize device metadata such as device location.
	BIOS Flash Management	Centralized management of BIOS, and BIOS flashing of multiple devices simultaneously.
	Security Management	Manage security settings for multiple devices at the same time
	Software Dispatch	Dispatch software packages to be installed on devices, or add software packages to the **Software Pool** for easy access later.
	Task Scheduler	Schedule specified tasks such as software dispatching, power on or off, security control, and service control for selected devices to be executed at set times
	Power Control	Control the power options of all managed devices (except for vSphere).
Report	**Software Report**	View and manage all software installed on managed devices. You can also view hotfix, license, and service reports for these software and receive notifications regarding new software installations.
	Hardware Report	View and manage all hardware installed on managed devices. You can also view a hardware item and all the devices which have this hardware item installed.
	Task Report	View the reports for the task status and progress for **Software Dispatch**, **BIOS Dispatch**, **Agent Update**, and **Agent Deploy**.
Notification	**Conditional Trigger**	Set notification methods when there are software changes such as an installation of a software not on the trust list, or when there are hardware anomalies that do not adhere to company policies.
	Subscription	Set periodic reports on the hardware or software of managed devices.

(continued on the next page)

Main Menu	Submenu	Description
Account	Role Privilege Management	Create and edit permissions for roles, which you may assign to accounts.
	Accounts Management	Add or manage accounts, and also assign roles to these accounts which determine what permissions these accounts have.
Options	General Configuration	Set the Time zone, and refreshment interval of main server and agent.
	Network Configuration	Set network configurations for ASUS Control Center, and also the settings for the network cards (if there are multiple).
	Appearance Configuration	Customize the banner logo for ASUS Control Center.
	Security Configuration	Set a password for agent removal from Windows system managed devices.
	SMTP Settings	Configure SMTP Server settings to send notifications for server alert events
	Backup & Restore	Backup or restore ASUS Control Center settings for ACC Physical Appliances.
	Maintenance	Displays information on the VM with ASUS Control Center, and also allows you to control the power options for this device, as well as the services running on VM.
	DBExpose Configuration	Set an account and password which will allow third-party database, such as MySQL to access the data in ASUS Control Center.
	Update	Update the Agents for Windows and/or Linux managed devices, or update the ASUS Control Center main server when a new update is available.
	Sensor Threshold	Centralized management of sensor threshold values for all managed devices.
	Software List	View and manage rules of the installed software of all managed devices.
License		Import a license key for ASUS Control Center Enterprise edition.

Chapter 2

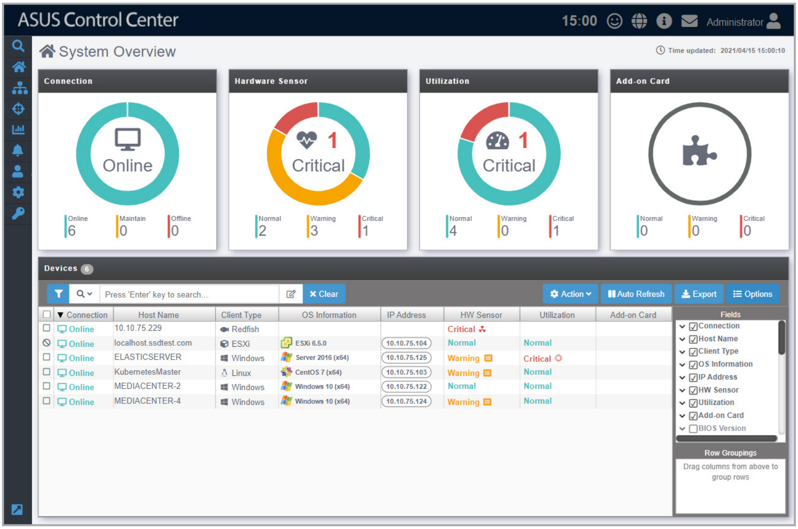
This chapter describes the various monitoring tools and options available.

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.

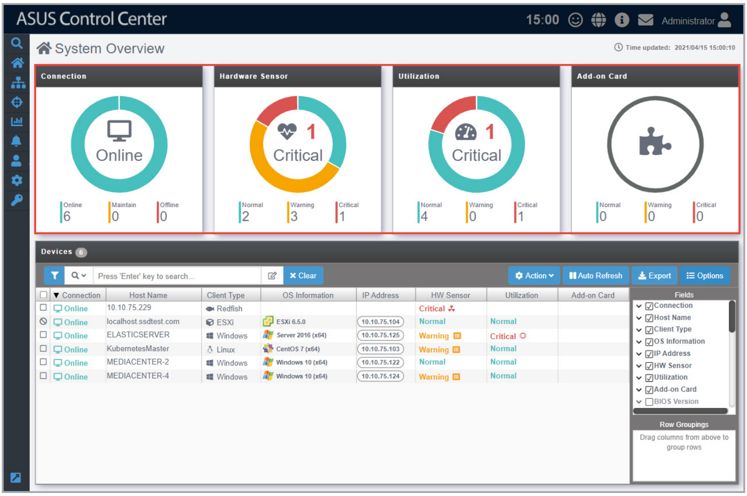
To access the **System Overview**, click 🏠 > **System Overview** from the left menu.



□	Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
□	Online	10.10.75.229	Redfish			Critical		
⊘	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
□	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
□	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
□	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
□	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

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.

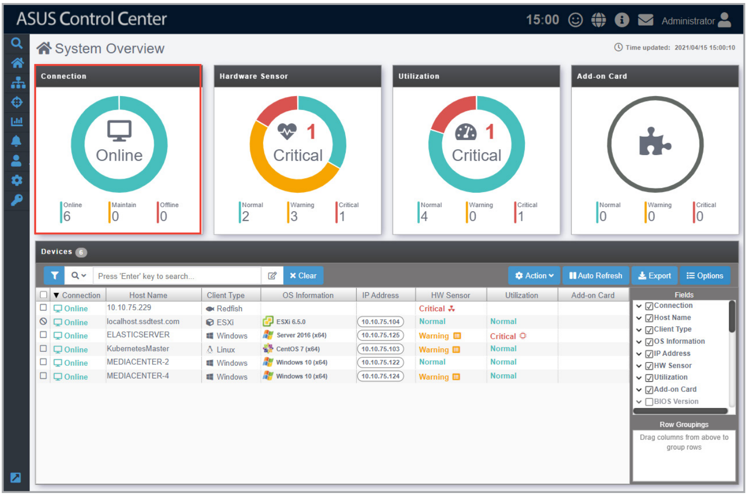


Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
Online	10.10.75.229	Redfish			Critical		
Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

☑ Connection
☑ Host Name
☑ Client Type
☑ OS Information
☑ IP Address
☑ HW Sensor
☑ Utilization
☑ Add-on Card
□ BIOS Version

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.



▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
Online	10.10.75.229	Redfish			Critical		
Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

Fields
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Add-on Card
- □ BIOS Version

Row Groupings

Drag columns from above to group rows

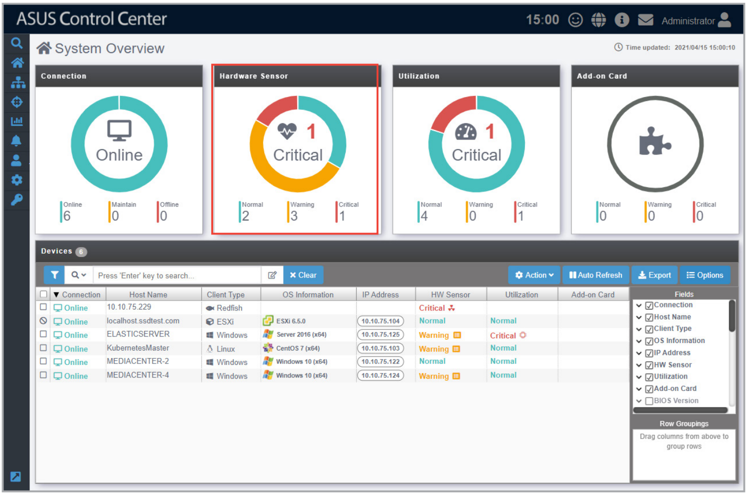
Please refer to the table below for the color status of the Connection overview circle

	Green	Orange	Red
Connection Status	Online	Maintain*	Offline

* This status represents the status for when 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.



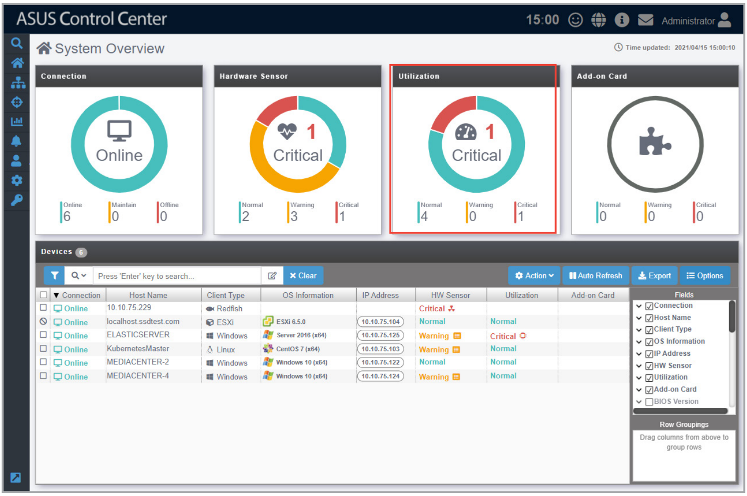
Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
Online	10.10.75.229	Redfish			Critical		
Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

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.



☐	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
☐	Online	10.10.75.229	Redfish			Critical		
⃠	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
☐	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
☐	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
☐	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
☐	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

Fields
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Add-on Card
- ☐ BIOS Version

Row Groupings

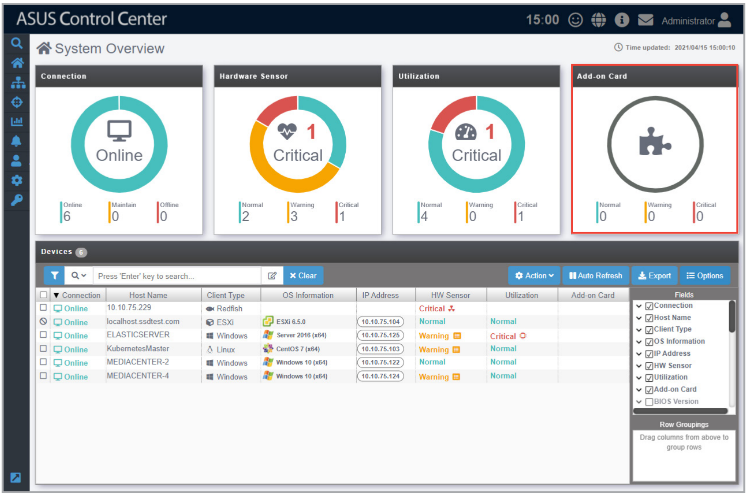
Drag columns from above to group rows

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.



□	Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
□	Online	10.10.75.229	Redfish			Critical		
⃠	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
□	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
□	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
□	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
□	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

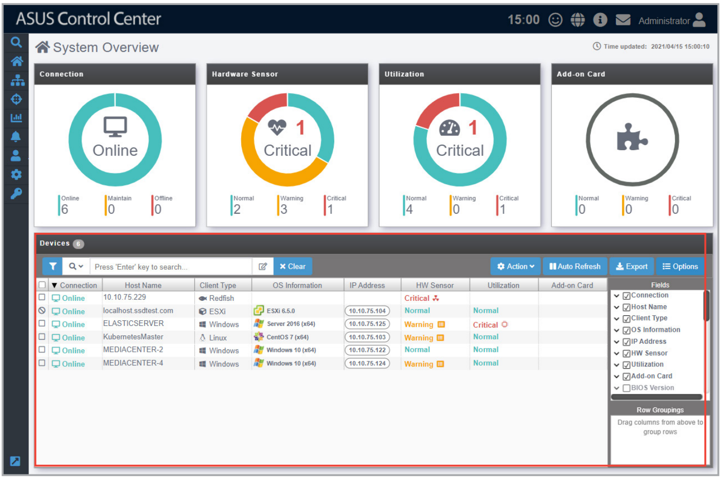
Please refer to the table below for the color status of the Add-on Card overview circle

	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.

- 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.

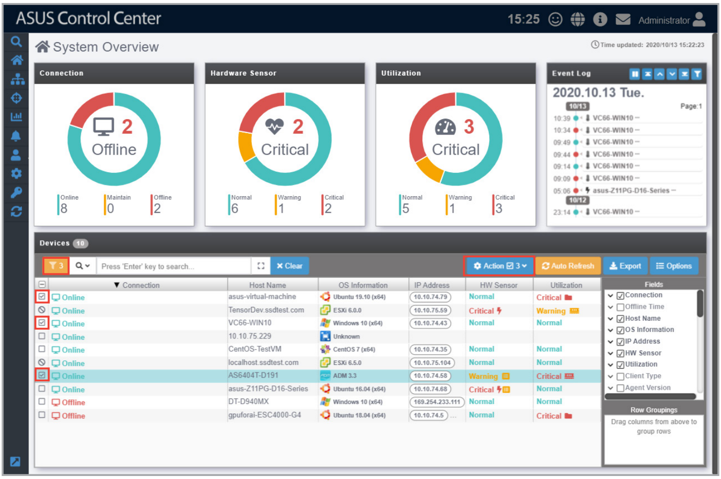


□	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
□	Online	10.10.75.229	Redfish			Critical		
⊘	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
□	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
□	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
□	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
□	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

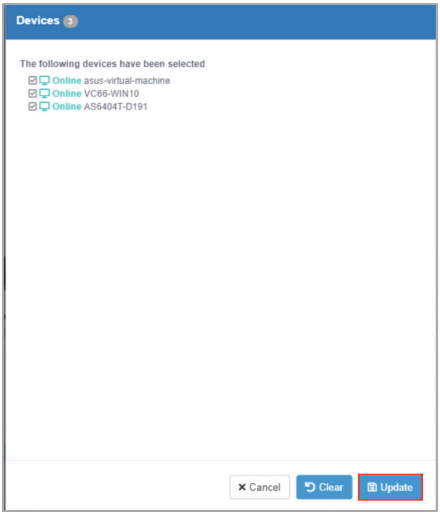
Setting power control (Action)

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**.



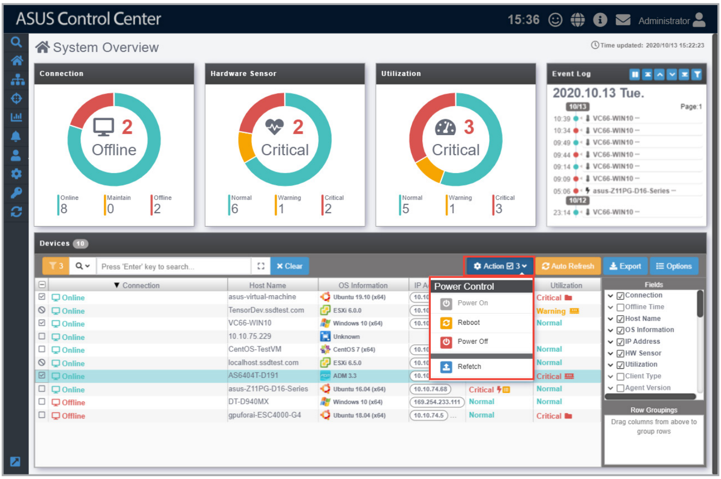
	Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
☑	Online	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10.74.79	Normal	Critical
⃠	Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59	Critical	Warning
☑	Online	VC66-WIN10	Windows 10 (x64)	10.10.74.43	Normal	Normal
□	Online	10.10.75.229	Unknown			
□	Online	CentOS-TestVM	CentOS 7 (x64)	10.10.74.35	Normal	Normal
⃠	Online	localhost.ssdtest.com	ESXi 6.5.0	10.10.75.104	Normal	Normal
☑	Online	AS6404T-D191	ADM 3.3	10.10.74.58	Warning	Critical
□	Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal
□	Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111	Normal	Normal
□	Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 ...	Normal	Critical



The following devices have been selected

- ☑ Online asus-virtual-machine
- ☑ Online VC66-WIN10
- ☑ Online AS6404T-D191

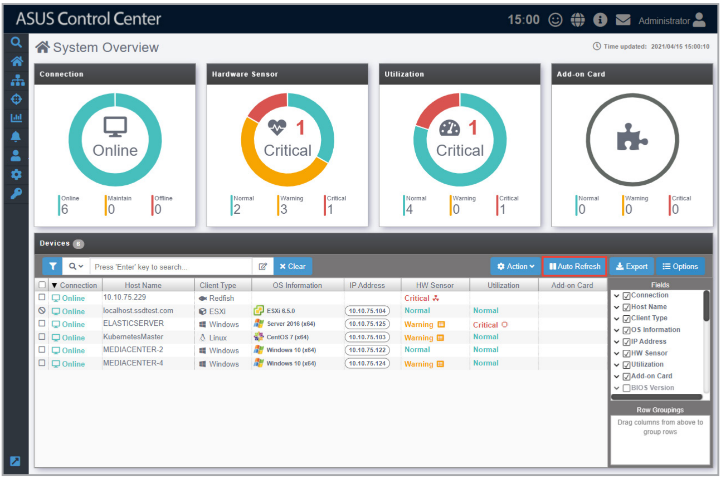
3. Click on **Action**, then select the power control option you would like to apply to the selected devices.



□	▼ Connection	Host Name	OS Information	IP A		Utilization
☑	Online	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10		Critical
⊘	Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10		Warning
☑	Online	VC66-WIN10	Windows 10 (x64)	10.10		Normal
□	Online	10.10.75.229	Unknown			
□	Online	CentOS-TestVM	CentOS 7 (x64)	10.10		Normal
⊘	Online	localhost.ssdtest.com	ESXi 6.5.0	10.10		Normal
☑	Online	AS6404T-D191	ADM 3.3	10.10		Critical
□	Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal
□	Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111	Normal	Normal
□	Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 ...	Normal	Critical

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 (Auto Refresh) or disable (Auto Refresh) it.



□	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
□	Online	10.10.75.229	Redfish			Critical		
⊘	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
□	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
□	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
□	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
□	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

Fields

- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Add-on Card
- □ BIOS Version

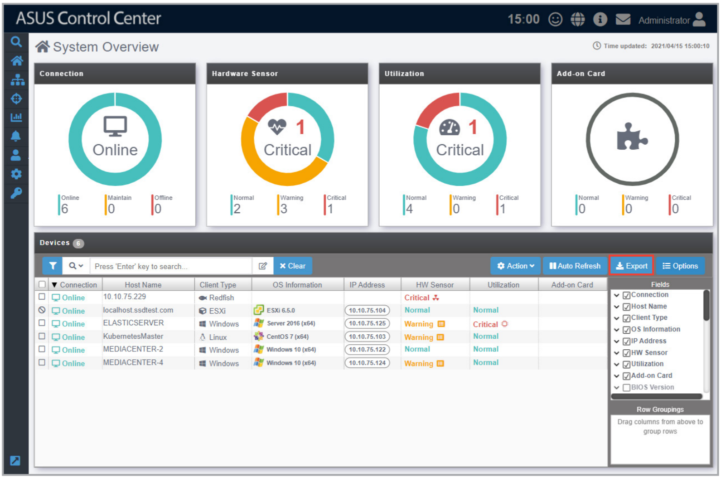
Row Groupings

Drag columns from above to group rows

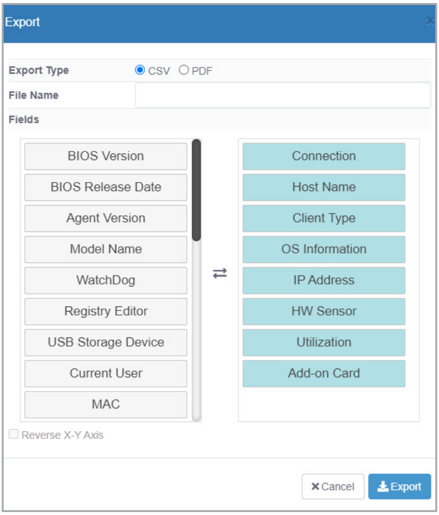
Exporting devices list (Export)

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 exclude it or to the right column to include it.
3. Click **Export** in the popup window to export the device list based on the selected settings.



☐	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
☐	Online	10.10.75.229	Redfish			Critical		
⃠	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
☐	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
☐	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
☐	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
☐	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	


Export

Export Type ● CSV ○ PDF

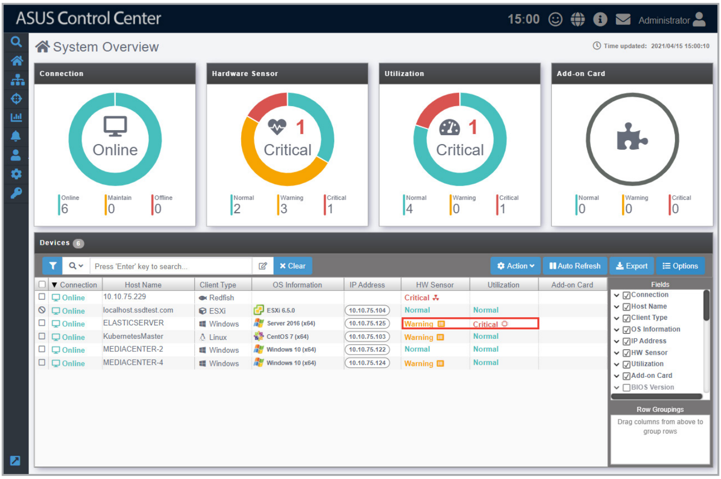
File Name

Fields

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.

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**.



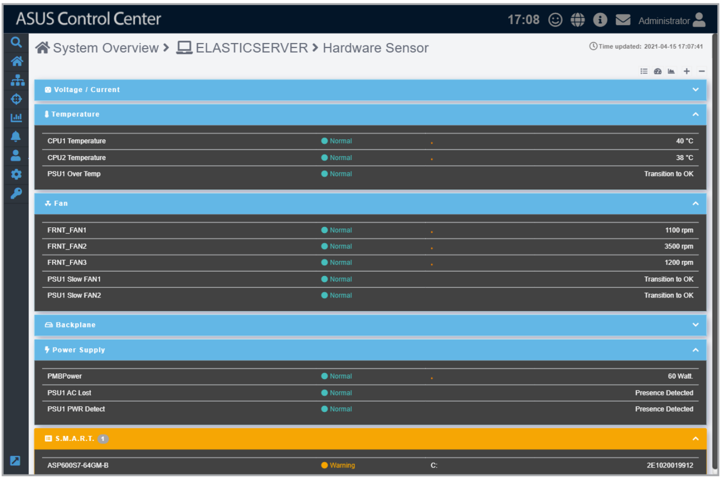
□	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
□	Online	10.10.75.229	Redfish			Critical		
⃠	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
□	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Critical	
□	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
□	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
□	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

Fields
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Add-on Card
- □ BIOS Version

Row Groupings

Drag columns from above to group rows

Link to managed device's Hardware Sensor:


ASUS Control Center
17:08
Administrator
System Overview › ELASTICSERVER › Hardware Sensor
Time updated: 2021-04-15 17:07:41

Voltage / Current

Temperature

CPU1 Temperature	● Normal	40 °C
CPU2 Temperature	● Normal	38 °C
PSU1 Over Temp	● Normal	Transition to OK

Fan

FRNT_FAN1	● Normal	1100 rpm
FRNT_FAN2	● Normal	3500 rpm
FRNT_FAN3	● Normal	1200 rpm
PSU1 Slow FAN1	● Normal	Transition to OK
PSU1 Slow FAN2	● Normal	Transition to OK

Backplane

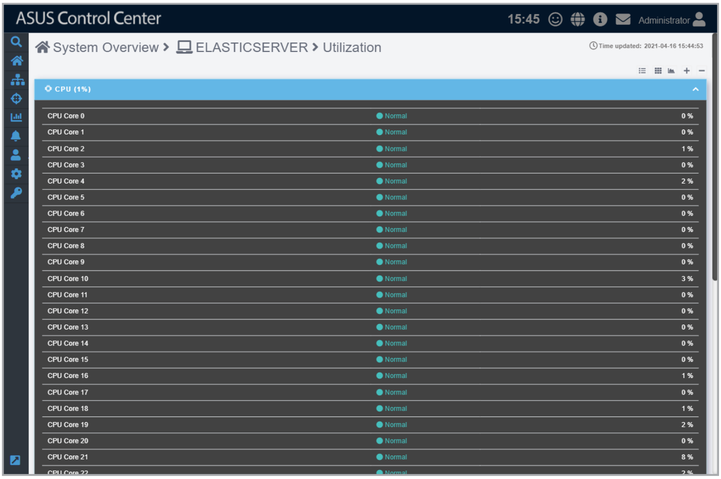
Power Supply

PMBPower	● Normal	60 Watt.
PSU1 AC Lost	● Normal	Presence Detected
PSU1 PWR Detect	● Normal	Presence Detected

S.M.A.R.T. 1

ASP600S7-64GM-B	● Warning	C:	2E1020019912

Link to managed device's Utilization:



System Overview > ELASTICSERVER > Utilization

Time updated: 2021-04-16 15:44:53

CPU (1%)

CPU Core 0	● Normal	0 %
CPU Core 1	● Normal	0 %
CPU Core 2	● Normal	1 %
CPU Core 3	● Normal	0 %
CPU Core 4	● Normal	2 %
CPU Core 5	● Normal	0 %
CPU Core 6	● Normal	0 %
CPU Core 7	● Normal	0 %
CPU Core 8	● Normal	0 %
CPU Core 9	● Normal	0 %
CPU Core 10	● Normal	3 %
CPU Core 11	● Normal	0 %
CPU Core 12	● Normal	0 %
CPU Core 13	● Normal	0 %
CPU Core 14	● Normal	0 %
CPU Core 15	● Normal	0 %
CPU Core 16	● Normal	1 %
CPU Core 17	● Normal	0 %
CPU Core 18	● Normal	1 %
CPU Core 19	● Normal	2 %
CPU Core 20	● Normal	0 %
CPU Core 21	● Normal	8 %
CPU Core 22	● Normal	2 %

2.1.3 Options

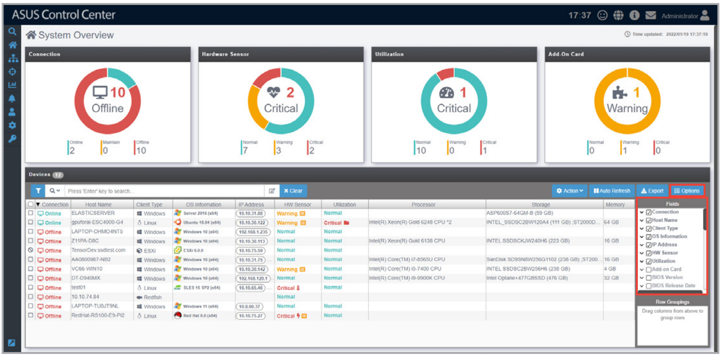
Clicking on **Options** will display the **Fields** and **Row Groupings** functions. The **Fields** function controls which metadata columns are displayed in the **Devices** list. You can check the metadata items you wish to hide or display in the **Fields** list.

> 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

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



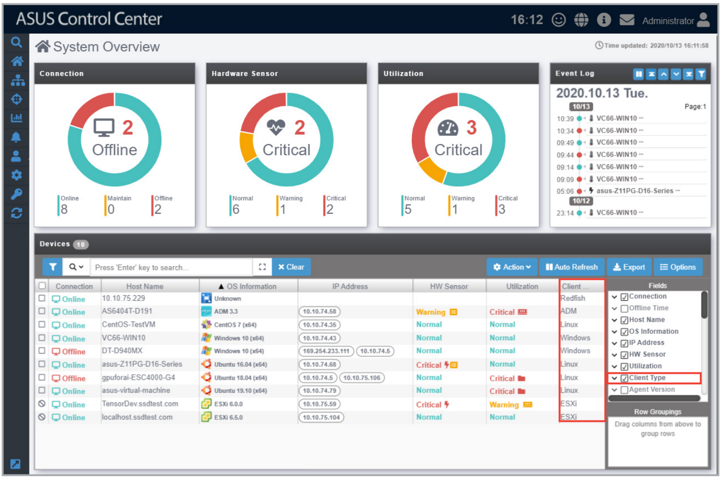
☐	Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Processor	Storage	Memory
☐	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.88	Warning	Normal		ASP600S7-64GM-B (59 GB)	
☐	Online	gpuforai-ESC4000-G4	Linux	Ubuntu 18.04 (x64)	10.10.30.122	Warning	Critical	Intel(R) Xeon(R) Gold 6248 CPU *2	INTEL_SSDSC2BW120A4 (111 GB) ;ST2000D...	64 GB
☐	Offline	LAPTOP-OHMO4NT5	Windows	Windows 10 (x64)	192.168.1.235	Normal	Normal			
☐	Offline	Z11PA-D8C	Windows	Windows 10 (x64)	10.10.30.113	Normal	Normal	Intel(R) Xeon(R) Gold 6138 CPU	INTEL SSDSCKJW240H6 (223 GB)	16 GB
⊘	Offline	TensorDev.ssdtest.com	ESXi	ESXi 6.0.0	10.10.75.59	Normal	Normal			
☐	Offline	AA0800987-NB2	Windows	Windows 10 (x64)	10.10.31.75 ...	Normal	Normal	Intel(R) Core(TM) i7-8565U CPU	SanDisk SD9SN8W256G1102 (238 GB) ;ST200...	16 GB
☐	Offline	VC66-WIN10	Windows	Windows 10 (x64)	10.10.30.142	Warning	Normal	Intel(R) Core(TM) i5-7400 CPU	INTEL SSDSC2BW256H6 (238 GB)	4 GB
☐	Offline	DT-D940MX	Windows	Windows 10 (x64)	192.168.120.1 ...	Normal	Normal	Intel(R) Core(TM) i9-9900K CPU	Intel Optane+477GBSSD (476 GB)	32 GB
☐	Offline	test01	Linux	SLES 15 SP2 (x64)	10.10.65.46 ...	Critical	Normal			
☐	Offline	10.10.74.84	Redfish			Normal				
☐	Offline	LAPTOP-TU0JT9NL	Windows	Windows 11 (x64)	10.8.60.37	Normal	Normal			
☐	Offline	RedHat-RS100-E9-PI2	Linux	Red Hat 8.0 (x64)	10.10.75.27	Critical	Normal			

Fields
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☐ Add-on Card
- ☐ BIOS Version
- ☐ BIOS Release Date

Row Groupings

Drag columns from above to group rows

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.



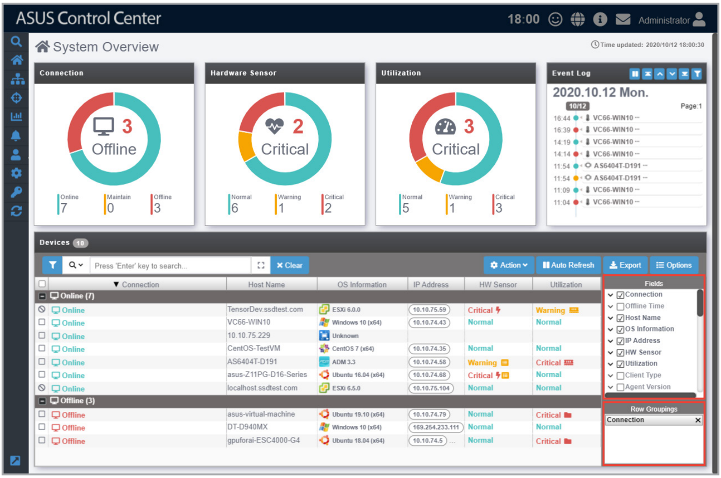
2020.10.13 Tue.
10/13 Page:1
10:39 VC66-WIN10 ···
10:34 VC66-WIN10 ···
09:49 VC66-WIN10 ···
09:44 VC66-WIN10 ···
09:14 VC66-WIN10 ···
09:09 VC66-WIN10 ···
05:06 asus-Z11PG-D16-Series ···
10/12
23:14 VC66-WIN10 ···

□	Connection	Host Name	▲ OS Information	IP Address	HW Sensor	Utilization	Client ...
□	Online	10.10.75.229	Unknown				Redfish
□	Online	AS6404T-D191	ADM 3.3	10.10.74.58	Warning	Critical	ADM
□	Online	CentOS-TestVM	CentOS 7 (x64)	10.10.74.35	Normal	Normal	Linux
□	Online	VC66-WIN10	Windows 10 (x64)	10.10.74.43	Normal	Normal	Windows
□	Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111 10.10.74.5	Normal	Normal	Windows
□	Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal	Linux
□	Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 10.10.75.106	Normal	Critical	Linux
□	Online	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10.74.79	Normal	Critical	Linux
⦸	Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59	Critical	Warning	ESXi
⦸	Online	localhost.ssdtest.com	ESXi 6.5.0	10.10.75.104	Normal	Normal	ESXi

Fields
- ☑ Connection
- □ Offline Time
- ☑ Host Name
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Client Type
- □ Agent Version

Using the Row Groupings function

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



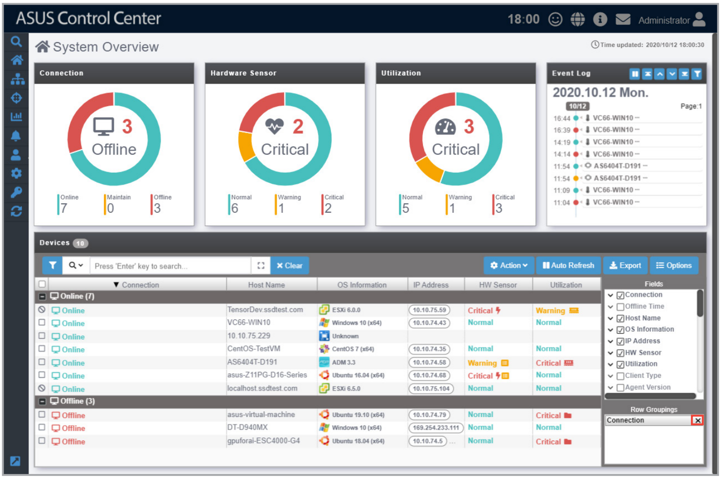
16:44 VC66-WIN10 ···
16:39 VC66-WIN10 ···
14:19 VC66-WIN10 ···
14:14 VC66-WIN10 ···
11:54 AS6404T-D191 ···
11:54 AS6404T-D191 ···
11:09 VC66-WIN10 ···
11:04 VC66-WIN10 ···

▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
⊟ Online (7)					
Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59	Critical	Warning
Online	VC66-WIN10	Windows 10 (x64)	10.10.74.43	Normal	Normal
Online	10.10.75.229	Unknown			
Online	CentOS-TestVM	CentOS 7 (x64)	10.10.74.35	Normal	Normal
Online	AS6404T-D191	ADM 3.3	10.10.74.58	Warning	Critical
Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal
Online	localhost.ssdtest.com	ESXi 6.5.0	10.10.75.104	Normal	Normal
⊟ Offline (3)					
Offline	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10.74.79	Normal	Critical
Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111	Normal	Normal
Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 ...	Normal	Critical

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

Row Groupings
Connection ✕

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


ASUS Control Center
18:00
Administrator
System Overview
Time updated: 2020/10/12 18:00:30

16:44 VC66-WIN10 ···
16:39 VC66-WIN10 ···
14:19 VC66-WIN10 ···
14:14 VC66-WIN10 ···
11:54 AS6404T-D191 ···
11:54 AS6404T-D191 ···
11:09 VC66-WIN10 ···
11:04 VC66-WIN10 ···

▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
⊟ Online (7)					
Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59	Critical	Warning
Online	VC66-WIN10	Windows 10 (x64)	10.10.74.43	Normal	Normal
Online	10.10.75.229	Unknown			
Online	CentOS-TestVM	CentOS 7 (x64)	10.10.74.35	Normal	Normal
Online	AS6404T-D191	ADM 3.3	10.10.74.58	Warning	Critical
Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal
Online	localhost.ssdtest.com	ESXi 6.5.0	10.10.75.104	Normal	Normal
⊟ Offline (3)					
Offline	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10.74.79	Normal	Critical
Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111	Normal	Normal
Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5	Normal	Critical

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

Row Groupings
Connection ✕

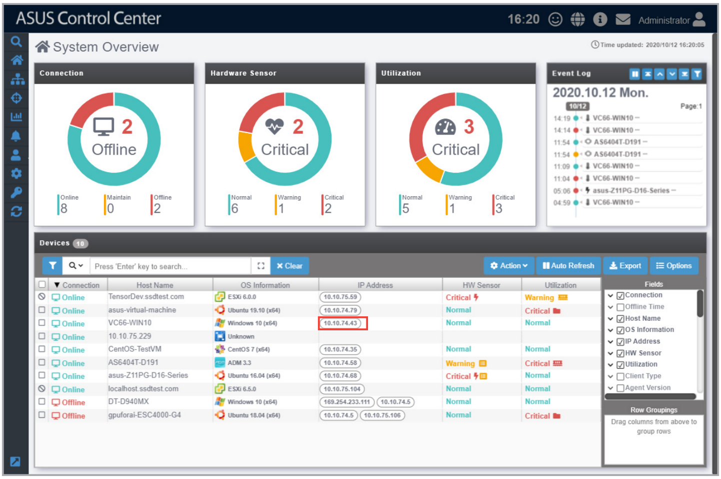
Accessing remote desktop

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.



```
2020.10.12 Mon.
10/12                         Page:1
14:19  VC66-WIN10 ···
14:14  VC66-WIN10 ···
11:54  AS6404T-D191 ···
11:54  AS6404T-D191 ···
11:09  VC66-WIN10 ···
11:04  VC66-WIN10 ···
05:06  asus-Z11PG-D16-Series ···
04:59  VC66-WIN10 ···
```

□	Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
⊘	Online	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59	Critical	Warning
□	Online	asus-virtual-machine	Ubuntu 19.10 (x64)	10.10.74.79	Normal	Critical
□	Online	VC66-WIN10	Windows 10 (x64)	10.10.74.43	Normal	Normal
□	Online	10.10.75.229	Unknown			
□	Online	CentOS-TestVM	CentOS 7 (x64)	10.10.74.35	Normal	Normal
□	Online	AS6404T-D191	ADM 3.3	10.10.74.58	Warning	Critical
□	Online	asus-Z11PG-D16-Series	Ubuntu 16.04 (x64)	10.10.74.68	Critical	Normal
⊘	Online	localhost.ssdtest.com	ESXi 6.5.0	10.10.75.104	Normal	Normal
□	Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111 10.10.74.5	Normal	Normal
□	Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 10.10.75.106	Normal	Critical

Fields
- ☑ Connection
- □ Offline Time
- ☑ Host Name
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- □ Client Type
- □ Agent Version

Row Groupings

Drag columns from above to group rows

3. Select a resolution to display the managed device in the Remote Desktop window.

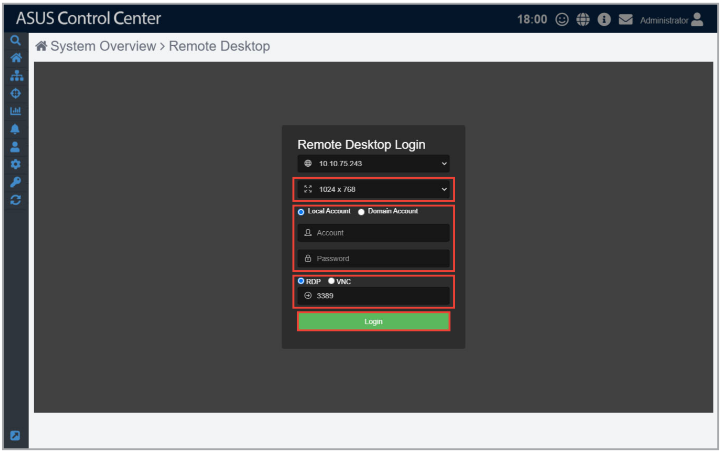
4. Select the login Account type, then enter the **Account**, **Password**, and **Domain** information.

- **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**.

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.



Remote Desktop Login

10.10.75.243

1024 x 768

● Local Account ○ Domain Account

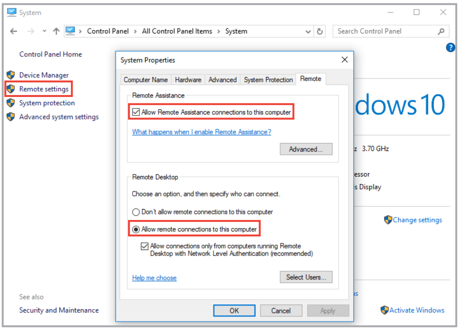
Account

Password

● RDP ○ VNC

3389

- 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**.



Remote Assistance

☑ Allow Remote Assistance connections to this computer

Remote Desktop

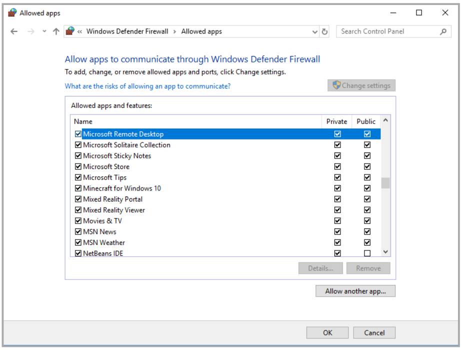
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

- (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**.


Allowed apps
« Windows Defender Firewall › Allowed apps
Search Control Panel
What are the risks of allowing an app to communicate?
Change settings
Details...
Remove
Allow another app...
OK
Cancel

Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

Allowed apps and features:

Name	Private	Public
☑ Microsoft Remote Desktop	☑	☑
☑ Microsoft Solitaire Collection	☑	☑
☑ Microsoft Sticky Notes	☑	☑
☑ Microsoft Store	☑	☑
☑ Microsoft Tips	☑	☑
☑ Minecraft for Windows 10	☑	☑
☑ Mixed Reality Portal	☑	☑
☑ Mixed Reality Viewer	☑	☑
☑ Movies & TV	☑	☑
☑ MSN News	☑	☑
☑ MSN Weather	☑	☑
☑ NetBeans IDE	☑	□

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.

> 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

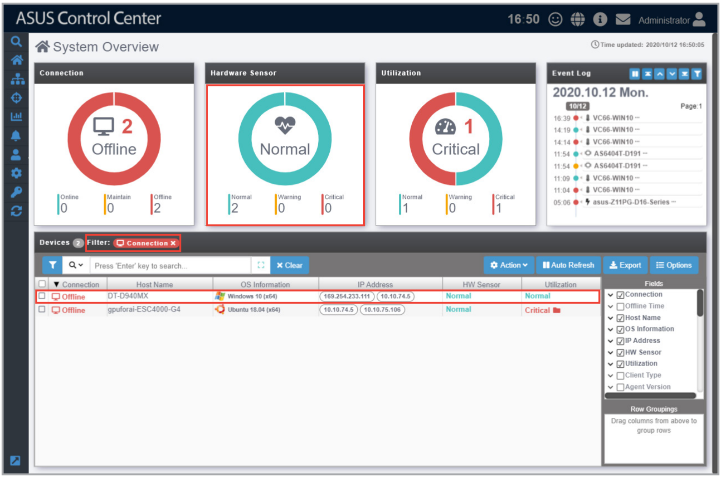
There are various methods of searching and filtering managed devices on the System Overview screen, giving you the freedom of searching or filtering managed devices according to your needs.

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

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

1. 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.
2. 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.



2020.10.12 Mon.

10/12 Page:1

16:39 VC66-WIN10 ···
14:19 VC66-WIN10 ···
14:14 VC66-WIN10 ···
11:54 AS6404T-D191 ···
11:54 AS6404T-D191 ···
11:09 VC66-WIN10 ···
11:04 VC66-WIN10 ···
05:06 asus-Z11PG-D16-Series ···

□	▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
□	Offline	DT-D940MX	Windows 10 (x64)	169.254.233.111 10.10.74.5	Normal	Normal
□	Offline	gpuforai-ESC4000-G4	Ubuntu 18.04 (x64)	10.10.74.5 10.10.75.106	Normal	Critical

Fields

☑ Connection
□ Offline Time
☑ Host Name
☑ OS Information
☑ IP Address
☑ HW Sensor
☑ Utilization
□ Client Type
□ Agent Version

Row Groupings

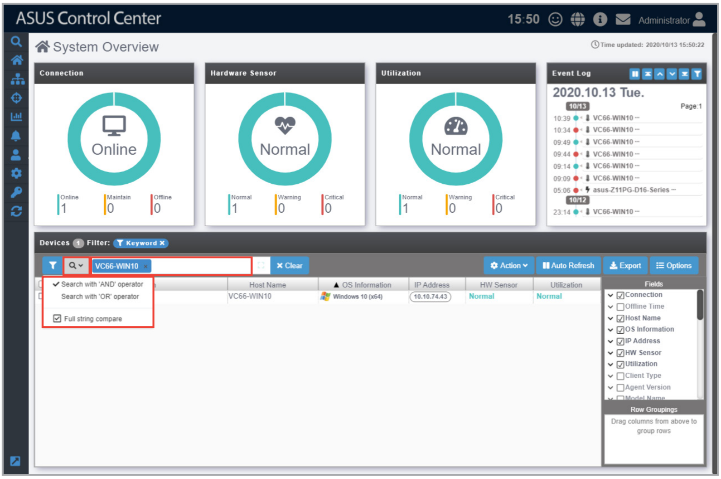
Drag columns from above to group rows

Filter devices using the Search Bar

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

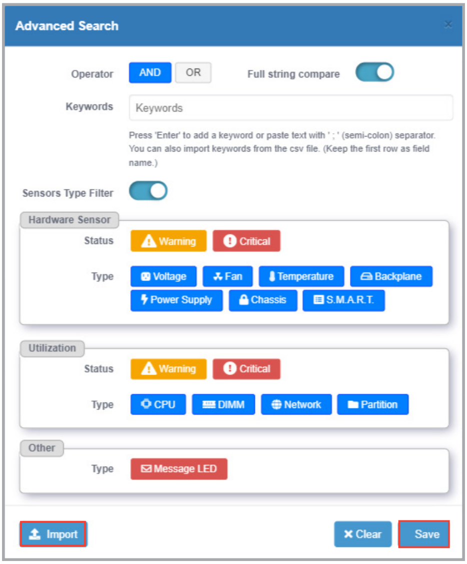
1. Enter keywords into the Search bar.
2. Click on 🔍⌄, then select the operator you wish to use.

- 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.

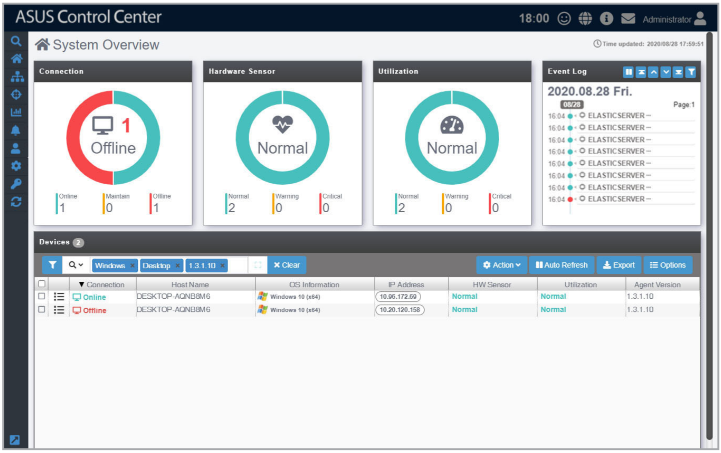
- Selecting the **‘AND’** option will return search results of items which match all the keywords.
- Selecting the **'OR'** option will return search results of items which at least one of the keywords.
- Enabling the **Full string compare** option will only return search results of items which have 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.



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.)

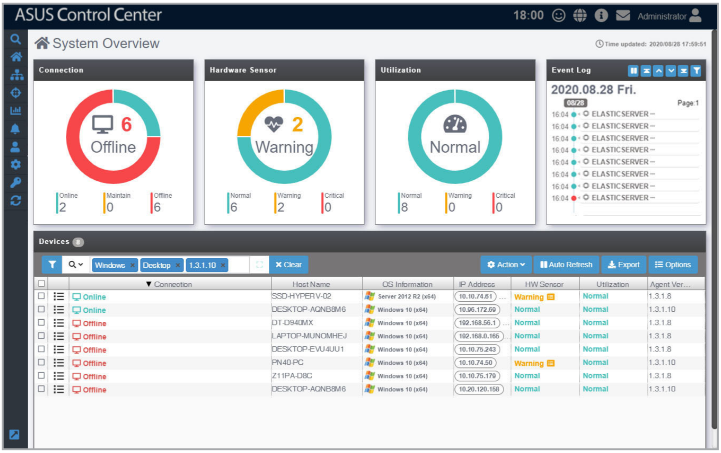
4. The search results will be displayed in the **Devices** list.

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



□		▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization	Agent Version
□	☰	Online	DESKTOP-AQNB8M6	Windows 10 (x64)	10.96.172.69	Normal	Normal	1.3.1.10
□	☰	Offline	DESKTOP-AQNB8M6	Windows 10 (x64)	10.20.120.158	Normal	Normal	1.3.1.10

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



□		▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization	Agent Ver...
□	☰	Online	SSD-HYPERV-02	Server 2012 R2 (x64)	10.10.74.61 ...	Warning	Normal	1.3.1.8
□	☰	Online	DESKTOP-AQNB8M6	Windows 10 (x64)	10.96.172.69	Normal	Normal	1.3.1.10
□	☰	Offline	DT-D940MX	Windows 10 (x64)	192.168.56.1 ...	Normal	Normal	1.3.1.8
□	☰	Offline	LAPTOP-MUNOMHEJ	Windows 10 (x64)	192.168.0.165 ...	Normal	Normal	1.3.1.8
□	☰	Offline	DESKTOP-EVU4UU1	Windows 10 (x64)	10.10.75.243	Normal	Normal	1.3.1.8
□	☰	Offline	PN40-PC	Windows 10 (x64)	10.10.74.50	Warning	Normal	1.3.1.10
□	☰	Offline	Z11PA-D8C	Windows 10 (x64)	10.10.75.179	Normal	Normal	1.3.1.8
□	☰	Offline	DESKTOP-AQNB8M6	Windows 10 (x64)	10.20.120.158	Normal	Normal	1.3.1.10

Filter devices using Column Headers

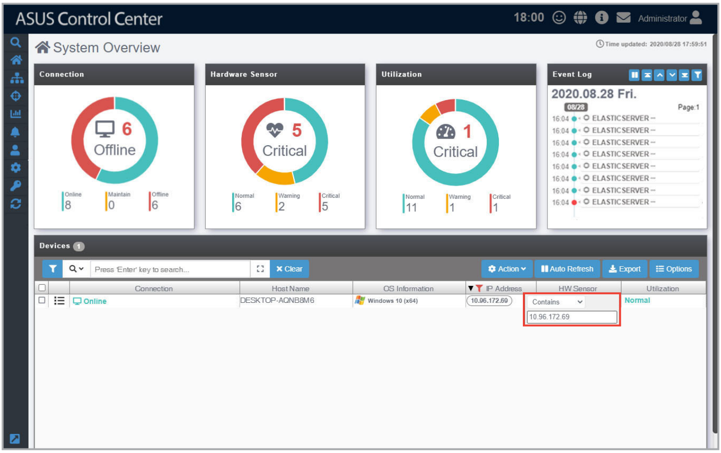
> To clear the filter and view all managed devices, click on **Clear**.

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

> 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.

> - 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.



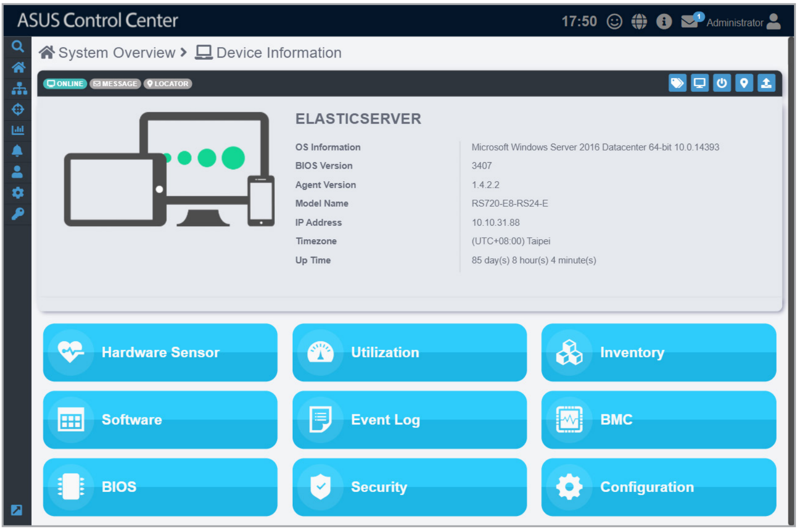
□		Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
□	☰	Online	DESKTOP-AQNB8M6	Windows 10 (x64)	10.96.172.69	Contains 10.96.172.69	Normal

2.2 Device Information

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**.



ELASTICSERVER

OS Information	Microsoft Windows Server 2016 Datacenter 64-bit 10.0.14393
BIOS Version	3407
Agent Version	1.4.2.2
Model Name	RS720-E8-RS24-E
IP Address	10.10.31.88
Timezone	(UTC+08:00) Taipei
Up Time	85 day(s) 8 hour(s) 4 minute(s)

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

- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

Device Statuses and Quick Buttons

ONLINE **Connection status** This item displays the connection status of the selected managed device.

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

> The Message status in only available on BMC enabled devices.

LOCATOR **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.

> The Locator status in only available on BMC enabled devices.

🏷 **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.

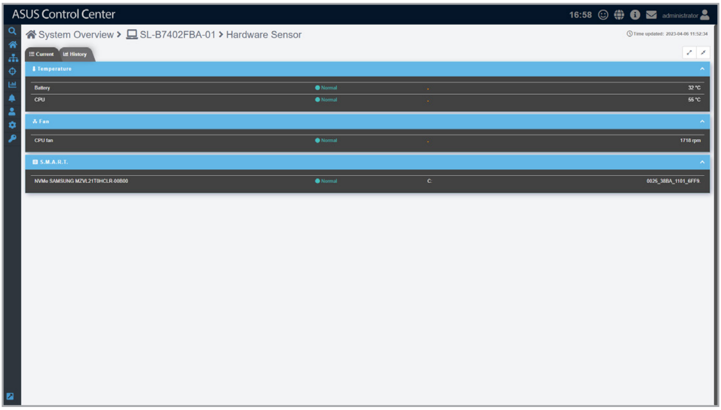
📍 **Locator LED** This item allows you to turn on/off the Locator LED.

⭱ **Refetch** This item will refetch the device data.

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.

- 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.


ASUS Control Center
16:58
administrator
System Overview > SL-B7402FBA-01 > Hardware Sensor
Time updated: 2023-04-06 11:52:34
Current
History

Temperature

Battery	● Normal	-	32 °C
CPU	● Normal	-	55 °C

Fan

CPU fan	● Normal	-	1718 rpm

S.M.A.R.T.

NVMe SAMSUNG MZVL21T0HCLR-00B00	● Normal	C:	0025_38BA_1101_6FF9.

Quick Buttons

☰ Click to switch to the Current tab.

📊 Click to switch to the History tab.

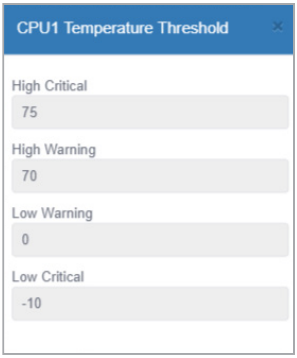
⤢ Click to expand all blocks.

⤡ 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

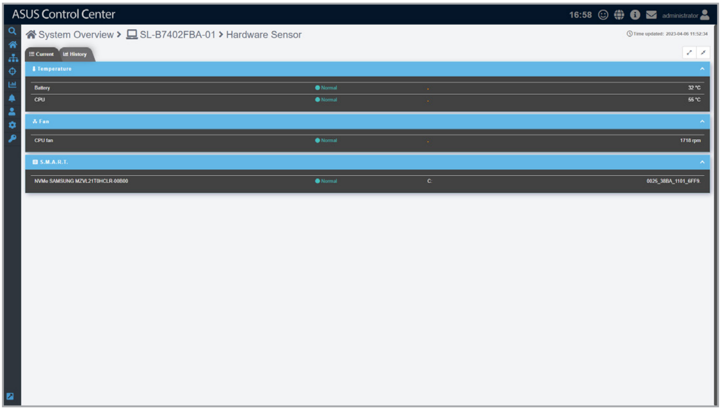
Low Critical
-10

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

Toggling between tabs

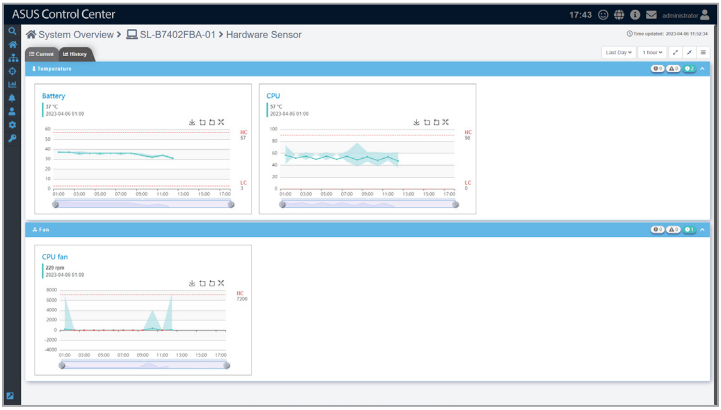
You can switch between different **Hardware Sensor** tabs by clicking the tabs in the top bar.

- **Current tab (default)**


ASUS Control Center
16:58
administrator
System Overview > SL-B7402FBA-01 > Hardware Sensor
Time updated: 2023-04-06 11:52:34
Current
History
Temperature
Fan
S.M.A.R.T.

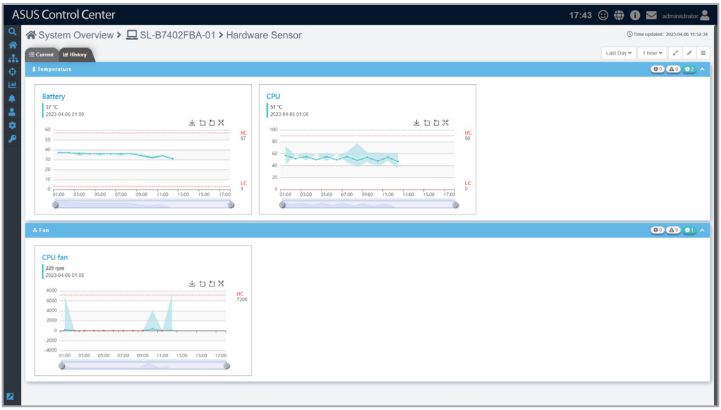
Battery	Normal	-	32 °C
CPU	Normal	-	55 °C
CPU fan	Normal	-	1718 rpm
NVMe SAMSUNG MZVL21T0HCLR-00B00	Normal	C:	0025_38BA_1101_6FF9.

- **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

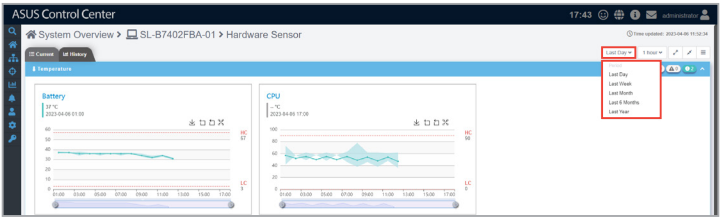
⤓ Click to download an image of the chart as a .png file.

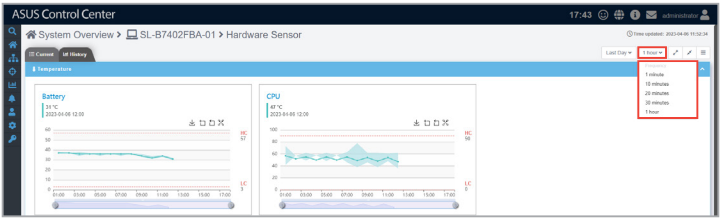
Click to zoom in on the timeline of the chart.

Click to zoom out on the timeline of the chart.

Click to restore the chart to its default view.

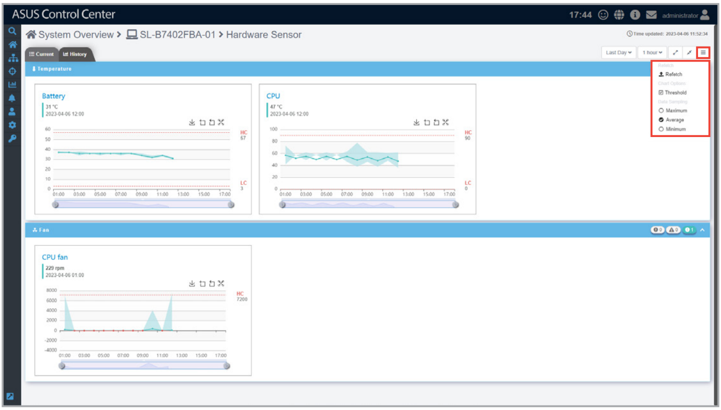
You can customize the charts by selecting the period of time you wish to view for the charts, then selecting the frequency for which the sensors should return data. This will be applied to the charts for all the sensors shown on this page.





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.



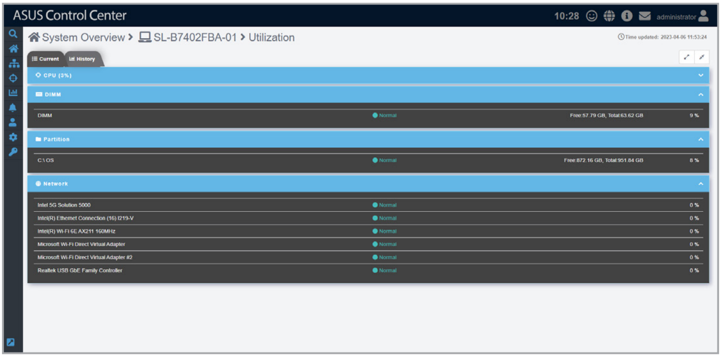
Refetch
Refetch
Chart Options
☑ Threshold
Data Sampling
○ Maximum
● Average
○ Minimum

Refetch	Allows you to trigger a refetch of device data.
Chart Options	Allows you to select whether the **Threshold** should be displayed on the chart.
Data Sampling	Allows you to select whether the **Maximum** values, **Average** values, or **Minimum** 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.

> 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.


ASUS Control Center
10:28
administrator
System Overview > SL-B7402FBA-01 > Utilization
Time updated: 2023-04-06 11:53:24
Current
History

CPU (3%)

DIMM

DIMM	Normal	Free:57.79 GB, Total:63.62 GB	9 %

Partition

C:\ OS	Normal	Free:872.16 GB, Total:951.84 GB	8 %

Network

Intel 5G Solution 5000	Normal	0 %
Intel(R) Ethernet Connection (16) I219-V	Normal	0 %
Intel(R) Wi-Fi 6E AX211 160MHz	Normal	0 %
Microsoft Wi-Fi Direct Virtual Adapter	Normal	0 %
Microsoft Wi-Fi Direct Virtual Adapter #2	Normal	0 %
Realtek USB GbE Family Controller	Normal	0 %

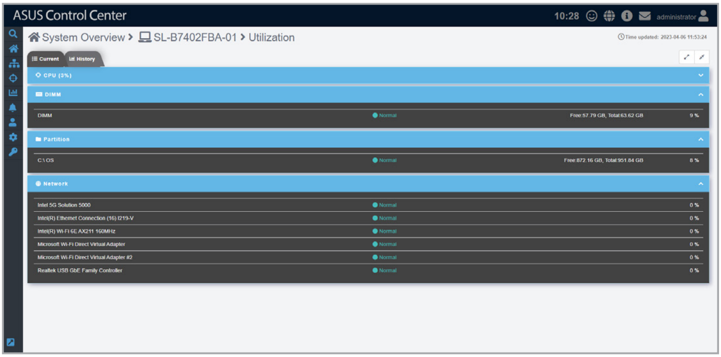
Quick Buttons

☰	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)**



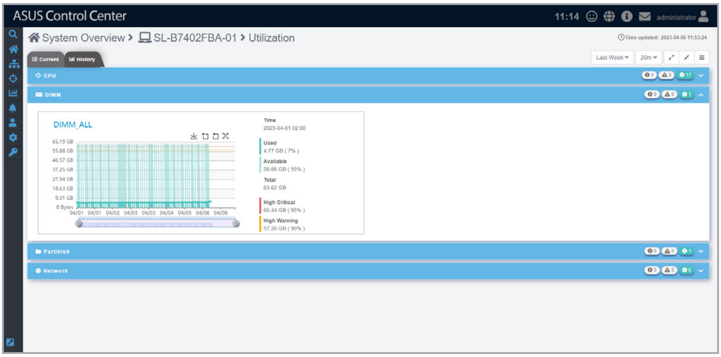
ASUS Control Center 10:28 administrator

System Overview > SL-B7402FBA-01 > Utilization

Time updated: 2023-04-06 11:53:24

DIMM	Normal	Free:57.79 GB, Total:63.62 GB	9 %
C:\ OS	Normal	Free:872.16 GB, Total:951.84 GB	8 %
Intel 5G Solution 5000	Normal		0 %
Intel(R) Ethernet Connection (16) I219-V	Normal		0 %
Intel(R) Wi-Fi 6E AX211 160MHz	Normal		0 %
Microsoft Wi-Fi Direct Virtual Adapter	Normal		0 %
Microsoft Wi-Fi Direct Virtual Adapter #2	Normal		0 %
Realtek USB GbE Family Controller	Normal		0 %

- **History tab**



ASUS Control Center 11:14 administrator

System Overview > SL-B7402FBA-01 > Utilization

Time updated: 2023-04-06 11:53:24

Time
2023-04-01 02:00

Used
4.77 GB (7%)

Available
58.86 GB (93%)

Total
63.62 GB

High Critical
60.44 GB (95%)

High Warning
57.26 GB (90%)

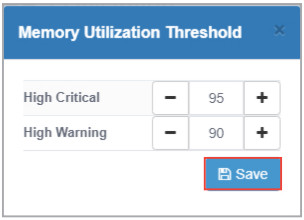
Editing the threshold values

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**.

The threshold options for each item may vary.

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

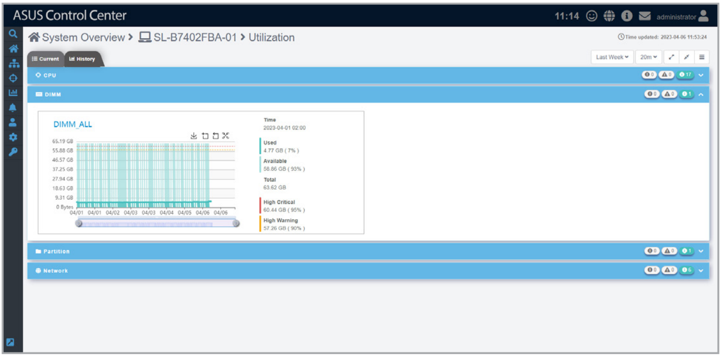


Memory Utilization Threshold

High Critical	−	95	+
High Warning	−	90	+

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.



Time
2023-04-01 02:00

Used
4.77 GB (7%)

Available
58.86 GB (93%)

Total
63.62 GB

High Critical
60.44 GB (95%)

High Warning
57.26 GB (90%)

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

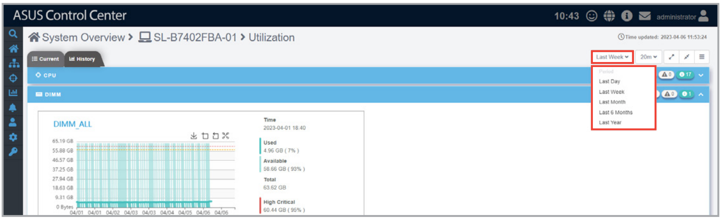
⤓ Click to download an image of the chart as a .png file.

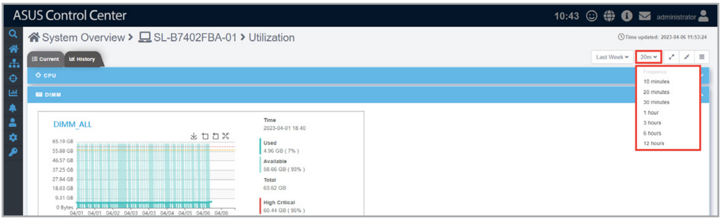
Click to zoom in on the timeline of the chart.

Click to zoom out on the timeline of the chart.

Click to restore the chart to its default view.

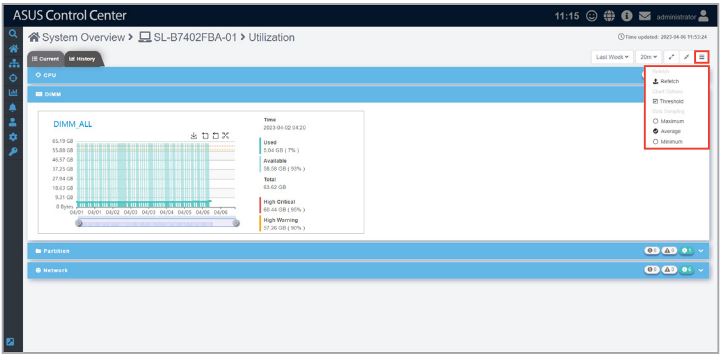
You can customize the charts by selecting the period of time you wish to view for the charts, then selecting the frequency for which the sensors should return data. This will be applied to the charts for all the sensors shown on this page.





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.



Time updated: 2023-04-06 11:53:24

Time
2023-04-02 04:20

Used
5.04 GB (7%)

Available
58.58 GB (93%)

Total
63.62 GB

High Critical
60.44 GB (95%)

High Warning
57.26 GB (90%)

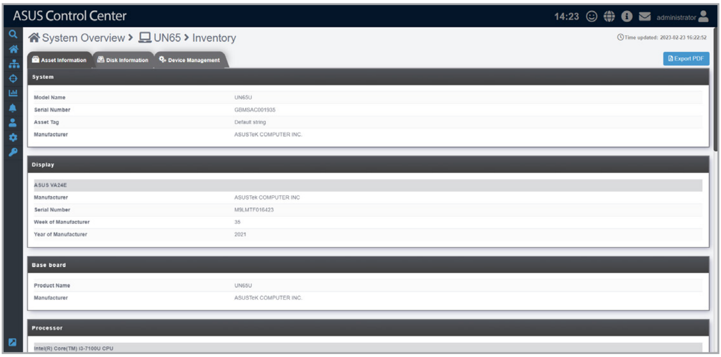
Refetch	Allows you to trigger a refetch of device data.
Chart Options	Allows you to select whether the **Threshold** should be displayed on the chart.
Data Sampling	Allows you to select whether the **Maximum** values, **Average** values, or **Minimum** values should be displayed on the charts.

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.



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

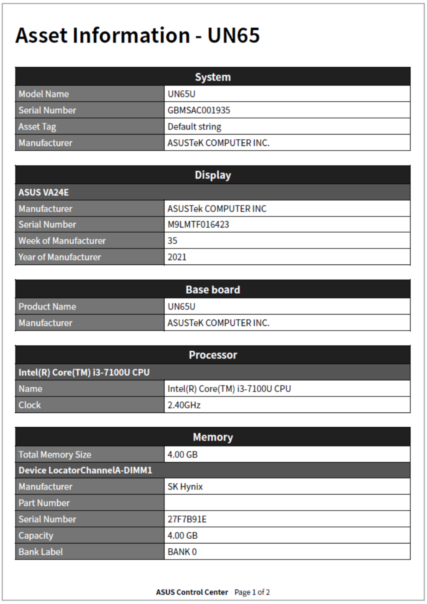
Base board

Product Name	UN65U
Manufacturer	ASUSTeK COMPUTER INC.

Processor

Intel(R) Core(TM) i3-7100U CPU

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.

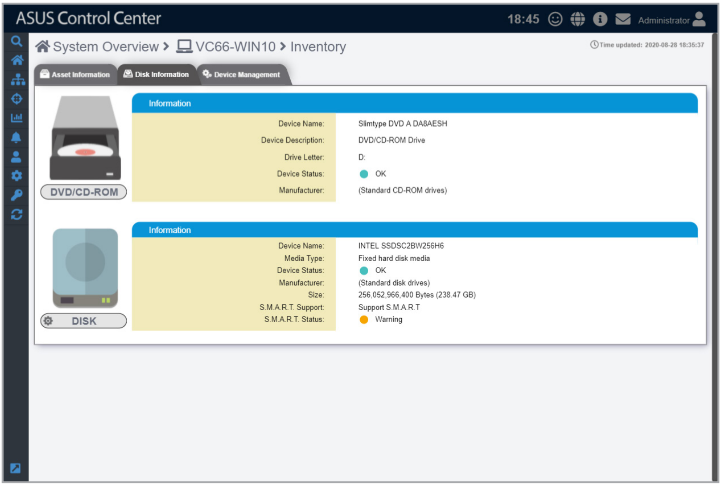
Processor	
Intel(R) Core(TM) i3-7100U CPU	
Name	Intel(R) Core(TM) i3-7100U CPU
Clock	2.40GHz

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.



Information

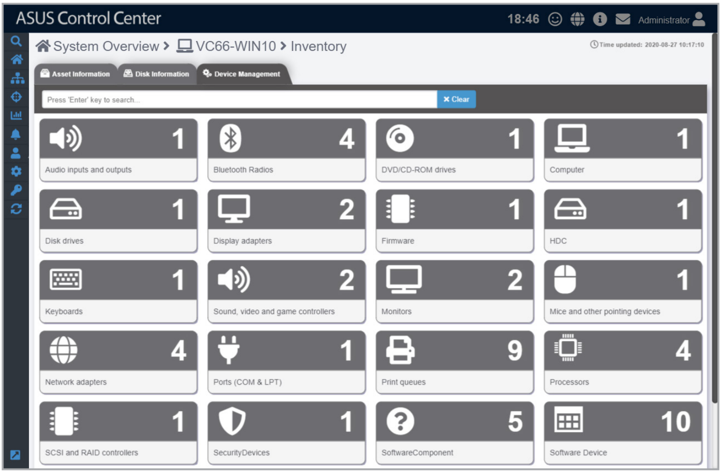
Device Name:	Slimtype DVD A DA8AESH
Device Description:	DVD/CD-ROM Drive
Drive Letter:	D:
Device Status:	● OK
Manufacturer:	(Standard CD-ROM drives)

Information

Device Name:	INTEL SSDSC2BW256H6
Media Type:	Fixed hard disk media
Device Status:	● OK
Manufacturer:	(Standard disk drives)
Size:	256,052,966,400 Bytes (238.47 GB)
S.M.A.R.T. Support:	Support S.M.A.R.T
S.M.A.R.T. Status:	● Warning

Device Management

View the Device Management properties of the managed device.


ASUS Control Center
18:46
Administrator
System Overview > VC66-WIN10 > Inventory
Time updated: 2020-08-27 10:17:10
Asset Information
Disk Information
Device Management
Press 'Enter' key to search...
✕ Clear

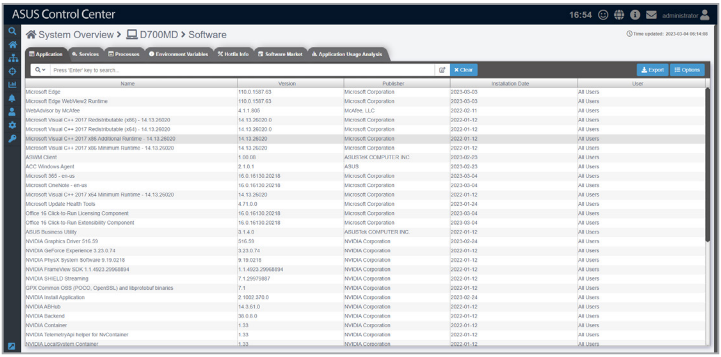
1 Audio inputs and outputs	4 Bluetooth Radios	1 DVD/CD-ROM drives	1 Computer
1 Disk drives	2 Display adapters	1 Firmware	1 HDC
1 Keyboards	2 Sound, video and game controllers	2 Monitors	1 Mice and other pointing devices
4 Network adapters	1 Ports (COM & LPT)	9 Print queues	4 Processors
1 SCSI and RAID controllers	1 SecurityDevices	5 SoftwareComponent	10 Software Device

2.2.4 Software

This item displays details on the software and applications with the **Application**, **Services**, **Processes**, **Environment Variables**, **Hotfix Info**, and **Application Usage Analysis** tab. You may also install applications from the **Software Market** tab.

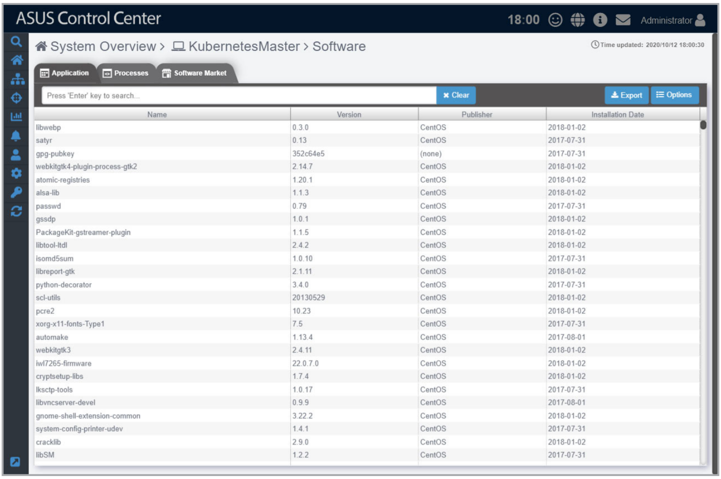
- To export the table click the **Export** button, enter a filename, then click **OK**.
- The tabs may differ between Linux and Windows® systems.

For Windows® system:



Name	Version	Publisher	Installation Date	User
Microsoft Edge	110.0.1587.63	Microsoft Corporation	2023-03-03	All Users
Microsoft Edge WebView2 Runtime	110.0.1587.63	Microsoft Corporation	2023-03-03	All Users
WebAdvisor by McAfee	4.1.1.805	McAfee, LLC	2022-02-11	All Users
Microsoft Visual C++ 2017 Redistributable (x86) - 14.13.26020	14.13.26020.0	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 Redistributable (x64) - 14.13.26020	14.13.26020.0	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 x86 Additional Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
ASWM Client	1.00.08	ASUSTeK COMPUTER INC.	2023-02-23	All Users
ACC Windows Agent	2.1.0.1	ASUS	2023-02-23	All Users
Microsoft 365 - en-us	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Microsoft OneNote - en-us	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
Microsoft Update Health Tools	4.71.0.0	Microsoft Corporation	2023-01-24	All Users
Office 16 Click-to-Run Licensing Component	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Office 16 Click-to-Run Extensibility Component	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
ASUS Business Utility	3.1.4.0	ASUSTek COMPUTER INC.	2022-01-12	All Users
NVIDIA Graphics Driver 516.59	516.59	NVIDIA Corporation	2023-02-24	All Users
NVIDIA GeForce Experience 3.23.0.74	3.23.0.74	NVIDIA Corporation	2022-01-12	All Users
NVIDIA PhysX System Software 9.19.0218	9.19.0218	NVIDIA Corporation	2022-01-12	All Users
NVIDIA FrameView SDK 1.1.4923.29968894	1.1.4923.29968894	NVIDIA Corporation	2022-01-12	All Users
NVIDIA SHIELD Streaming	7.1.29979887	NVIDIA Corporation	2022-01-12	All Users
GPX Common OSS (POCO, OpenSSL) and libprotobuf binaries	7.1	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Install Application	2.1002.370.0	NVIDIA Corporation	2023-02-24	All Users
NVIDIA ABHub	14.3.61.0	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Backend	38.0.8.0	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Container	1.33	NVIDIA Corporation	2022-01-12	All Users
NVIDIA TelemetryApi helper for NvContainer	1.33	NVIDIA Corporation	2022-01-12	All Users
NVIDIA LocalSystem Container	1.33	NVIDIA Corporation	2022-01-12	All Users

For Linux system:

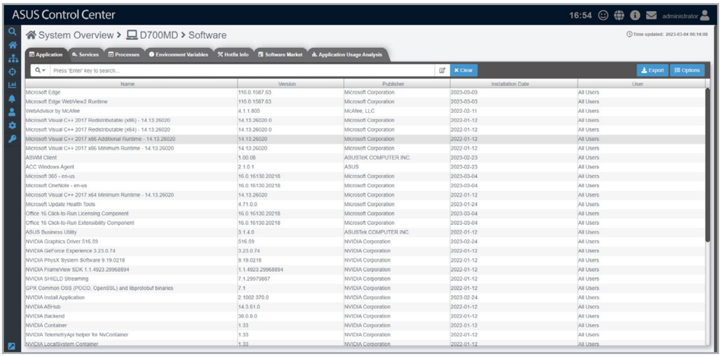

ASUS Control Center
18:00
Administrator
System Overview > KubernetesMaster > Software
Time updated: 2020/10/12 18:00:30
Application
Processes
Software Market
Press 'Enter' key to search...
Clear
Export
Options

Name	Version	Publisher	Installation Date
libwebp	0.3.0	CentOS	2018-01-02
satyr	0.13	CentOS	2017-07-31
gpg-pubkey	352c64e5	(none)	2017-07-31
webkitgtk4-plugin-process-gtk2	2.14.7	CentOS	2018-01-02
atomic-registries	1.20.1	CentOS	2018-01-02
alsa-lib	1.1.3	CentOS	2018-01-02
passwd	0.79	CentOS	2017-07-31
gssdp	1.0.1	CentOS	2018-01-02
PackageKit-gstreamer-plugin	1.1.5	CentOS	2018-01-02
libtool-ltdl	2.4.2	CentOS	2018-01-02
isomd5sum	1.0.10	CentOS	2017-07-31
libreport-gtk	2.1.11	CentOS	2018-01-02
python-decorator	3.4.0	CentOS	2017-07-31
scl-utils	20130529	CentOS	2018-01-02
pcre2	10.23	CentOS	2018-01-02
xorg-x11-fonts-Type1	7.5	CentOS	2017-07-31
automake	1.13.4	CentOS	2017-08-01
webkitgtk3	2.4.11	CentOS	2018-01-02
iwl7265-firmware	22.0.7.0	CentOS	2018-01-02
cryptsetup-libs	1.7.4	CentOS	2018-01-02
lksctp-tools	1.0.17	CentOS	2017-07-31
libvncserver-devel	0.9.9	CentOS	2017-08-01
gnome-shell-extension-common	3.22.2	CentOS	2018-01-02
system-config-printer-udev	1.4.1	CentOS	2017-07-31
cracklib	2.9.0	CentOS	2018-01-02
libSM	1.2.2	CentOS	2017-07-31

Application

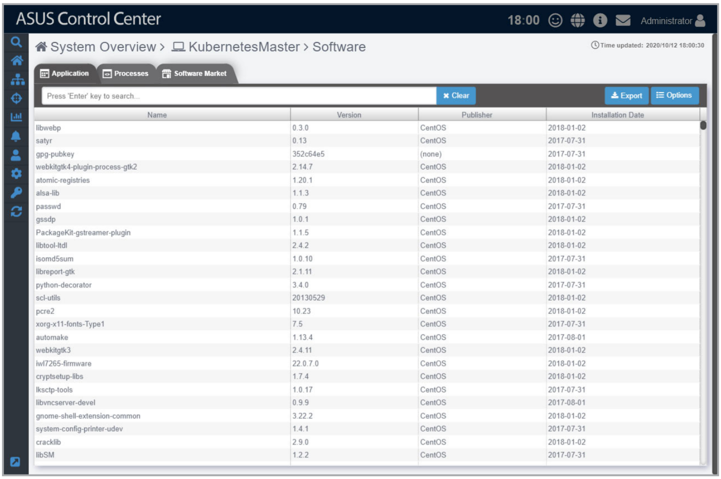
This tab shows all the applications installed on the managed device, it should be the same as the Programs and Feature folder in Windows®.

For Windows® system:



Name	Version	Publisher	Installation Date	User
Microsoft Edge	110.0.1587.63	Microsoft Corporation	2023-03-03	All Users
Microsoft Edge WebView2 Runtime	110.0.1587.63	Microsoft Corporation	2023-03-03	All Users
WebAdvisor by McAfee	4.1.1.805	McAfee, LLC	2022-02-11	All Users
Microsoft Visual C++ 2017 Redistributable (x86) - 14.13.26020	14.13.26020.0	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 Redistributable (x64) - 14.13.26020	14.13.26020.0	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 x86 Additional Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
Microsoft Visual C++ 2017 x86 Minimum Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
ASWM Client	1.00.08	ASUSTeK COMPUTER INC.	2023-02-23	All Users
ACC Windows Agent	2.1.0.1	ASUS	2023-02-23	All Users
Microsoft 365 - en-us	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Microsoft OneNote - en-us	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Microsoft Visual C++ 2017 x64 Minimum Runtime - 14.13.26020	14.13.26020	Microsoft Corporation	2022-01-12	All Users
Microsoft Update Health Tools	4.71.0.0	Microsoft Corporation	2023-01-24	All Users
Office 16 Click-to-Run Licensing Component	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
Office 16 Click-to-Run Extensibility Component	16.0.16130.20218	Microsoft Corporation	2023-03-04	All Users
ASUS Business Utility	3.1.4.0	ASUSTek COMPUTER INC.	2022-01-12	All Users
NVIDIA Graphics Driver 516.59	516.59	NVIDIA Corporation	2023-02-24	All Users
NVIDIA GeForce Experience 3.23.0.74	3.23.0.74	NVIDIA Corporation	2022-01-12	All Users
NVIDIA PhysX System Software 9.19.0218	9.19.0218	NVIDIA Corporation	2022-01-12	All Users
NVIDIA FrameView SDK 1.1.4923.29968894	1.1.4923.29968894	NVIDIA Corporation	2022-01-12	All Users
NVIDIA SHIELD Streaming	7.1.29979887	NVIDIA Corporation	2022-01-12	All Users
GPX Common OSS (POCO, OpenSSL) and libprotobuf binaries	7.1	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Install Application	2.1002.370.0	NVIDIA Corporation	2023-02-24	All Users
NVIDIA ABHub	14.3.61.0	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Backend	38.0.8.0	NVIDIA Corporation	2022-01-12	All Users
NVIDIA Container	1.33	NVIDIA Corporation	2022-01-12	All Users
NVIDIA TelemetryApi helper for NvContainer	1.33	NVIDIA Corporation	2022-01-12	All Users
NVIDIA LocalSystem Container	1.33	NVIDIA Corporation	2022-01-12	All Users

For Linux system:

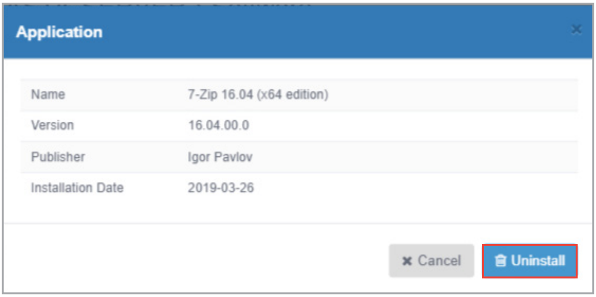


ASUS Control Center
18:00
Administrator
System Overview > KubernetesMaster > Software
Time updated: 2020/10/12 18:00:30
Application
Processes
Software Market
Press 'Enter' key to search...
Clear
Export
Options

Name	Version	Publisher	Installation Date
libwebp	0.3.0	CentOS	2018-01-02
satyr	0.13	CentOS	2017-07-31
gpg-pubkey	352c64e5	(none)	2017-07-31
webkitgtk4-plugin-process-gtk2	2.14.7	CentOS	2018-01-02
atomic-registries	1.20.1	CentOS	2018-01-02
alsa-lib	1.1.3	CentOS	2018-01-02
passwd	0.79	CentOS	2017-07-31
gssdp	1.0.1	CentOS	2018-01-02
PackageKit-gstreamer-plugin	1.1.5	CentOS	2018-01-02
libtool-ltdl	2.4.2	CentOS	2018-01-02
isomd5sum	1.0.10	CentOS	2017-07-31
libreport-gtk	2.1.11	CentOS	2018-01-02
python-decorator	3.4.0	CentOS	2017-07-31
scl-utils	20130529	CentOS	2018-01-02
pcre2	10.23	CentOS	2018-01-02
xorg-x11-fonts-Type1	7.5	CentOS	2017-07-31
automake	1.13.4	CentOS	2017-08-01
webkitgtk3	2.4.11	CentOS	2018-01-02
iwl7265-firmware	22.0.7.0	CentOS	2018-01-02
cryptsetup-libs	1.7.4	CentOS	2018-01-02
lksctp-tools	1.0.17	CentOS	2017-07-31
libvncserver-devel	0.9.9	CentOS	2017-08-01
gnome-shell-extension-common	3.22.2	CentOS	2018-01-02
system-config-printer-udev	1.4.1	CentOS	2017-07-31
cracklib	2.9.0	CentOS	2018-01-02
libSM	1.2.2	CentOS	2017-07-31

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

- 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.

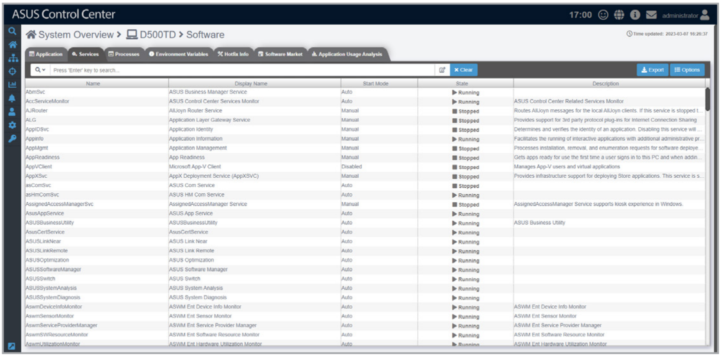


Application

Name	7-Zip 16.04 (x64 edition)
Version	16.04.00.0
Publisher	Igor Pavlov
Installation Date	2019-03-26

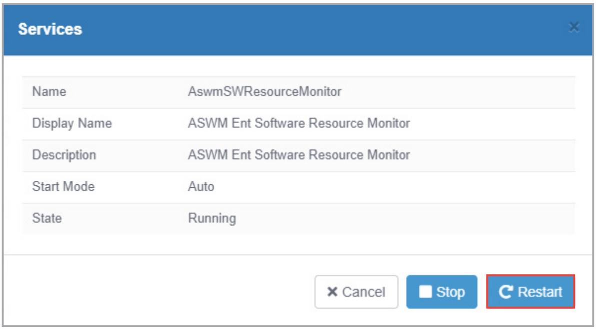
Services (Windows only)

This tab shows all the services available on the managed device, it should be the same as the Services tab in Windows® Task manager.



Name	Display Name	Start Mode	State	Description
AbmSvc	ASUS Business Manager Service	Auto	▶ Running	
AccServiceMonitor	ASUS Control Center Services Monitor	Auto	▶ Running	ASUS Control Center Related Services Monitor
AJRouter	AllJoyn Router Service	Manual	■ Stopped	Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped t...
ALG	Application Layer Gateway Service	Manual	■ Stopped	Provides support for 3rd party protocol plug-ins for Internet Connection Sharing
AppIDSvc	Application Identity	Manual	■ Stopped	Determines and verifies the identity of an application. Disabling this service will ...
Appinfo	Application Information	Manual	▶ Running	Facilitates the running of interactive applications with additional administrative pr...
AppMgmt	Application Management	Manual	■ Stopped	Processes installation, removal, and enumeration requests for software deploye...
AppReadiness	App Readiness	Manual	■ Stopped	Gets apps ready for use the first time a user signs in to this PC and when addin...
AppVClient	Microsoft App-V Client	Disabled	■ Stopped	Manages App-V users and virtual applications
AppXSvc	AppX Deployment Service (AppXSVC)	Manual	■ Stopped	Provides infrastructure support for deploying Store applications. This service is s...
asComSvc	ASUS Com Service	Auto	■ Stopped	
asHmComSvc	ASUS HM Com Service	Auto	▶ Running	
AssignedAccessManagerSvc	AssignedAccessManager Service	Manual	■ Stopped	AssignedAccessManager Service supports kiosk experience in Windows.
AsusAppService	ASUS App Service	Auto	▶ Running	
ASUSBusinessUtility	ASUSBusinessUtility	Auto	▶ Running	ASUS Business Utility
AsusCertService	AsusCertService	Auto	▶ Running	
ASUSLinkNear	ASUS Link Near	Auto	▶ Running	
ASUSLinkRemote	ASUS Link Remote	Auto	▶ Running	
ASUSOptimization	ASUS Optimization	Auto	▶ Running	
ASUSSoftwareManager	ASUS Software Manager	Auto	▶ Running	
ASUSSwitch	ASUS Switch	Auto	▶ Running	
ASUSSystemAnalysis	ASUS System Analysis	Auto	▶ Running	
ASUSSystemDiagnosis	ASUS System Diagnosis	Auto	▶ Running	
AswmDeviceInfoMonitor	ASWM Ent Device Info Monitor	Auto	▶ Running	ASWM Ent Device Info Monitor
AswmSensorMonitor	ASWM Ent Sensor Monitor	Auto	▶ Running	ASWM Ent Sensor Monitor
AswmServiceProviderManager	ASWM Ent Service Provider Manager	Auto	▶ Running	ASWM Ent Service Provider Manager
AswmSWResourceMonitor	ASWM Ent Software Resource Monitor	Auto	▶ Running	ASWM Ent Software Resource Monitor
AswmUtilizationMonitor	ASWM Ent Hardware Utilization Monitor	Auto	▶ Running	ASWM Ent Hardware Utilization Monitor

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**.

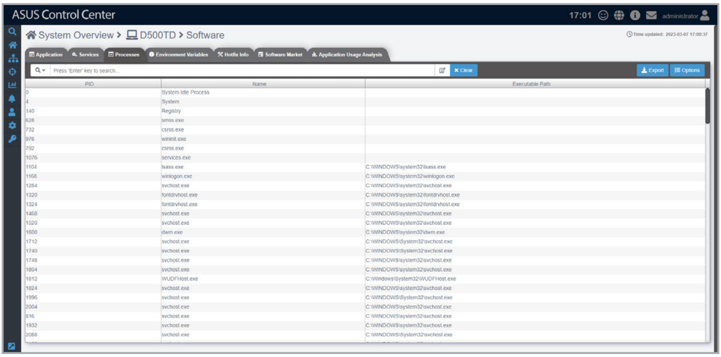


Name	AswmSWResourceMonitor
Display Name	ASWM Ent Software Resource Monitor
Description	ASWM Ent Software Resource Monitor
Start Mode	Auto
State	Running

Processes

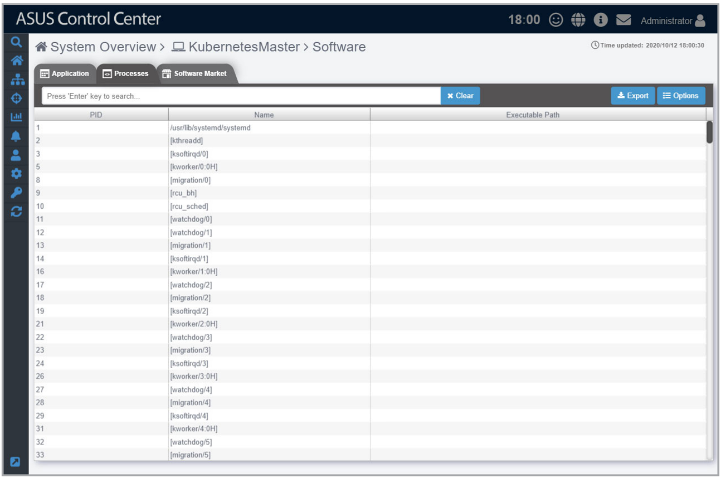
This tab shows all the processes on the managed device, it should be the same as the Process tab in Windows® Task manager.

For Windows® system:



PID	Name	Executable Path
0	System Idle Process	
4	System	
140	Registry	
628	smss.exe	
732	csrss.exe	
976	wininit.exe	
792	csrss.exe	
1076	services.exe	
1104	lsass.exe	C:\WINDOWS\system32\lsass.exe
1168	winlogon.exe	C:\WINDOWS\system32\winlogon.exe
1284	svchost.exe	C:\WINDOWS\system32\svchost.exe
1320	fontdrvhost.exe	C:\WINDOWS\system32\fontdrvhost.exe
1324	fontdrvhost.exe	C:\WINDOWS\system32\fontdrvhost.exe
1468	svchost.exe	C:\WINDOWS\system32\svchost.exe
1520	svchost.exe	C:\WINDOWS\system32\svchost.exe
1600	dwm.exe	C:\WINDOWS\system32\dwm.exe
1712	svchost.exe	C:\WINDOWS\System32\svchost.exe
1740	svchost.exe	C:\WINDOWS\System32\svchost.exe
1748	svchost.exe	C:\WINDOWS\system32\svchost.exe
1804	svchost.exe	C:\WINDOWS\system32\svchost.exe
1812	WUDFHost.exe	C:\Windows\System32\WUDFHost.exe
1824	svchost.exe	C:\WINDOWS\system32\svchost.exe
1996	svchost.exe	C:\WINDOWS\System32\svchost.exe
2004	svchost.exe	C:\WINDOWS\system32\svchost.exe
816	svchost.exe	C:\WINDOWS\system32\svchost.exe
1932	svchost.exe	C:\WINDOWS\system32\svchost.exe
2088	svchost.exe	C:\WINDOWS\System32\svchost.exe

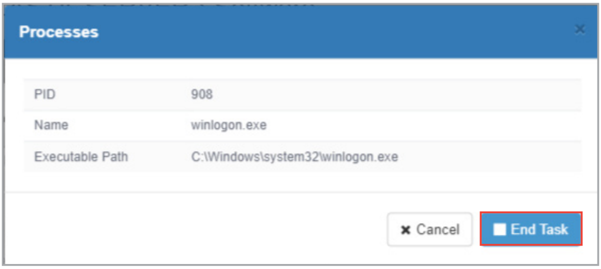
For Linux system:



ASUS Control Center
18:00
Administrator
System Overview > KubernetesMaster > Software
Time updated: 2020/10/12 18:00:30
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/0]	
5	[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]	

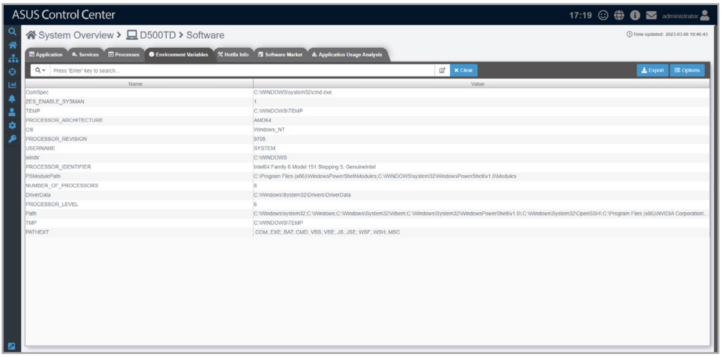
You may also click on a process then select **End Task** to end the process.



PID	908
Name	winlogon.exe
Executable Path	C:\Windows\system32\winlogon.exe

Environment Variables (Windows only)

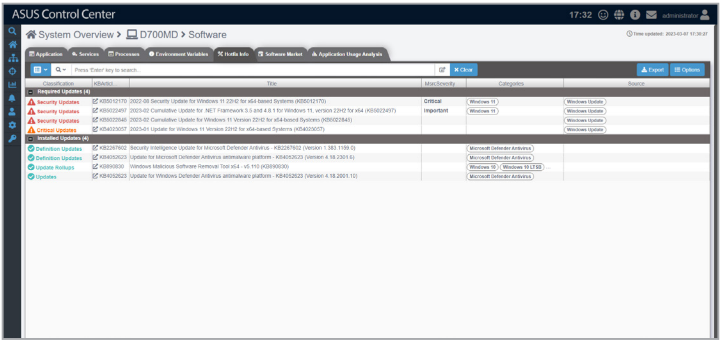
This tab shows all the environment variables on the managed device, it should be the same as Environment Variables in Windows® System Properties menu.



Name	Value
ComSpec	C:\WINDOWS\system32\cmd.exe
ZES_ENABLE_SYSMAN	1
TEMP	C:\WINDOWS\TEMP
PROCESSOR_ARCHITECTURE	AMD64
OS	Windows_NT
PROCESSOR_REVISION	9705
USERNAME	SYSTEM
windir	C:\WINDOWS
PROCESSOR_IDENTIFIER	Intel64 Family 6 Model 151 Stepping 5, GenuineIntel
PSModulePath	C:\Program Files (x86)\WindowsPowerShell\Modules;C:\WINDOWS\system32\WindowsPowerShell\v1.0\Modules
NUMBER_OF_PROCESSORS	8
DriverData	C:\Windows\System32\Drivers\DriverData
PROCESSOR_LEVEL	6
Path	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files (x86)\NVIDIA Corporation\...
TMP	C:\WINDOWS\TEMP
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

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**.



ASUS Control Center

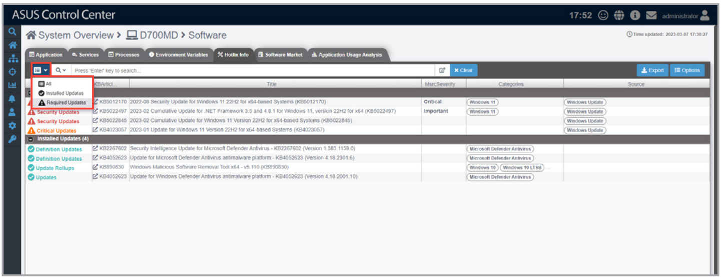
17:32 administrator

System Overview > D700MD > Software

Time updated: 2023-03-07 17:30:27

Classification	KBArticl...	Title	MsrcSeverity	Categories	Source
Required Updates (4)					
Security Updates	KB5012170	2022-08 Security Update for Windows 11 22H2 for x64-based Systems (KB5012170)	Critical	Windows 11	Windows Update
Security Updates	KB5022497	2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 (KB5022497)	Important	Windows 11	Windows Update
Security Updates	KB5022845	2023-02 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5022845)			Windows Update
Critical Updates	KB4023057	2023-01 Update for Windows 11 Version 22H2 for x64-based Systems (KB4023057)			Windows Update
Installed Updates (4)					
Definition Updates	KB2267602	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.383.1159.0)		Microsoft Defender Antivirus	
Definition Updates	KB4052623	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2301.6)		Microsoft Defender Antivirus	
Update Rollups	KB890830	Windows Malicious Software Removal Tool x64 - v5.110 (KB890830)		Windows 10 Windows 10 LTSB ...	
Updates	KB4052623	Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)		Microsoft Defender Antivirus	

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.



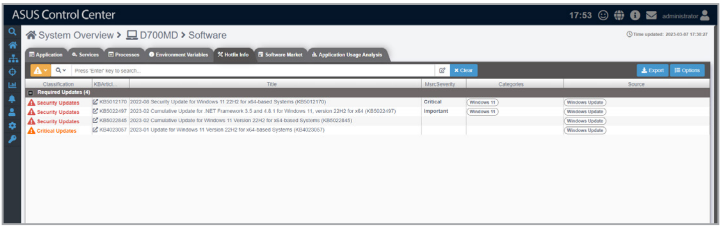
ASUS Control Center

17:52 administrator

System Overview > D700MD > Software

Time updated: 2023-03-07 17:30:27

Classification	KBArticl...	Title	MsrcSeverity	Categories	Source
	KB5012170	2022-08 Security Update for Windows 11 22H2 for x64-based Systems (KB5012170)	Critical	Windows 11	Windows Update
Security Updates	KB5022497	2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 (KB5022497)	Important	Windows 11	Windows Update
Security Updates	KB5022845	2023-02 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5022845)			Windows Update
Critical Updates	KB4023057	2023-01 Update for Windows 11 Version 22H2 for x64-based Systems (KB4023057)			Windows Update
Installed Updates (4)					
Definition Updates	KB2267602	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.383.1159.0)		Microsoft Defender Antivirus	
Definition Updates	KB4052623	Update for Microsoft Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2301.6)		Microsoft Defender Antivirus	
Update Rollups	KB890830	Windows Malicious Software Removal Tool x64 - v5.110 (KB890830)		Windows 10 Windows 10 LTSB ...	
Updates	KB4052623	Update for Windows Defender Antivirus antimalware platform - KB4052623 (Version 4.18.2001.10)		Microsoft Defender Antivirus	



ASUS Control Center

17:53 administrator

System Overview > D700MD > Software

Time updated: 2023-03-07 17:30:27

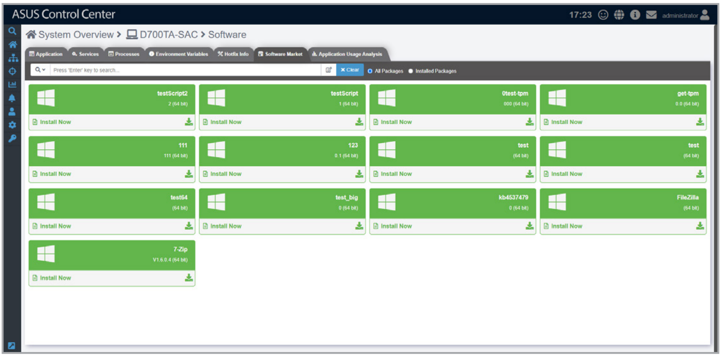
Classification	KBArticl...	Title	MsrcSeverity	Categories	Source
Required Updates (4)					
Security Updates	KB5012170	2022-08 Security Update for Windows 11 22H2 for x64-based Systems (KB5012170)	Critical	Windows 11	Windows Update
Security Updates	KB5022497	2023-02 Cumulative Update for .NET Framework 3.5 and 4.8.1 for Windows 11, version 22H2 for x64 (KB5022497)	Important	Windows 11	Windows Update
Security Updates	KB5022845	2023-02 Cumulative Update for Windows 11 Version 22H2 for x64-based Systems (KB5022845)			Windows Update
Critical Updates	KB4023057	2023-01 Update for Windows 11 Version 22H2 for x64-based Systems (KB4023057)			Windows Update

Software Market

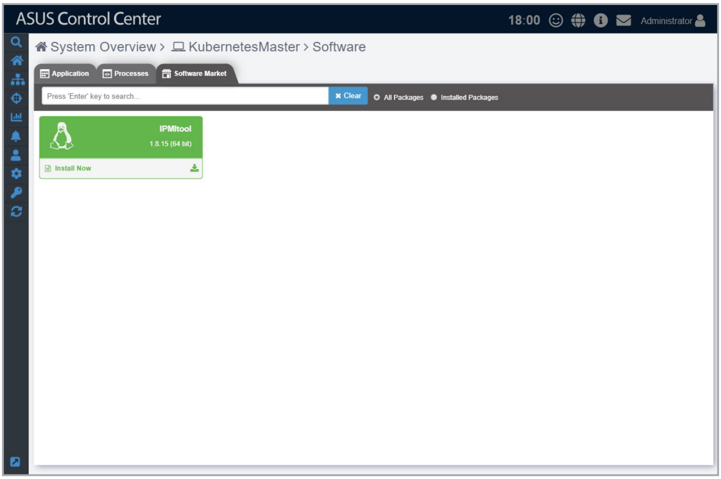
This tab shows software packages uploaded to the software pool, and also whether a software package has been installed to this device. The software packages displayed depends on the OS of this device, Windows® devices will only see Windows® softwares, and Linux devices will only see Linux softwares. You may also click on **Install Now** on software package that has not yet been installed on to install the software package to this device.

Refer to the **Software Pool** section for more information on adding and removing software packages from the software pool.

For Windows® system:

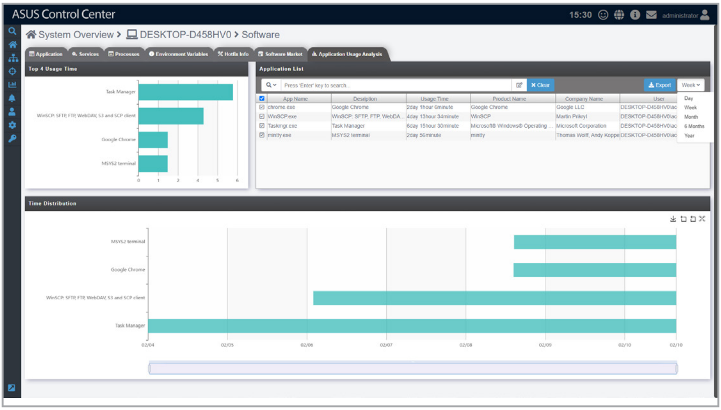


For Linux system:



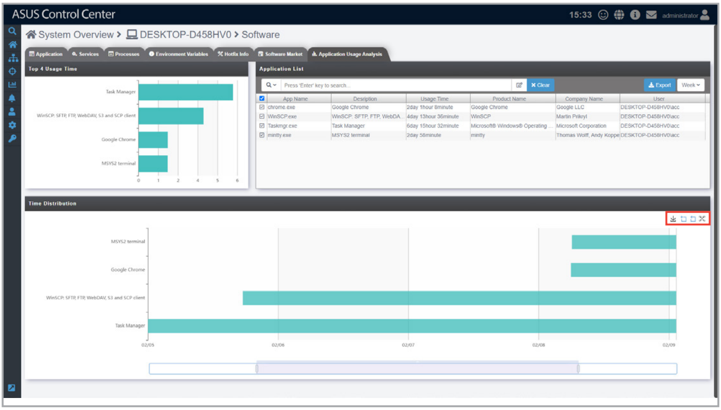
Application Usage Analysis

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.



☑	App Name	Desription	Usage Time	Product Name	Company Name	User
☑	chrome.exe	Google Chrome	2day 1hour 6minute	Google Chrome	Google LLC	DESKTOP-D458HV0\ac
☑	WinSCP.exe	WinSCP: SFTP, FTP, WebDA...	4day 13hour 34minute	WinSCP	Martin Prikryl	DESKTOP-D458HV0\ac
☑	Taskmgr.exe	Task Manager	6day 15hour 30minute	Microsoft® Windows® Operating ...	Microsoft Corporation	DESKTOP-D458HV0\ac
☑	mintty.exe	MSYS2 terminal	2day 56minute	mintty	Thomas Wolff, Andy Koppe	DESKTOP-D458HV0\ac

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.



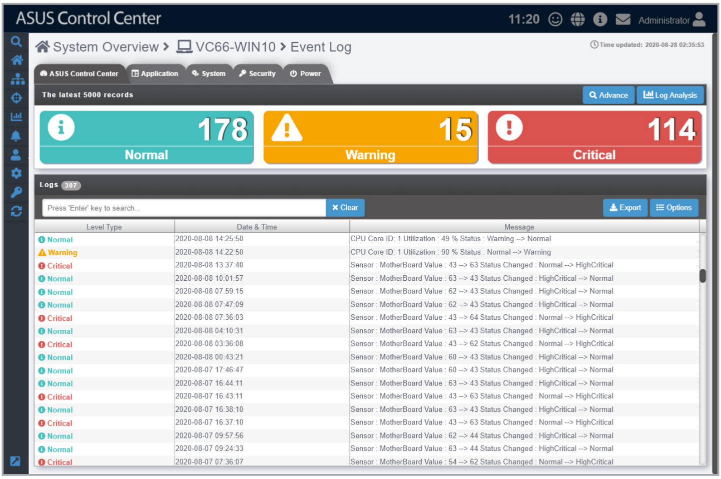
☑	App Name	Desription	Usage Time	Product Name	Company Name	User
☑	chrome.exe	Google Chrome	2day 1hour 8minute	Google Chrome	Google LLC	DESKTOP-D458HV0\acc
☑	WinSCP.exe	WinSCP: SFTP, FTP, WebDA...	4day 13hour 36minute	WinSCP	Martin Prikryl	DESKTOP-D458HV0\acc
☑	Taskmgr.exe	Task Manager	6day 15hour 32minute	Microsoft® Windows® Operating ...	Microsoft Corporation	DESKTOP-D458HV0\acc
☑	mintty.exe	MSYS2 terminal	2day 58minute	mintty	Thomas Wolff, Andy Koppe	DESKTOP-D458HV0\acc

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.

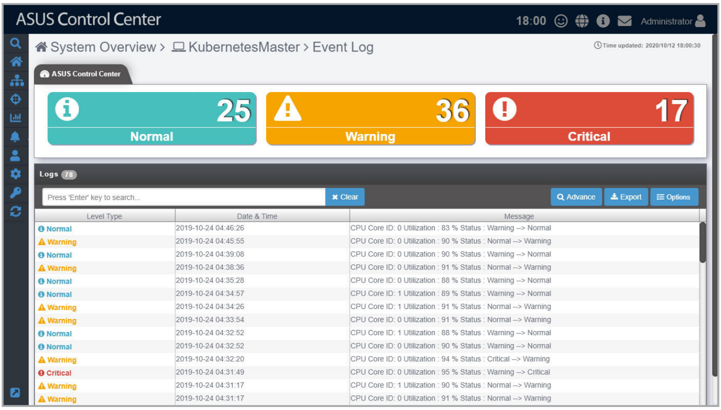
- To export the Event Log click the **Export** button, enter a filename, then click **OK**.
- Linux systems only support the **ASUS Control Center** tab.

For Windows® system:



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:

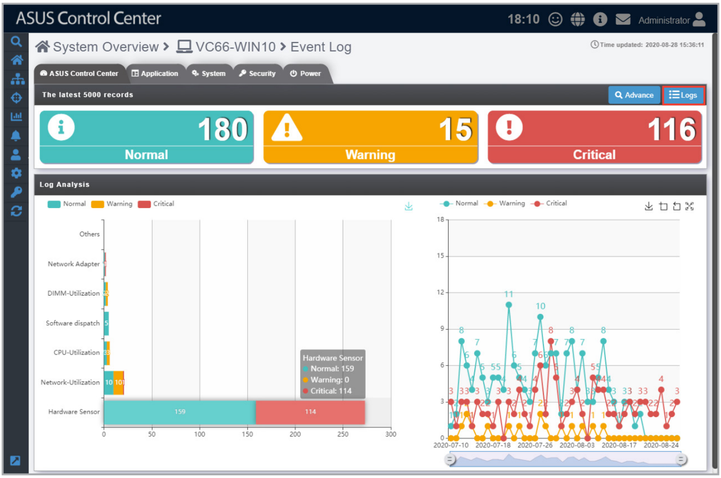


Level Type	Date & Time	Message
Normal	2019-10-24 04:46:26	CPU Core ID: 0 Utilization : 83 % Status : Warning --> Normal
Warning	2019-10-24 04:45:55	CPU Core ID: 0 Utilization : 90 % Status : Normal --> Warning
Normal	2019-10-24 04:39:08	CPU Core ID: 0 Utilization : 90 % Status : Warning --> Normal
Warning	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: 1 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

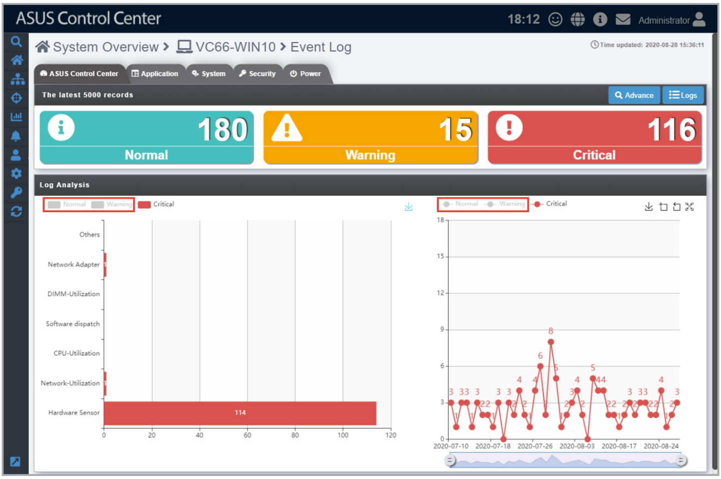
Switching to Log Analysis view

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.

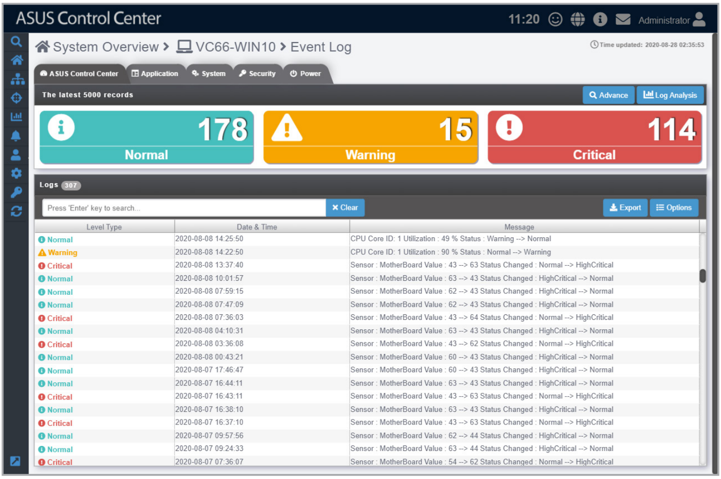
Click on **Logs** to switch back to the list view of the event log.



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

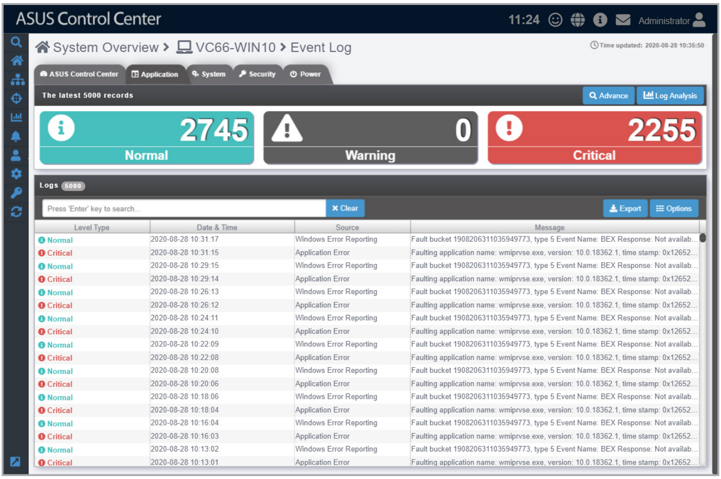


ASUS Control Center tab



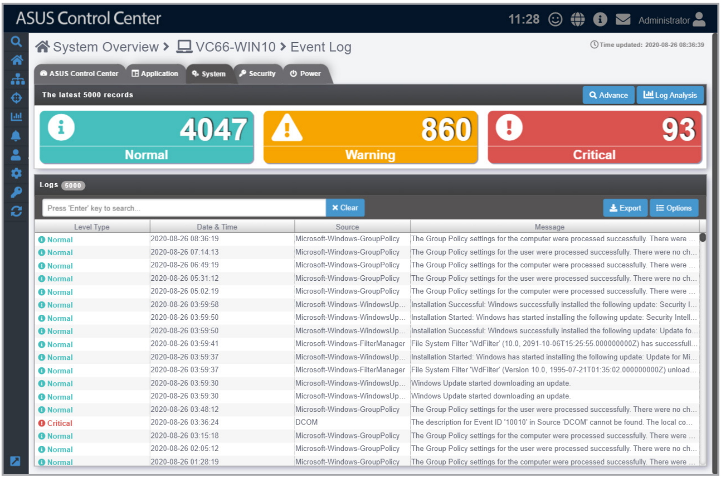
Level Type	Date & Time	Message
Normal	2020-08-08 14:25:50	CPU Core ID: 1 Utilization : 49 % Status : Warning --> Normal
Warning	2020-08-08 14:22:50	CPU Core ID: 1 Utilization : 90 % Status : Normal --> Warning
Critical	2020-08-08 13:37:40	Sensor : MotherBoard Value : 43 --> 63 Status Changed : Normal --> 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

Application tab (Windows only)



Level Type	Date & Time	Source	Message
Normal	2020-08-28 10:31:17	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:31:15	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:29:15	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:29:14	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:26:13	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:26:12	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:24:11	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:24:10	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:22:09	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:22:08	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:20:08	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:20:06	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:18:06	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:18:04	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:16:04	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:16:03	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...
Normal	2020-08-28 10:13:02	Windows Error Reporting	Fault bucket 1908206311035949773, type 5 Event Name: BEX Response: Not availab...
Critical	2020-08-28 10:13:01	Application Error	Faulting application name: wmiprvse.exe, version: 10.0.18362.1, time stamp: 0x12652...

System tab (Windows only)



System Overview > VC66-WIN10 > Event Log

Time updated: 2020-08-26 08:36:39

The latest 5000 records

4047 Normal

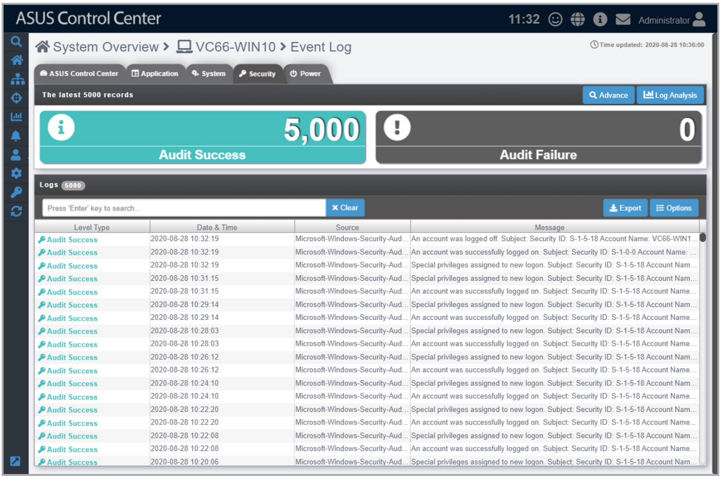
860 Warning

93 Critical

Logs 5000

Level Type	Date & Time	Source	Message
Normal	2020-08-26 08:36:19	Microsoft-Windows-GroupPolicy	The Group Policy settings for the computer were processed successfully. There were ...
Normal	2020-08-26 07:14:13	Microsoft-Windows-GroupPolicy	The Group Policy settings for the user were processed successfully. There were no ch...
Normal	2020-08-26 06:49:19	Microsoft-Windows-GroupPolicy	The Group Policy settings for the computer were processed successfully. There were ...
Normal	2020-08-26 05:31:12	Microsoft-Windows-GroupPolicy	The Group Policy settings for the user were processed successfully. There were no ch...
Normal	2020-08-26 05:02:19	Microsoft-Windows-GroupPolicy	The Group Policy settings for the computer were processed successfully. There were ...
Normal	2020-08-26 03:59:58	Microsoft-Windows-WindowsUp...	Installation Successful: Windows successfully installed the following update: Security I...
Normal	2020-08-26 03:59:50	Microsoft-Windows-WindowsUp...	Installation Started: Windows has started installing the following update: Security Intell...
Normal	2020-08-26 03:59:50	Microsoft-Windows-WindowsUp...	Installation Successful: Windows successfully installed the following update: Update fo...
Normal	2020-08-26 03:59:41	Microsoft-Windows-FilterManager	File System Filter 'WdFilter' (10.0, 2091-10-06T15:25:55.000000000Z) has successfull...
Normal	2020-08-26 03:59:37	Microsoft-Windows-WindowsUp...	Installation Started: Windows has started installing the following update: Update for Mi...
Normal	2020-08-26 03:59:37	Microsoft-Windows-FilterManager	File System Filter 'WdFilter' (Version 10.0, 1995-07-21T01:35:02.000000000Z) unload...
Normal	2020-08-26 03:59:30	Microsoft-Windows-WindowsUp...	Windows Update started downloading an update.
Normal	2020-08-26 03:59:30	Microsoft-Windows-WindowsUp...	Windows Update started downloading an update.
Normal	2020-08-26 03:48:12	Microsoft-Windows-GroupPolicy	The Group Policy settings for the user were processed successfully. There were no ch...
Critical	2020-08-26 03:36:24	DCOM	The description for Event ID '10010' in Source 'DCOM' cannot be found. The local co...
Normal	2020-08-26 03:15:18	Microsoft-Windows-GroupPolicy	The Group Policy settings for the computer were processed successfully. There were ...
Normal	2020-08-26 02:05:12	Microsoft-Windows-GroupPolicy	The Group Policy settings for the user were processed successfully. There were no ch...
Normal	2020-08-26 01:28:19	Microsoft-Windows-GroupPolicy	The Group Policy settings for the computer were processed successfully. There were ...

Security tab (Windows only)



System Overview > VC66-WIN10 > Event Log

Time updated: 2020-08-28 10:36:00

The latest 5000 records

5,000 Audit Success

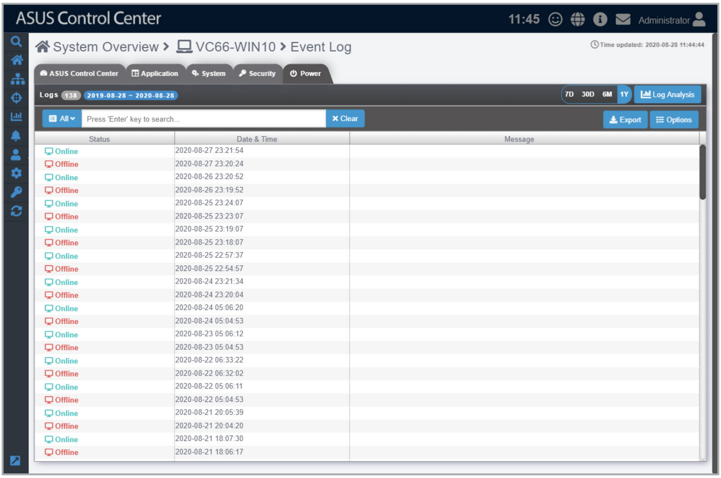
0 Audit Failure

Logs 5000

Level Type	Date & Time	Source	Message
Audit Success	2020-08-28 10:32:19	Microsoft-Windows-Security-Aud...	An account was logged off. Subject: Security ID: S-1-5-18 Account Name: VC66-WIN1...
Audit Success	2020-08-28 10:32:19	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: ...
Audit Success	2020-08-28 10:32:19	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:31:15	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:31:15	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:29:14	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:29:14	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:28:03	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:28:03	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:26:12	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:26:12	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:24:10	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:24:10	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:22:20	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:22:20	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:22:08	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...
Audit Success	2020-08-28 10:22:08	Microsoft-Windows-Security-Aud...	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name...
Audit Success	2020-08-28 10:20:06	Microsoft-Windows-Security-Aud...	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Nam...

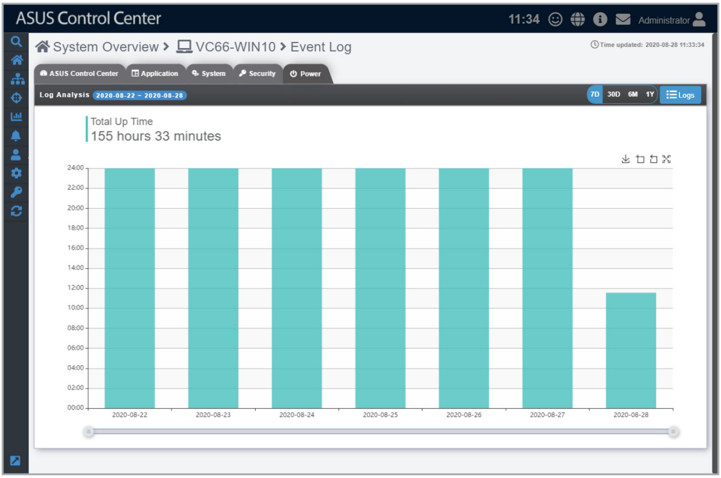
Power tab (Windows only)

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.

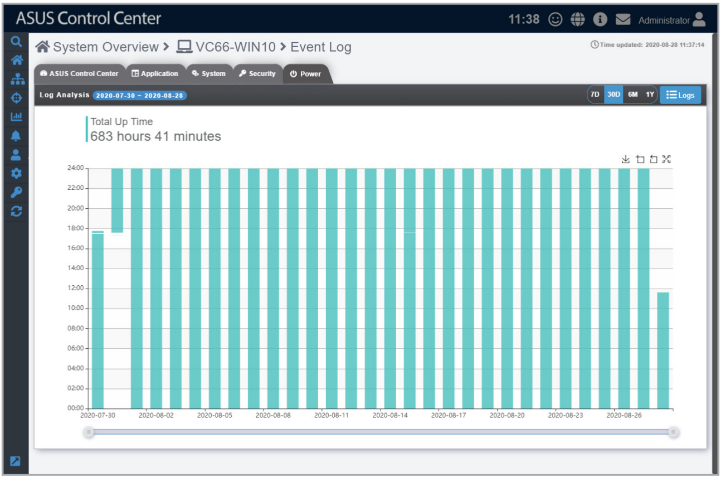

ASUS Control Center
11:45
Administrator
System Overview > VC66-WIN10 > Event Log
Time updated: 2020-08-28 11:44:44
ASUS Control Center
Application
System
Security
Power
Logs 138 2019-08-28 ~ 2020-08-28
7D 30D 6M 1Y
Log Analysis
All
Press 'Enter' key to search...
Clear
Export
Options

Status	Date & Time	Message
Online	2020-08-27 23:21:54	
Offline	2020-08-27 23:20:24	
Online	2020-08-26 23:20:52	
Offline	2020-08-26 23:19:52	
Online	2020-08-25 23:24:07	
Offline	2020-08-25 23:23:07	
Online	2020-08-25 23:19:07	
Offline	2020-08-25 23:18:07	
Online	2020-08-25 22:57:37	
Offline	2020-08-25 22:54:57	
Online	2020-08-24 23:21:34	
Offline	2020-08-24 23:20:04	
Online	2020-08-24 05:06:20	
Offline	2020-08-24 05:04:53	
Online	2020-08-23 05:06:12	
Offline	2020-08-23 05:04:53	
Online	2020-08-22 06:33:22	
Offline	2020-08-22 06:32:02	
Online	2020-08-22 05:06:11	
Offline	2020-08-22 05:04:53	
Online	2020-08-21 20:05:39	
Offline	2020-08-21 20:04:20	
Online	2020-08-21 18:07:30	
Offline	2020-08-21 18:06:17	

7 Days (Log Analysis):

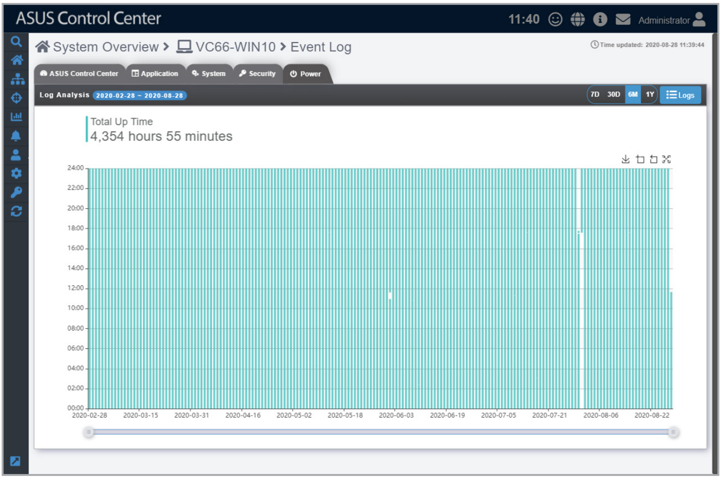


30 Days (Log Analysis):



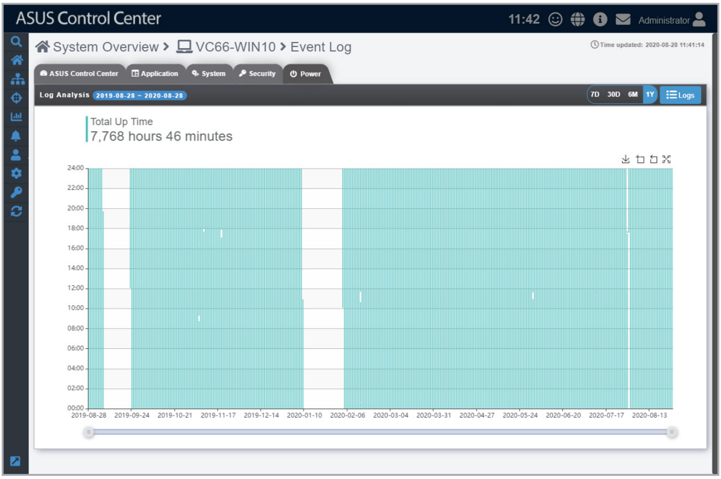
Total Up Time
683 hours 41 minutes

6 Months (Log Analysis):



Total Up Time
4,354 hours 55 minutes

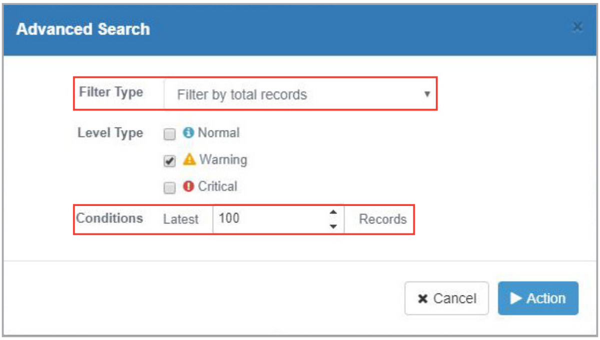
1 Year (Log Analysis):



Total Up Time
7,768 hours 46 minutes

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.



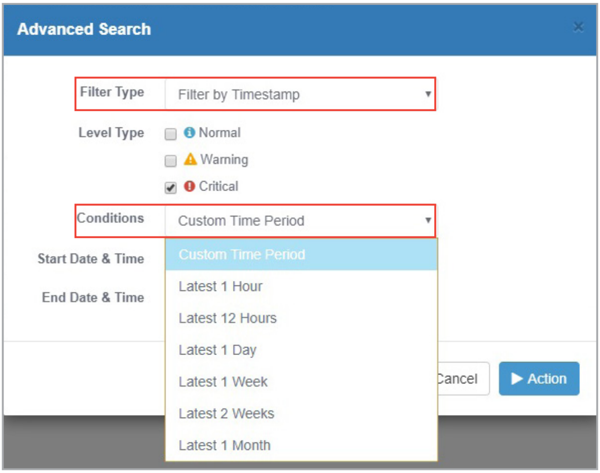
Advanced Search

Filter Type: Filter by total records

Level Type: □ Normal ☑ Warning □ Critical

Conditions: Latest 100 Records

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



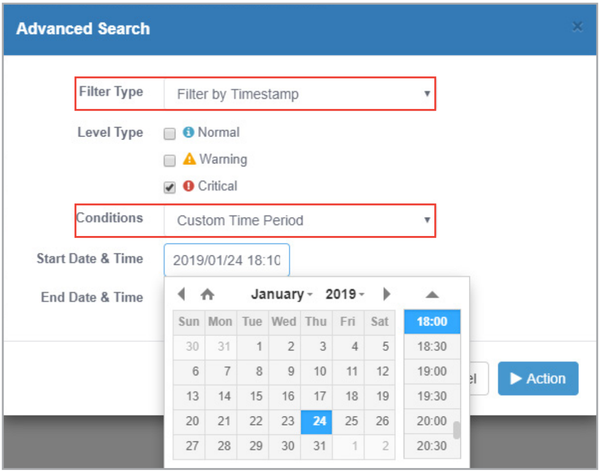
Advanced Search

Filter Type: Filter by Timestamp

Level Type: □ Normal □ Warning ☑ Critical

Conditions: Custom Time Period

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



Advanced Search

Filter Type: Filter by Timestamp

Level Type: □ Normal □ Warning ☑ Critical

Conditions: Custom Time Period

Start Date & Time: 2019/01/24 18:10

January 2019

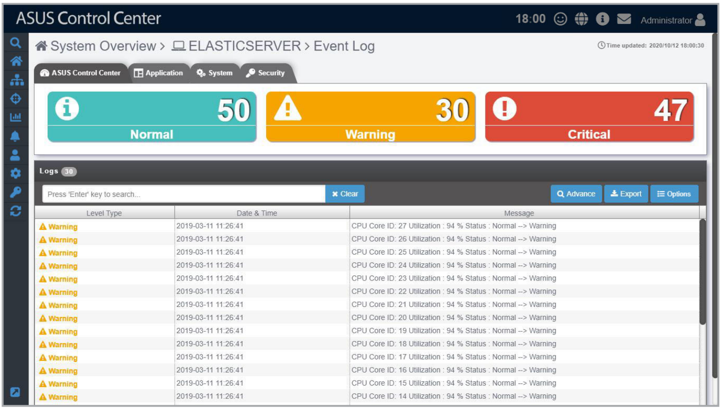
Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

18:00
18:30
19:00
19:30
20:00
20:30

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

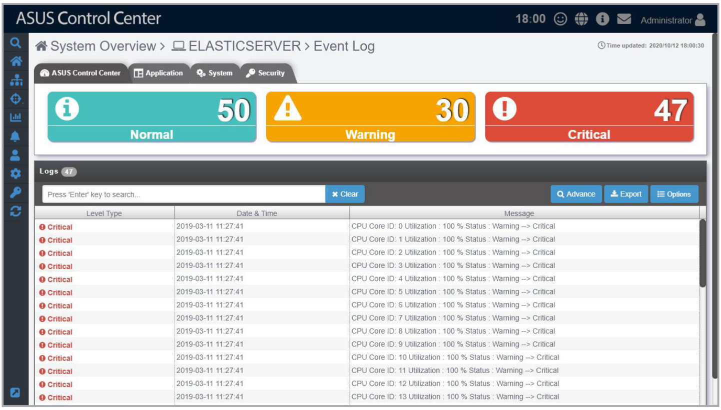
> This function will replace the Event Log list with the new results, and searching / filtering using the Search toolbar will only perform a search / filter on the new Event Log list.

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



Level Type	Date & Time	Message
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 27 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 26 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 25 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 24 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 23 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 22 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 21 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 20 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 19 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 18 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 17 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 16 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 15 Utilization : 94 % Status : Normal --> Warning
⚠ Warning	2019-03-11 11:26:41	CPU Core ID: 14 Utilization : 94 % Status : Normal --> Warning

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

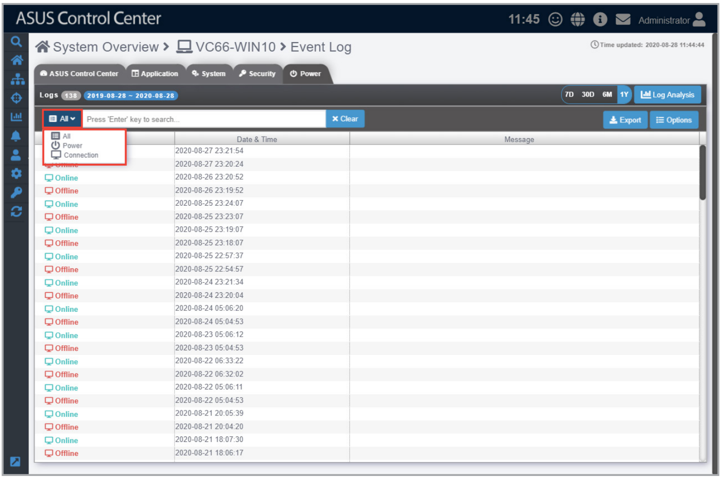


Level Type	Date & Time	Message
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 0 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 1 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 2 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 3 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 4 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 5 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 6 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 7 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 8 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 9 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 10 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 11 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 12 Utilization : 100 % Status : Warning --> Critical
❗ Critical	2019-03-11 11:27:41	CPU Core ID: 13 Utilization : 100 % Status : Warning --> Critical

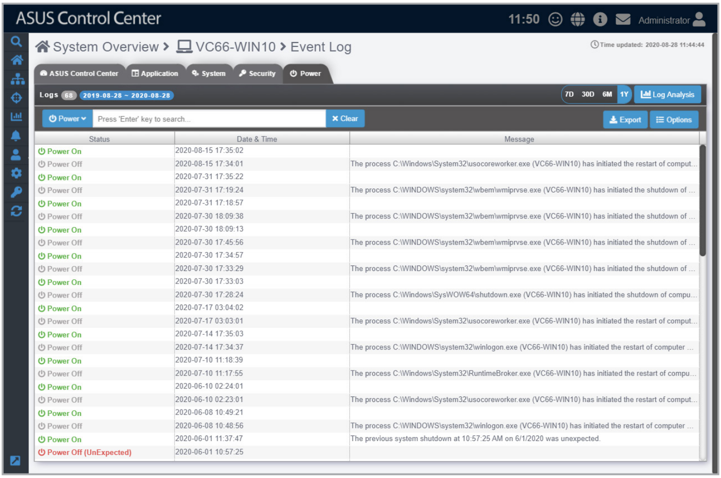
Filtering the Power event log

Click on ▤ All, then select the criteria to filter.

- 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.



	Date & Time	Message
	2020-08-27 23:21:54	
Offline	2020-08-27 23:20:24	
Online	2020-08-26 23:20:52	
Offline	2020-08-26 23:19:52	
Online	2020-08-25 23:24:07	
Offline	2020-08-25 23:23:07	
Online	2020-08-25 23:19:07	
Offline	2020-08-25 23:18:07	
Online	2020-08-25 22:57:37	
Offline	2020-08-25 22:54:57	
Online	2020-08-24 23:21:34	
Offline	2020-08-24 23:20:04	
Online	2020-08-24 05:06:20	
Offline	2020-08-24 05:04:53	
Online	2020-08-23 05:06:12	
Offline	2020-08-23 05:04:53	
Online	2020-08-22 06:33:22	
Offline	2020-08-22 06:32:02	
Online	2020-08-22 05:06:11	
Offline	2020-08-22 05:04:53	
Online	2020-08-21 20:05:39	
Offline	2020-08-21 20:04:20	
Online	2020-08-21 18:07:30	
Offline	2020-08-21 18:06:17	

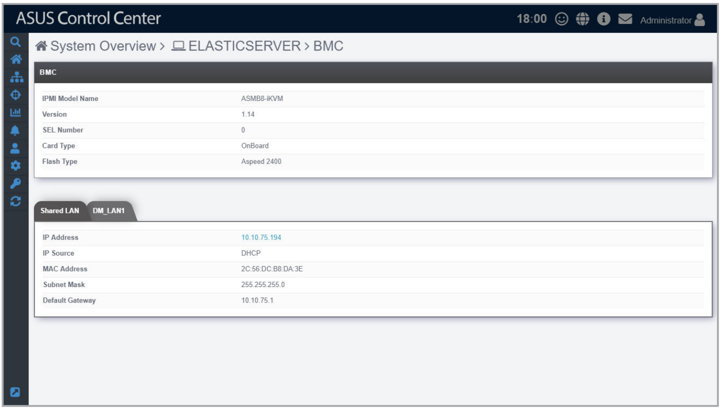


Status	Date & Time	Message
Power On	2020-08-15 17:35:02	
Power Off	2020-08-15 17:34:01	The process C:\Windows\System32\usocoreworker.exe (VC66-WIN10) has initiated the restart of comput...
Power On	2020-07-31 17:35:22	
Power Off	2020-07-31 17:19:24	The process C:\WINDOWS\system32\wbem\wmiprvse.exe (VC66-WIN10) has initiated the shutdown of ...
Power On	2020-07-31 17:18:57	
Power Off	2020-07-30 18:09:38	The process C:\WINDOWS\system32\wbem\wmiprvse.exe (VC66-WIN10) has initiated the shutdown of ...
Power On	2020-07-30 18:09:13	
Power Off	2020-07-30 17:45:56	The process C:\WINDOWS\system32\wbem\wmiprvse.exe (VC66-WIN10) has initiated the shutdown of ...
Power On	2020-07-30 17:34:57	
Power Off	2020-07-30 17:33:29	The process C:\WINDOWS\system32\wbem\wmiprvse.exe (VC66-WIN10) has initiated the shutdown of ...
Power On	2020-07-30 17:33:03	
Power Off	2020-07-30 17:28:24	The process C:\Windows\SysWOW64\shutdown.exe (VC66-WIN10) has initiated the shutdown of compu...
Power On	2020-07-17 03:04:02	
Power Off	2020-07-17 03:03:01	The process C:\Windows\System32\usocoreworker.exe (VC66-WIN10) has initiated the restart of comput...
Power On	2020-07-14 17:35:03	
Power Off	2020-07-14 17:34:37	The process C:\WINDOWS\system32\winlogon.exe (VC66-WIN10) has initiated the restart of computer ...
Power On	2020-07-10 11:18:39	
Power Off	2020-07-10 11:17:55	The process C:\Windows\System32\RuntimeBroker.exe (VC66-WIN10) has initiated the restart of compu...
Power On	2020-06-10 02:24:01	
Power Off	2020-06-10 02:23:01	The process C:\Windows\System32\usocoreworker.exe (VC66-WIN10) has initiated the restart of comput...
Power On	2020-06-08 10:49:21	
Power Off	2020-06-08 10:48:56	The process C:\WINDOWS\system32\winlogon.exe (VC66-WIN10) has initiated the restart of computer ...
Power On	2020-06-01 11:37:47	The previous system shutdown at 10:57:25 AM on 6/1/2020 was unexpected.
Power Off (UnExpected)	2020-06-01 10:57:25	

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.

- 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.



BMC

IPMI Model Name	ASMB8-iKVM
Version	1.14
SEL Number	0
Card Type	OnBoard
Flash Type	Aspeed 2400

IP Address	10.10.75.194
IP Source	DHCP
MAC Address	2C:56:DC:B8:DA:3E
Subnet Mask	255.255.255.0
Default Gateway	10.10.75.1

Shared LAN

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

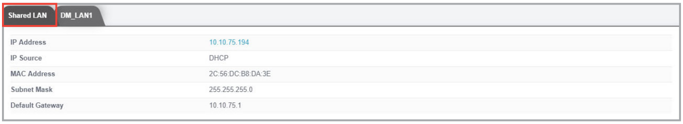
BMC is required to use this item.

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

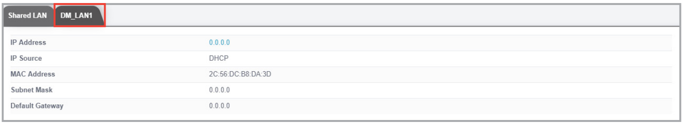
To edit BMC settings using ASMB on the device:

1. Select **Share Lan**



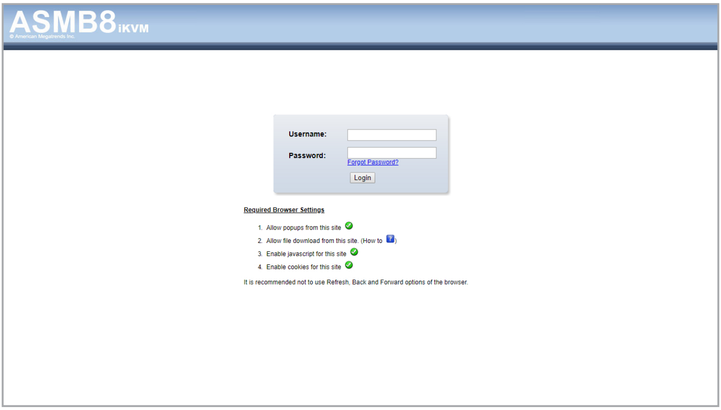
IP Address	10.10.75.194
IP Source	DHCP
MAC Address	2C:56:DC:B8:DA:3E
Subnet Mask	255.255.255.0
Default Gateway	10.10.75.1

or **DM_LAN1** tab, then click the IP Address.



IP Address	0.0.0.0
IP Source	DHCP
MAC Address	2C:56:DC:B8:DA:3D
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0

2. Login ASMB.



Required Browser Settings

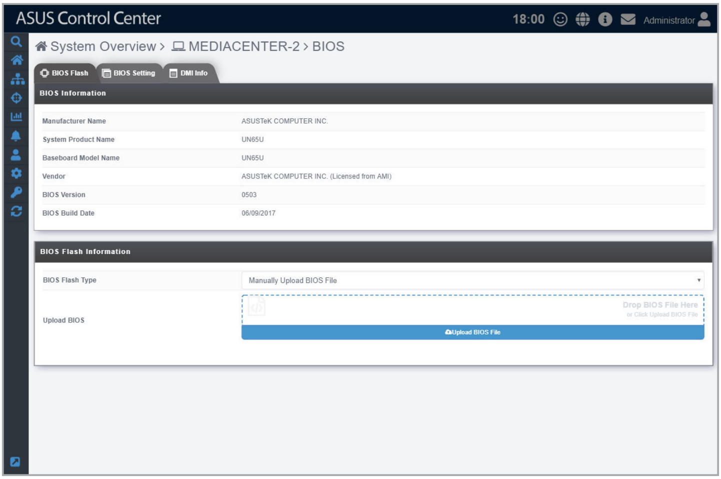
1. Allow popups from this site ✓
2. Allow file download from this site. (How to ?)
3. Enable javascript for this site ✓
4. Enable cookies for this site ✓

It is recommended not to use Refresh, Back and Forward options of the browser.

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.

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



BIOS Information

Manufacturer Name	ASUSTeK COMPUTER INC.
System Product Name	UN65U
Baseboard Model Name	UN65U
Vendor	ASUSTeK COMPUTER INC. (Licensed from AMI)
BIOS Version	0503
BIOS Build Date	06/09/2017

BIOS Flash Information

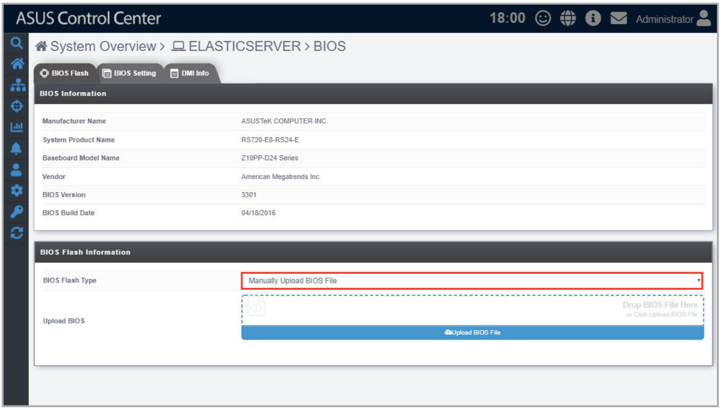
BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	

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.

> 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.



BIOS Information

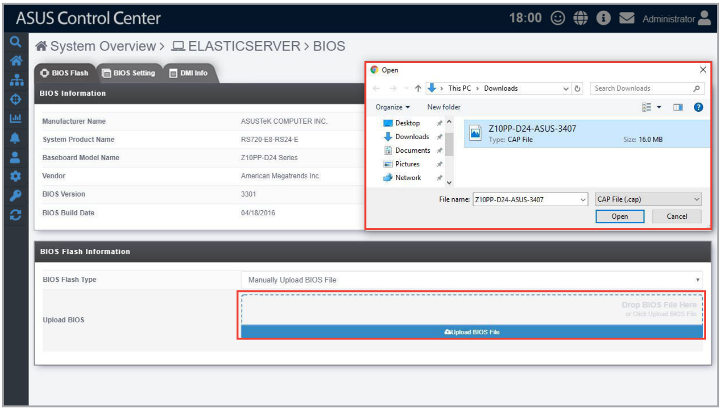
Manufacturer Name	ASUSTeK COMPUTER INC.
System Product Name	RS720-E8-RS24-E
Baseboard Model Name	Z10PP-D24 Series
Vendor	American Megatrends Inc.
BIOS Version	3301
BIOS Build Date	04/18/2016

BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	

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

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



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

Z10PP-D24-ASUS-3407
Type: CAP File
Size: 16.0 MB

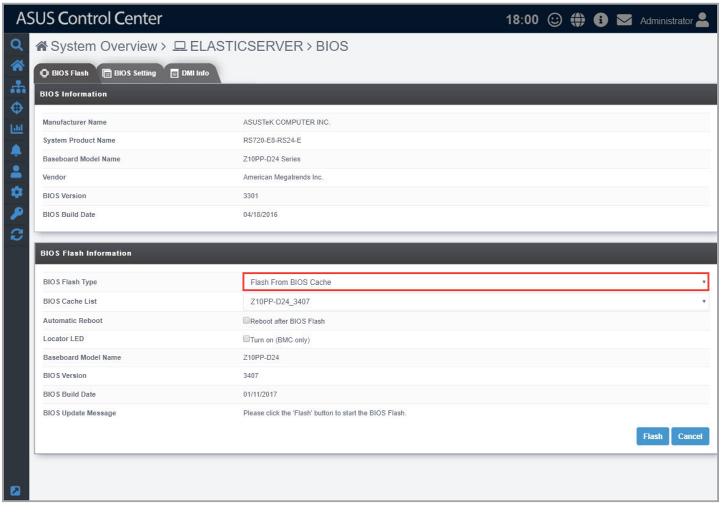
File name: Z10PP-D24-ASUS-3407
CAP File (.cap)

BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	

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

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



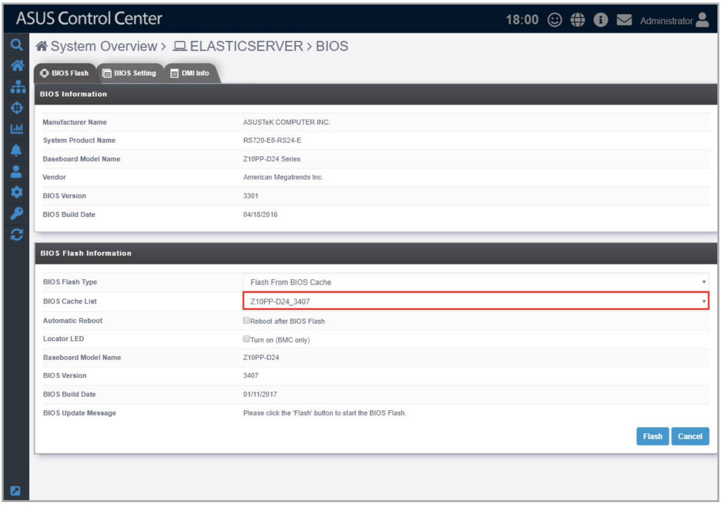
BIOS Information

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	Flash From BIOS Cache
BIOS Cache List	Z10PP-D24_3407
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.

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



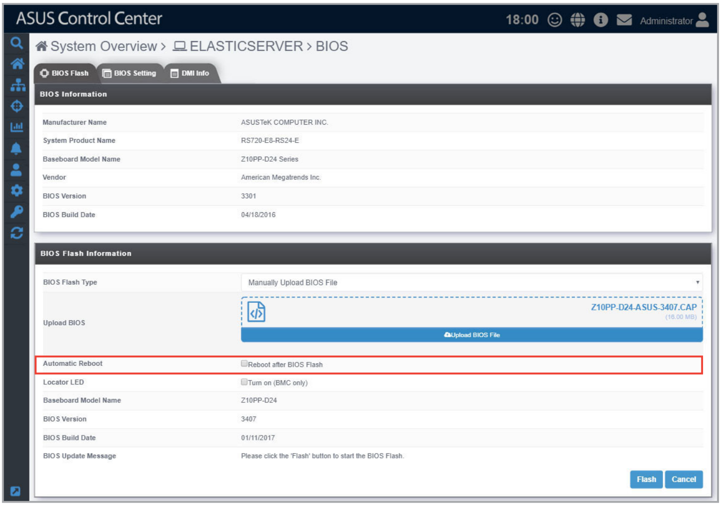
BIOS Information

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	Flash From BIOS Cache
BIOS Cache List	Z10PP-D24_3407
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.

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.



BIOS Information

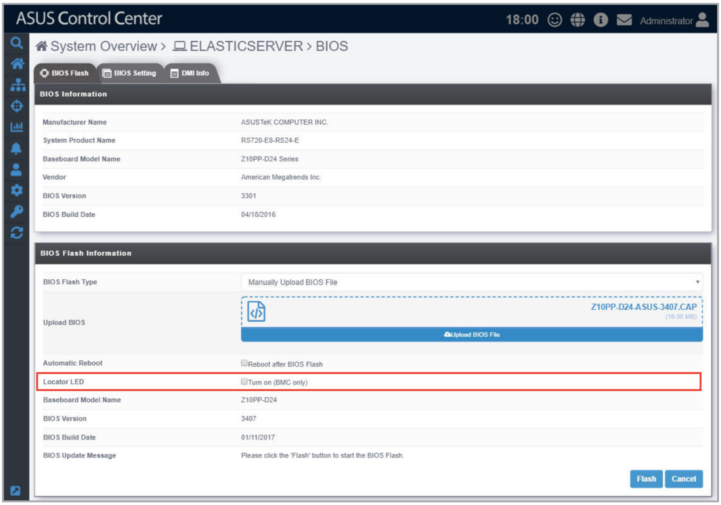
Manufacturer Name	ASUSTeK COMPUTER INC.
System Product Name	RS720-E8-RS24-E
Baseboard Model Name	Z10PP-D24 Series
Vendor	American Megatrends Inc.
BIOS Version	3301
BIOS Build Date	04/18/2016

BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	Z10PP-D24-ASUS-3407.CAP (16.00 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.

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.

BMC is required for this option to work properly.



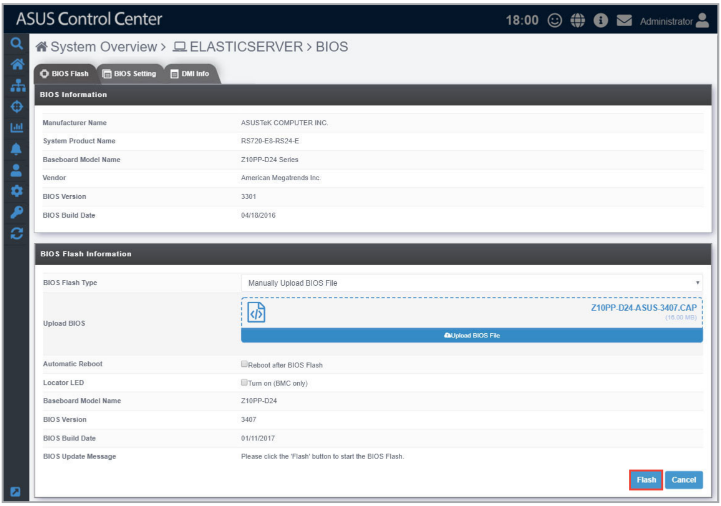
BIOS Information

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 (16.00 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.

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

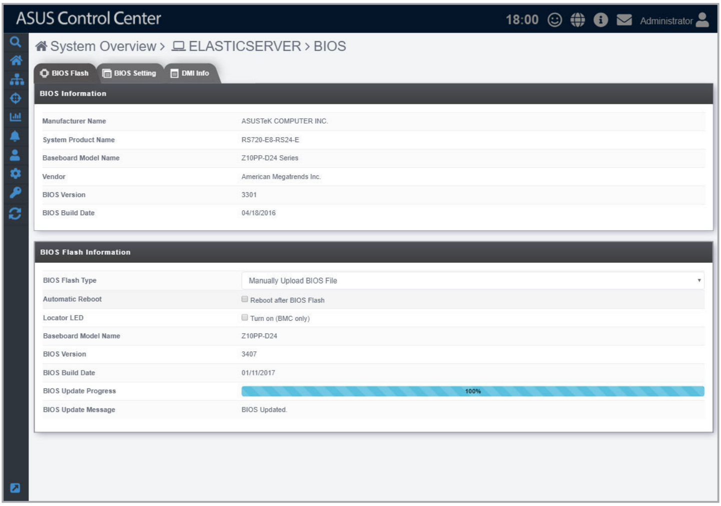


BIOS Information

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 (16.00 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.



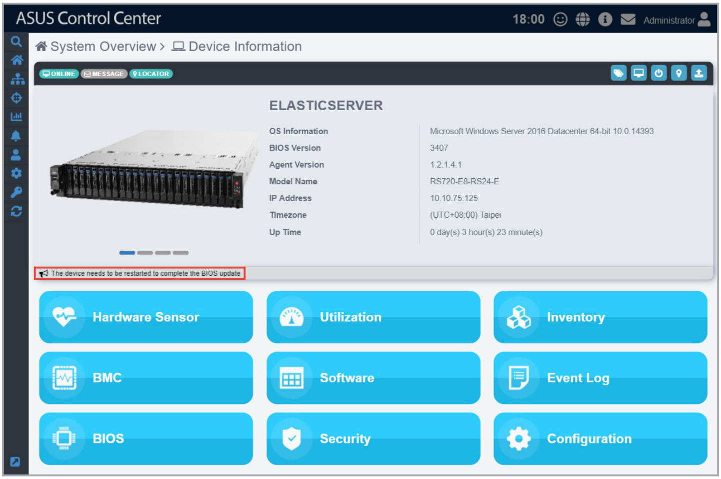
BIOS Information

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
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.

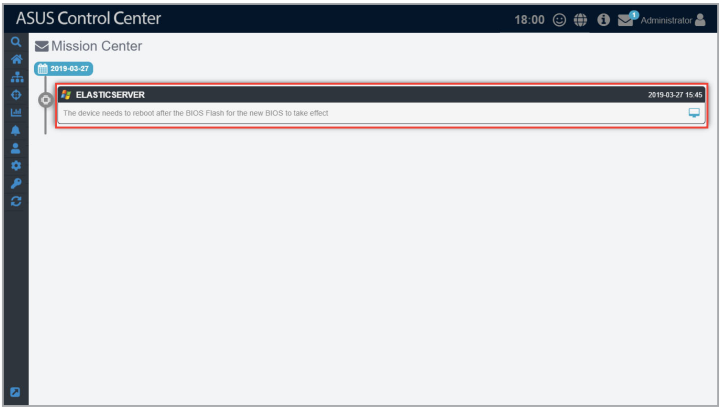
5. Once the BIOS flash has been completed, a pop-up window will appear, prompting you to reboot the system, click **OK**. You can also view this message in the **Device Information** screen and **Mission Center**.



ELASTICSERVER

OS Information	Microsoft Windows Server 2016 Datacenter 64-bit 10.0.14393
BIOS Version	3407
Agent Version	1.2.1.4.1
Model Name	RS720-E8-RS24-E
IP Address	10.10.75.125
Timezone	(UTC+08:00) Taipei
Up Time	0 day(s) 3 hour(s) 23 minute(s)

The device needs to be restarted to complete the BIOS update



ELASTICSERVER 2019-03-27 15:45

The device needs to reboot after the BIOS Flash for the new BIOS to take effect

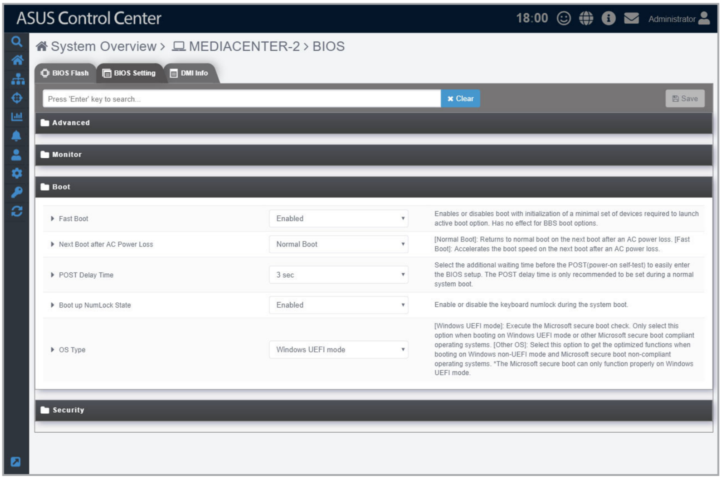
6. Reboot the device to complete the BIOS flash.

BIOS Setting

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.

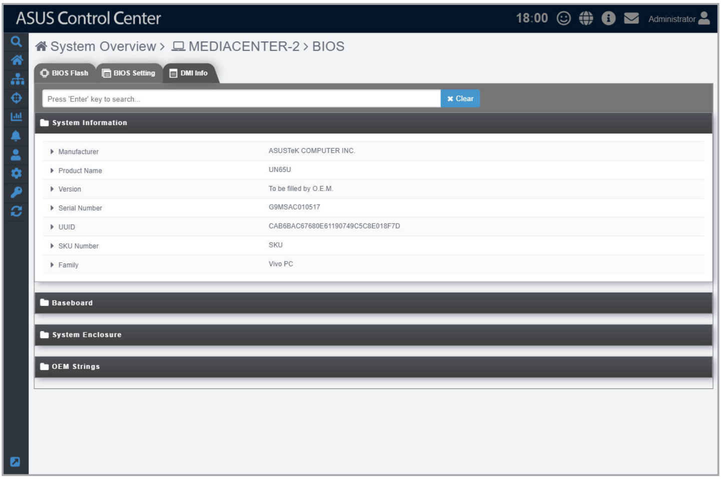
The BIOS settings may differ between devices. Please refer to the device's motherboard user manual for more information about the BIOS settings.



Fast Boot	Enabled	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
Next Boot after AC Power Loss	Normal Boot	[Normal Boot]: Returns to normal boot on the next boot after an AC power loss. [Fast Boot]: Accelerates the boot speed on the next boot after an AC power loss.
POST Delay Time	3 sec	Select the additional waiting time before the POST(power-on self-test) to easily enter the BIOS setup. The POST delay time is only recommended to be set during a normal system boot.
Boot up NumLock State	Enabled	Enable or disable the keyboard numlock during the system boot.
OS Type	Windows UEFI mode	[Windows UEFI mode]: Execute the Microsoft secure boot check. Only select this option when booting on Windows UEFI mode or other Microsoft secure boot compliant operating systems. [Other OS]: Select this option to get the optimized functions when booting on Windows non-UEFI mode and Microsoft secure boot non-compliant operating systems. *The Microsoft secure boot can only function properly on Windows UEFI mode.

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.



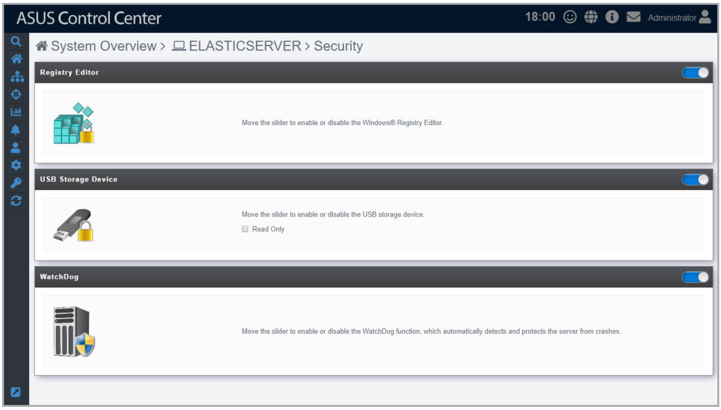
Manufacturer	ASUSTeK COMPUTER INC.
Product Name	UN65U
Version	To be filled by O.E.M.
Serial Number	G9MSAC010517
UUID	CAB6BAC67680E61190749C5C8E018F7D
SKU Number	SKU
Family	Vivo PC

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.

Linux systems only supports **Watchdog**.

For Windows® system:



ASUS Control Center

18:00 Administrator

System Overview > ELASTICSERVER > Security

Registry Editor

Move the slider to enable or disable the Windows® Registry Editor.

USB Storage Device

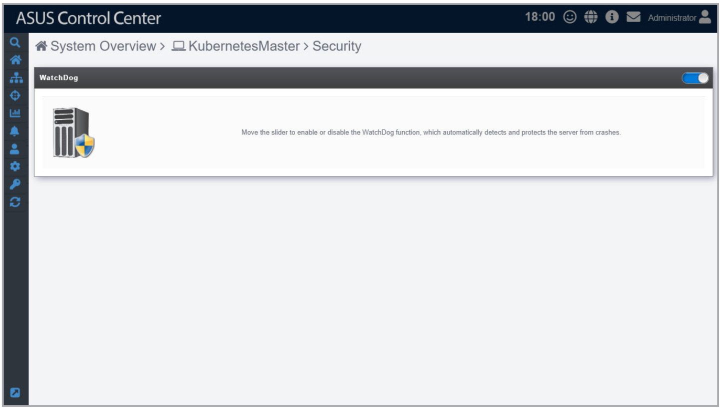
Move the slider to enable or disable the USB storage device.

□ Read Only

WatchDog

Move the slider to enable or disable the WatchDog function, which automatically detects and protects the server from crashes.

For Linux system:



ASUS Control Center

18:00 Administrator

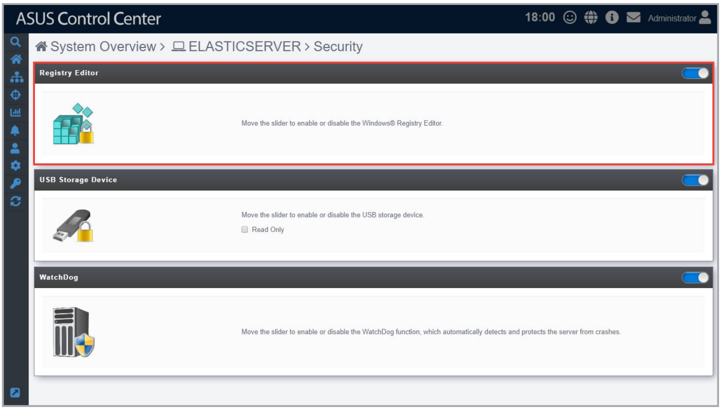
System Overview > KubernetesMaster > Security

WatchDog

Move the slider to enable or disable the WatchDog function, which automatically detects and protects the server from crashes.

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**.



Registry Editor

Move the slider to enable or disable the Windows® Registry Editor.

USB Storage Device

Move the slider to enable or disable the USB storage device.

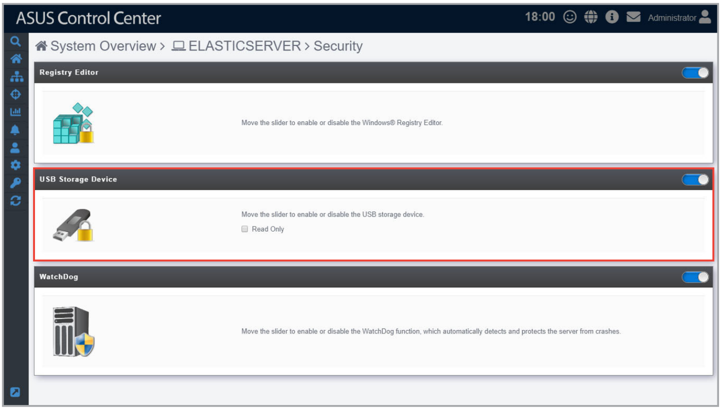
□ Read Only

WatchDog

Move the slider to enable or disable the WatchDog function, which automatically detects and protects the server from crashes.

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**.



Registry Editor

Move the slider to enable or disable the Windows® Registry Editor.

USB Storage Device

Move the slider to enable or disable the USB storage device.

□ Read Only

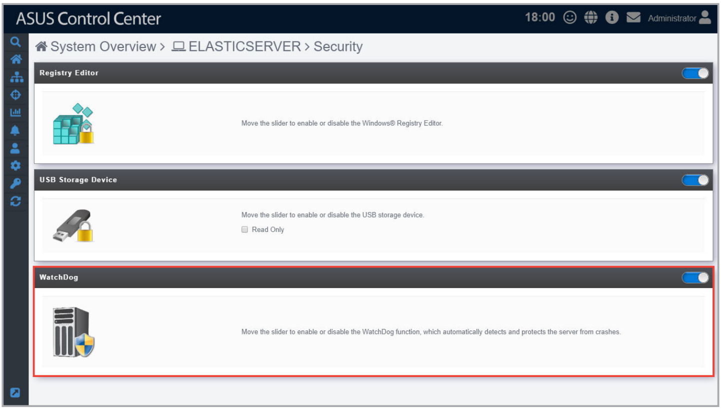
WatchDog

Move the slider to enable or disable the WatchDog function, which automatically detects and protects the server from crashes.

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**.

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**.



Move the slider to enable or disable the Windows® Registry Editor.

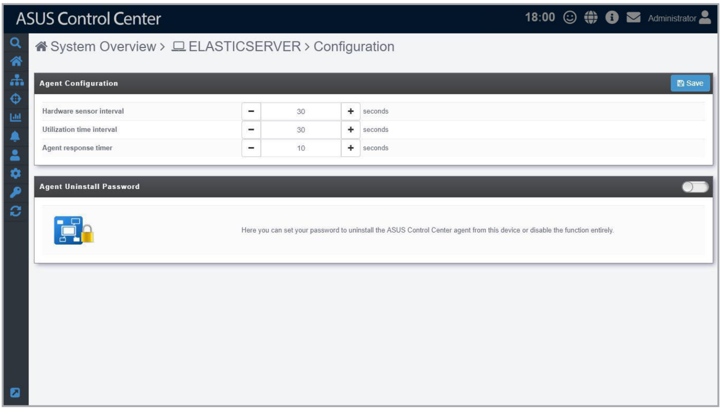
Move the slider to enable or disable the USB storage device.

□ Read Only

Move the slider to enable or disable the WatchDog function, which automatically detects and protects the server from crashes.

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

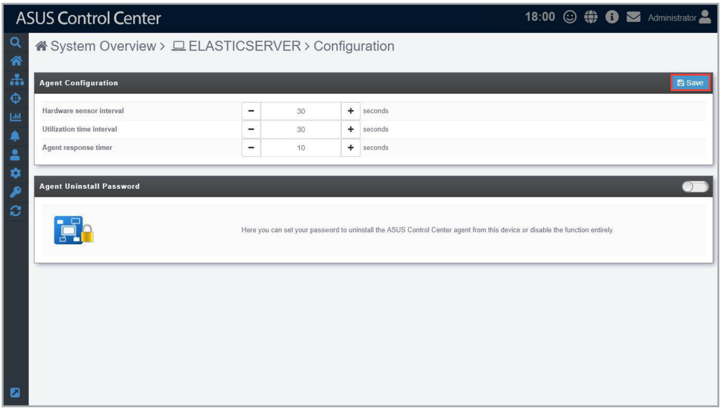
Hardware sensor interval	−	30	+	seconds
Utilization time interval	−	30	+	seconds
Agent response timer	−	10	+	seconds

Agent Uninstall Password

Here you can set your password to uninstall the ASUS Control Center agent from this device or disable the function entirely.

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.



Agent Configuration

Hardware sensor interval − 30 + seconds
Utilization time interval − 30 + seconds
Agent response timer − 10 + seconds

Agent Uninstall Password

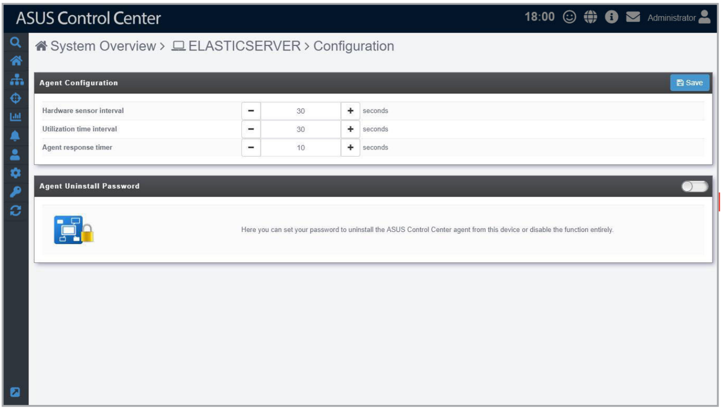
Here you can set your password to uninstall the ASUS Control Center agent from this device or disable the function entirely.

Hardware sensor interval	Interval in seconds at which the hardware sensor information is sent to the ASUS Control Center server. 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.
Utilization time interval	Interval in seconds at which the utilization information is sent to the ASUS Control Center server. 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.
Agent response timer	Interval in seconds at which the agent will query the ASUS Control Center server for task updates. 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.

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.



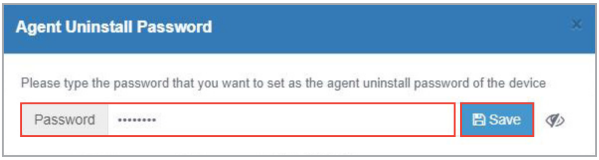
Agent Configuration

Hardware sensor interval	−	30 +	seconds
Utilization time interval	−	30 +	seconds
Agent response timer	−	10 +	seconds

Agent Uninstall Password

Here you can set your password to uninstall the ASUS Control Center agent from this device or disable the function entirely.

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

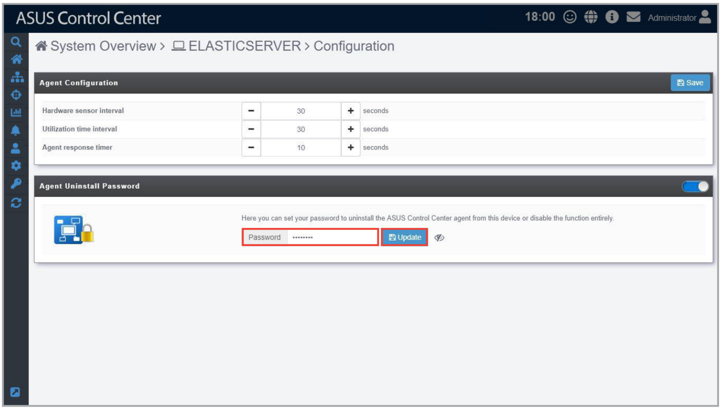


Agent Uninstall Password

Please type the password that you want to set as the agent uninstall password of the device

Password ••••••••

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



Agent Configuration

Hardware sensor interval	−	30 +	seconds
Utilization time interval	−	30 +	seconds
Agent response timer	−	10 +	seconds

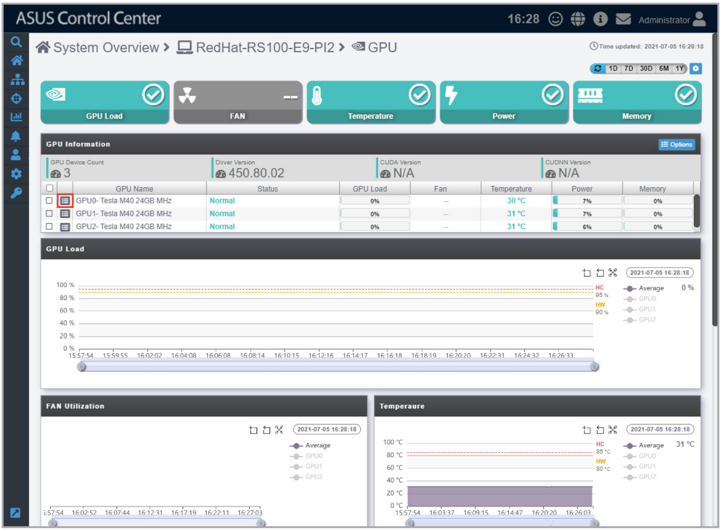
Agent Uninstall Password

Here you can set your password to uninstall the ASUS Control Center agent from this device or disable the function entirely.

Password ••••••••

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.



ASUS Control Center 16:28 Administrator

System Overview > RedHat-RS100-E9-PI2 > GPU

Time updated: 2021-07-05 16:28:18

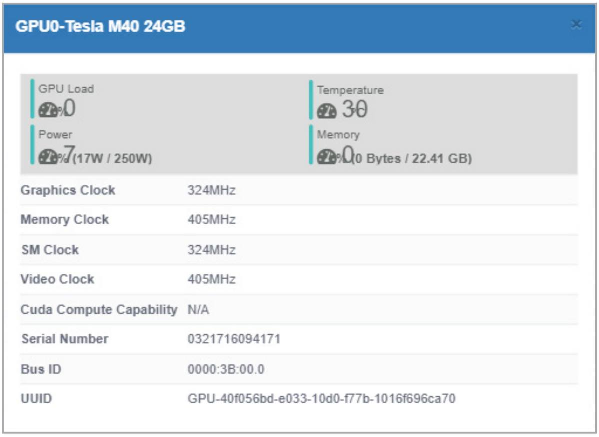
1D 7D 30D 6M 1Y

GPU Load ✓ | FAN -- | Temperature ✓ | Power ✓ | Memory ✓

GPU Information

GPU Device Count: 3
Dirver Version: 450.80.02
CUDA Version: N/A
CUDNN Version: N/A

□		GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□	☰	GPU0- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□	☰	GPU1- Tesla M40 24GB MHz	Normal	0%	--	31 °C	7%	0%
□	☰	GPU2- Tesla M40 24GB MHz	Normal	0%	--	31 °C	6%	0%



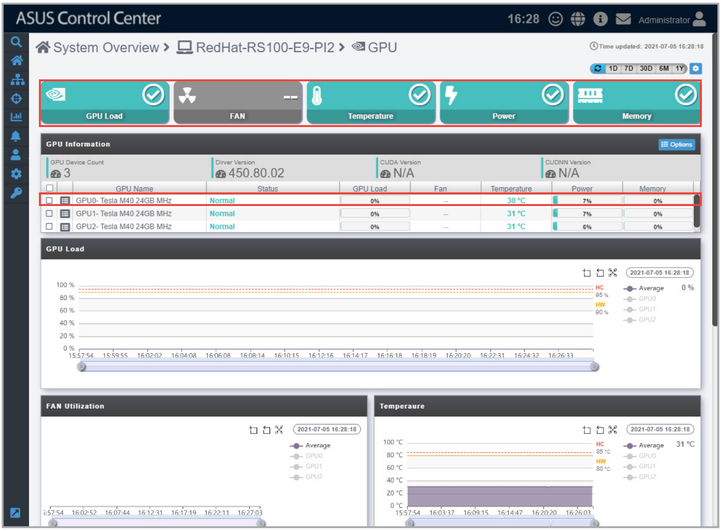
GPU0-Tesla M40 24GB

GPU Load: 0
Temperature: 30
Power: 7 (17W / 250W)
Memory: 0 (0 Bytes / 22.41 GB)

Graphics Clock	324MHz
Memory Clock	405MHz
SM Clock	324MHz
Video Clock	405MHz
Cuda Compute Capability	N/A
Serial Number	0321716094171
Bus ID	0000:3B:00.0
UUID	GPU-40f056bd-e033-10d0-f77b-1016f696ca70

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



GPU Device Count: 3

Dirver Version: 450.80.02

CUDA Version: N/A

CUDNN Version: N/A

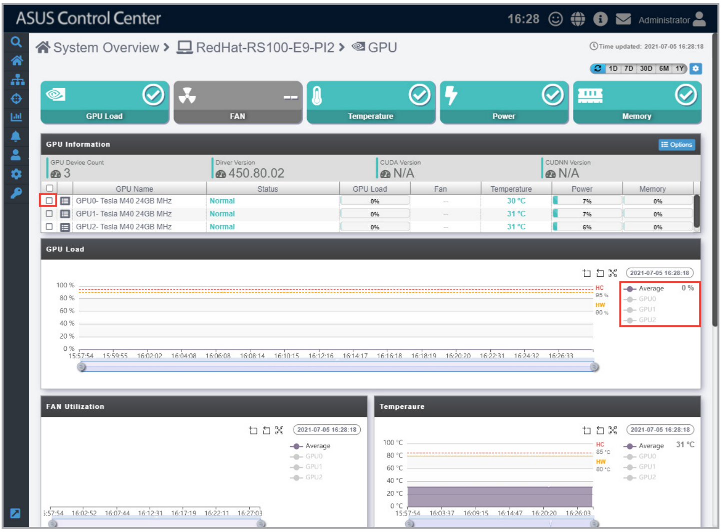
□		GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□		GPU0- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□		GPU1- Tesla M40 24GB MHz	Normal	0%	--	31 °C	7%	0%
□		GPU2- Tesla M40 24GB MHz	Normal	0%	--	31 °C	6%	0%

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.

> 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.



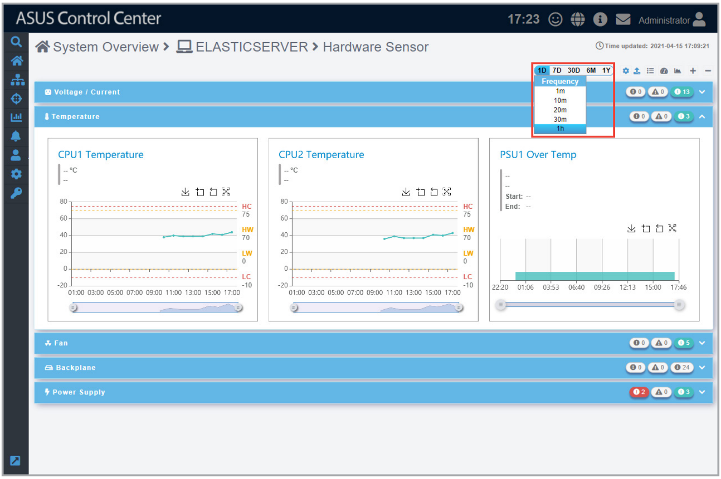
GPU Device Count 3 | Dirver Version 450.80.02 | CUDA Version N/A | CUDNN Version N/A

☐	GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
☐	GPU0- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
☐	GPU1- Tesla M40 24GB MHz	Normal	0%	--	31 °C	7%	0%
☐	GPU2- Tesla M40 24GB MHz	Normal	0%	--	31 °C	6%	0%

Chart Quick Buttons

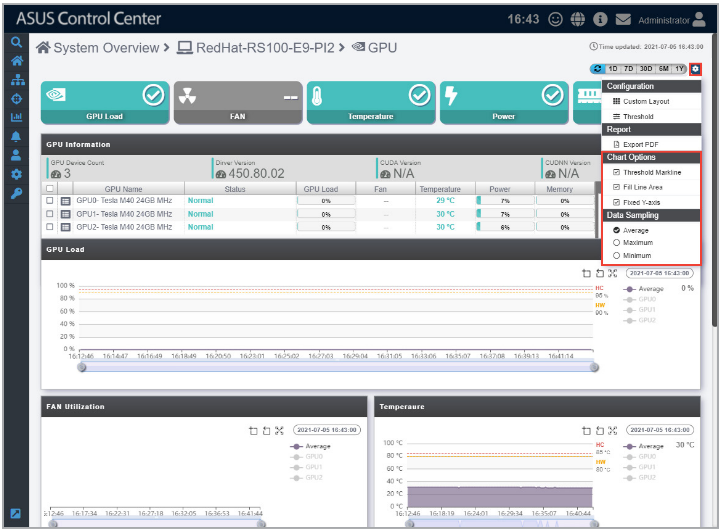
⬚	Click to zoom in on the timeline of the chart.
⬚	Click to zoom out on the timeline of the chart.
⤧	Click to restore the chart to its default view.

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.



GPU Device Count 3

Dirver Version 450.80.02

CUDA Version N/A

CUDNN Version N/A

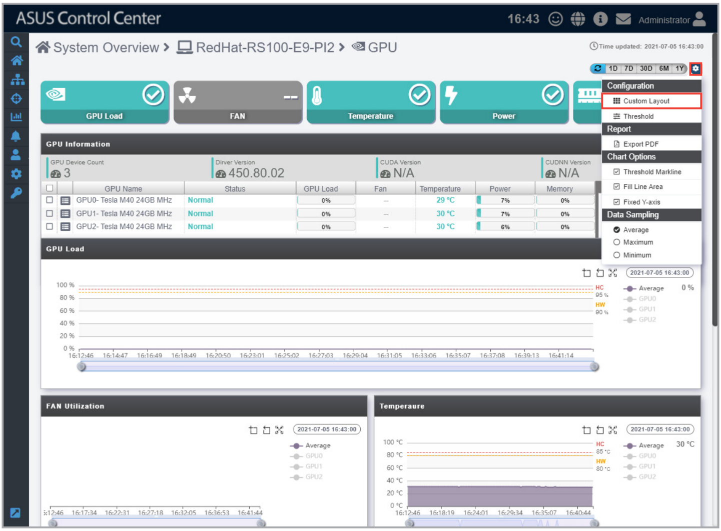
□		GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□		GPU0- Tesla M40 24GB MHz	Normal	0%	--	29 °C	7%	0%
□		GPU1- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□		GPU2- Tesla M40 24GB MHz	Normal	0%	--	30 °C	6%	0%

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



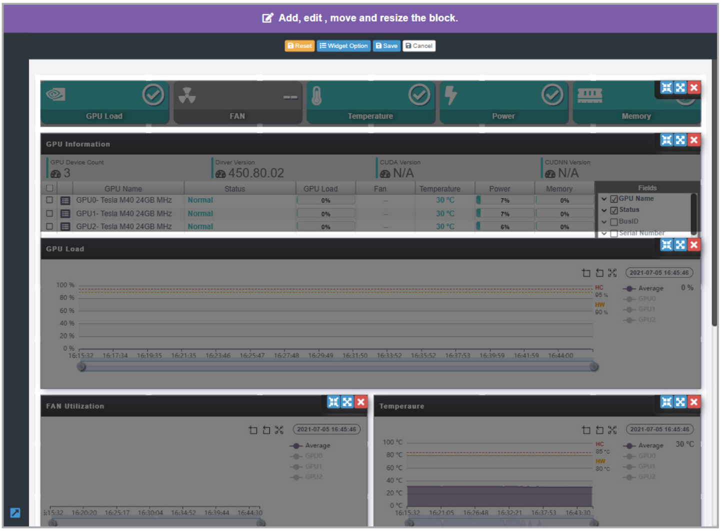
GPU Information

GPU Device Count 3 · Dirver Version 450.80.02 · CUDA Version N/A · CUDNN Version N/A

□	GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□	GPU0- Tesla M40 24GB MHz	Normal	0%	--	29 °C	7%	0%
□	GPU1- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□	GPU2- Tesla M40 24GB MHz	Normal	0%	--	30 °C	6%	0%

☑ Threshold Markline ☑ Fill Line Area ☑ Fixed Y-axis · Data Sampling: ● Average ○ Maximum ○ Minimum

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.



GPU Information

GPU Device Count 3 · Dirver Version 450.80.02 · CUDA Version N/A · CUDNN Version N/A

□	GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□	GPU0- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□	GPU1- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□	GPU2- Tesla M40 24GB MHz	Normal	0%	--	30 °C	6%	0%

Fields: ☑ GPU Name ☑ Status □ BusID □ Serial Number

- **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:**

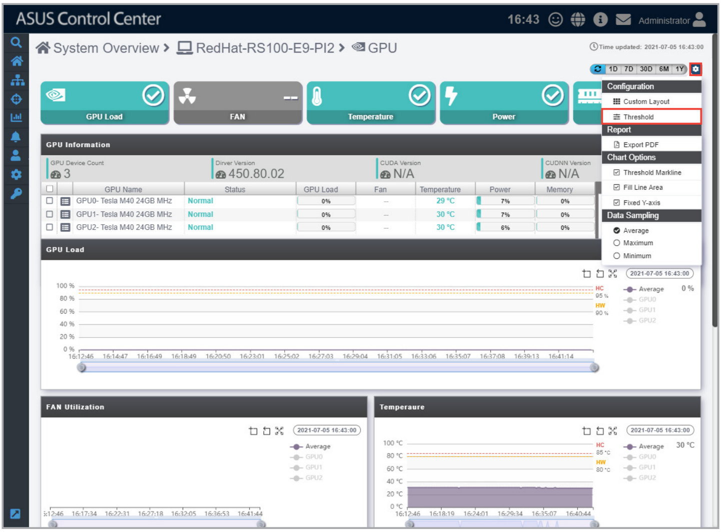
  Click on Reset to reset the GPU page to its default layout.

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**.



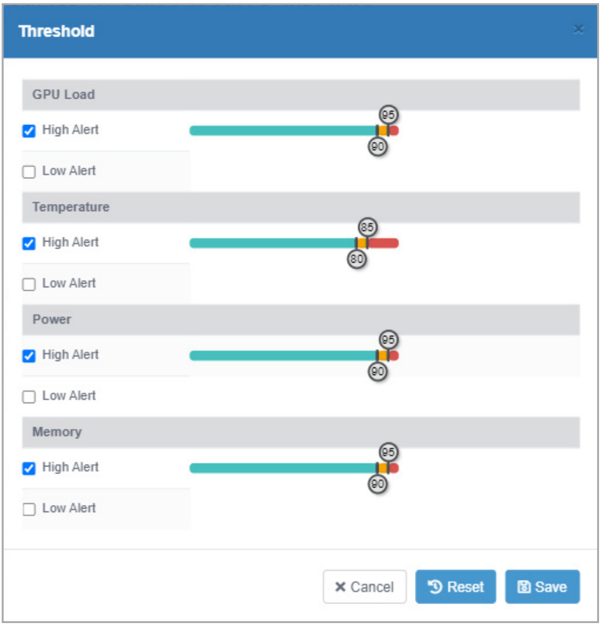
GPU Information

GPU Device Count 3 | Dirver Version 450.80.02 | CUDA Version N/A | CUDNN Version N/A

□		GPU Name	Status	GPU Load	Fan	Temperature	Power	Memory
□		GPU0- Tesla M40 24GB MHz	Normal	0%	--	29 °C	7%	0%
□		GPU1- Tesla M40 24GB MHz	Normal	0%	--	30 °C	7%	0%
□		GPU2- Tesla M40 24GB MHz	Normal	0%	--	30 °C	6%	0%

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**.

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



Threshold

GPU Load

☑ High Alert 90 95

□ Low Alert

Temperature

☑ High Alert 80 85

□ Low Alert

Power

☑ High Alert 90 95

□ Low Alert

Memory

☑ High Alert 90 95

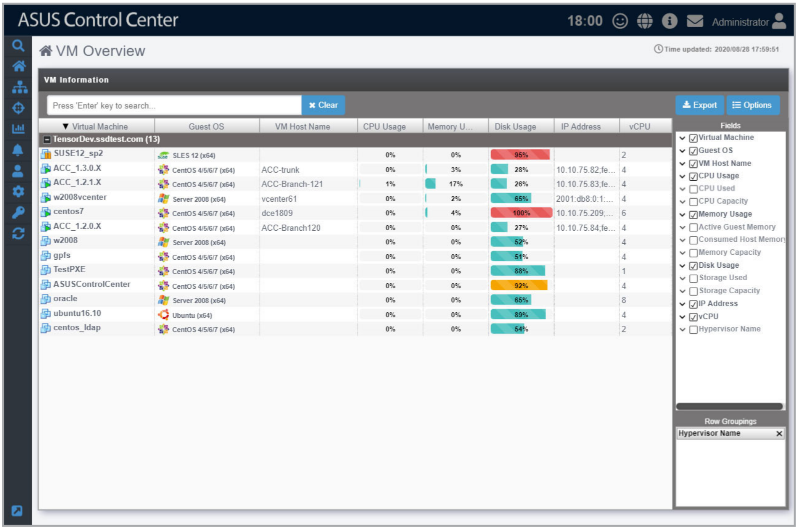
□ Low Alert

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.



ASUS Control Center 18:00 Administrator

VM Overview

Time updated: 2020/08/28 17:59:51

VM Information

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

Export ☰ Options

▼ Virtual Machine	Guest OS	VM Host Name	CPU Usage	Memory U...	Disk Usage	IP Address	vCPU
⊟ TensorDev.ssdtest.com (13)							
SUSE12_sp2	SLES 12 (x64)		0%	0%	95%		2
ACC_1.3.0.X	CentOS 4/5/6/7 (x64)	ACC-trunk	0%	3%	28%	10.10.75.82;fe...	4
ACC_1.2.1.X	CentOS 4/5/6/7 (x64)	ACC-Branch-121	1%	17%	26%	10.10.75.83;fe...	4
w2008vcenter	Server 2008 (x64)	vcenter61	0%	2%	65%	2001:db8:0:1:...	4
centos7	CentOS 4/5/6/7 (x64)	dce1809	0%	4%	100%	10.10.75.209;...	6
ACC_1.2.0.X	CentOS 4/5/6/7 (x64)	ACC-Branch120	0%	0%	27%	10.10.75.84;fe...	4
w2008	Server 2008 (x64)		0%	0%	52%		4
gpfs	CentOS 4/5/6/7 (x64)		0%	0%	51%		4
TestPXE	CentOS 4/5/6/7 (x64)		0%	0%	88%		1
ASUSControlCenter	CentOS 4/5/6/7 (x64)		0%	0%	92%		4
oracle	Server 2008 (x64)		0%	0%	65%		8
ubuntu16.10	Ubuntu (x64)		0%	0%	89%		4
centos_ldap	CentOS 4/5/6/7 (x64)		0%	0%	54%		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

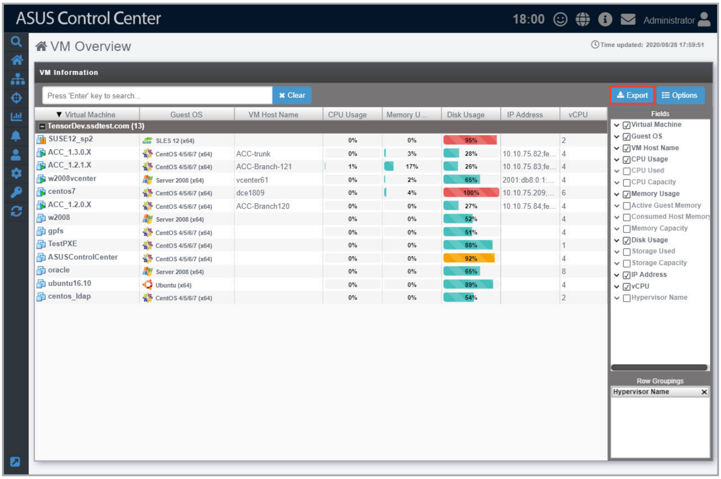
Hypervisor Name ✕

- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.
- 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**.

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**.

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.



▼ Virtual Machine	Guest OS	VM Host Name	CPU Usage	Memory U...	Disk Usage	IP Address	vCPU
TensorDev.ssdtest.com (13)							
SUSE12_sp2	SLES 12 (x64)		0%	0%	95%		2
ACC_1.3.0.X	CentOS 4/5/6/7 (x64)	ACC-trunk	0%	3%	28%	10.10.75.82;fe...	4
ACC_1.2.1.X	CentOS 4/5/6/7 (x64)	ACC-Branch-121	1%	17%	26%	10.10.75.83;fe...	4
w2008vcenter	Server 2008 (x64)	vcenter61	0%	2%	65%	2001:db8:0:1:...	4
centos7	CentOS 4/5/6/7 (x64)	dce1809	0%	4%	100%	10.10.75.209;...	6
ACC_1.2.0.X	CentOS 4/5/6/7 (x64)	ACC-Branch120	0%	0%	27%	10.10.75.84;fe...	4
w2008	Server 2008 (x64)		0%	0%	52%		4
gpfs	CentOS 4/5/6/7 (x64)		0%	0%	51%		4
TestPXE	CentOS 4/5/6/7 (x64)		0%	0%	88%		1
ASUSControlCenter	CentOS 4/5/6/7 (x64)		0%	0%	92%		4
oracle	Server 2008 (x64)		0%	0%	65%		8
ubuntu16.10	Ubuntu (x64)		0%	0%	89%		4
centos_ldap	CentOS 4/5/6/7 (x64)		0%	0%	54%		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

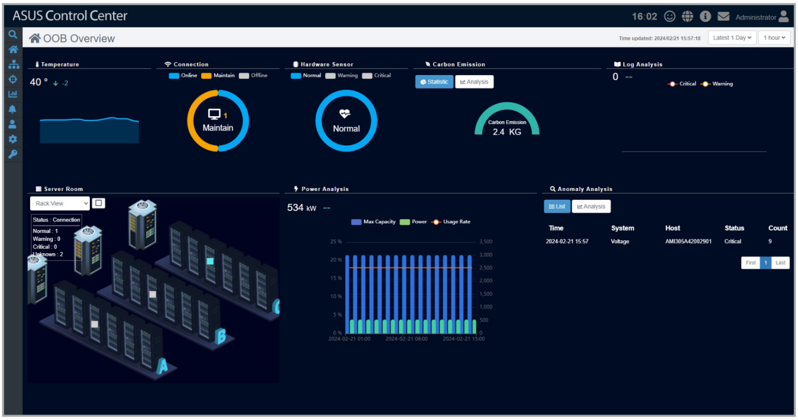
Row Groupings

Hypervisor Name ✕

2.4 OOB Overview

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

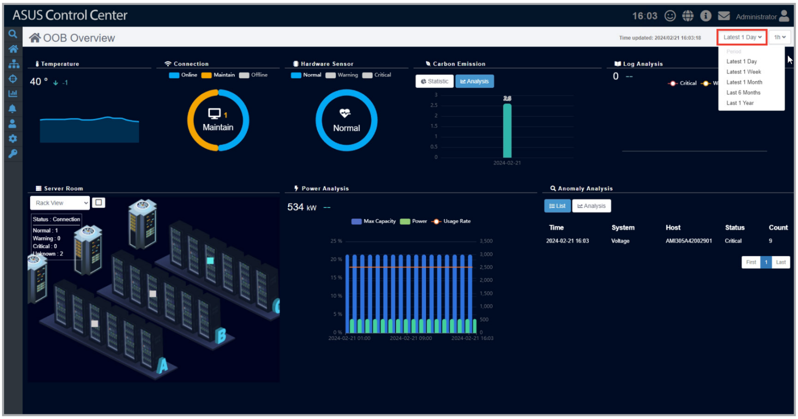
To access the **OOB Overview**, click 🏠 > **OOB Overview** from the left menu.



Time	System	Host	Status	Count
2024-02-21 15:57	Voltage	AMI305A42002901	Critical	9

Filtering the displayed information by time period

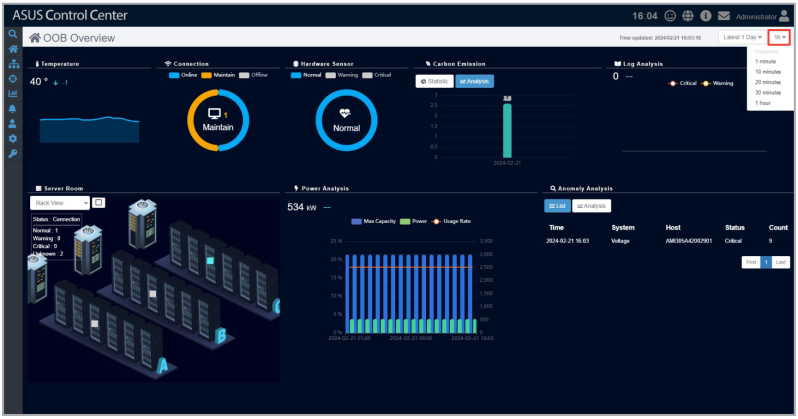
Select a time period from the **Period** drop down menu to only show records within the specified time period.



Time	System	Host	Status	Count
2024-02-21 16:03	Voltage	AMI305A42002901	Critical	9

Adjusting the frequency of displayed information

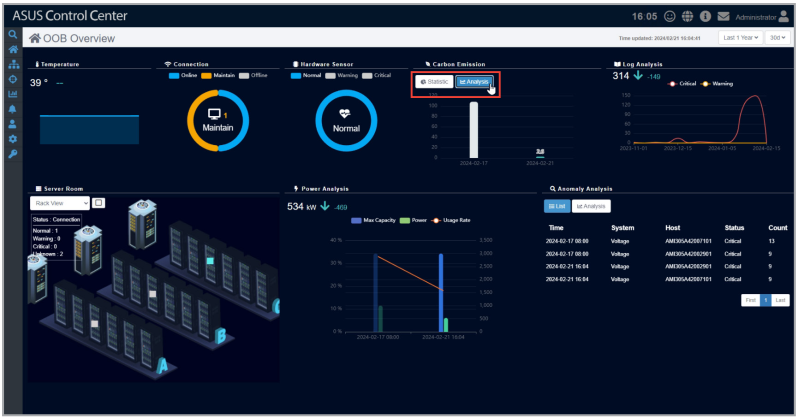
Select a frequency from the **Frequency** drop down menu to group the displayed information by the selected frequency.



Time	System	Host	Status	Count
2024-02-21 16:03	Voltage	AMI305A42002901	Critical	9

Switching between views for displayed information

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



Time	System	Host	Status	Count
2024-02-17 08:00	Voltage	AMI305A42007101	Critical	13
2024-02-17 08:00	Voltage	AMI305A42002901	Critical	9
2024-02-21 16:04	Voltage	AMI305A42002901	Critical	9
2024-02-21 16:04	Voltage	AMI305A42007101	Critical	9

2.5 Host Information

- 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.
- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

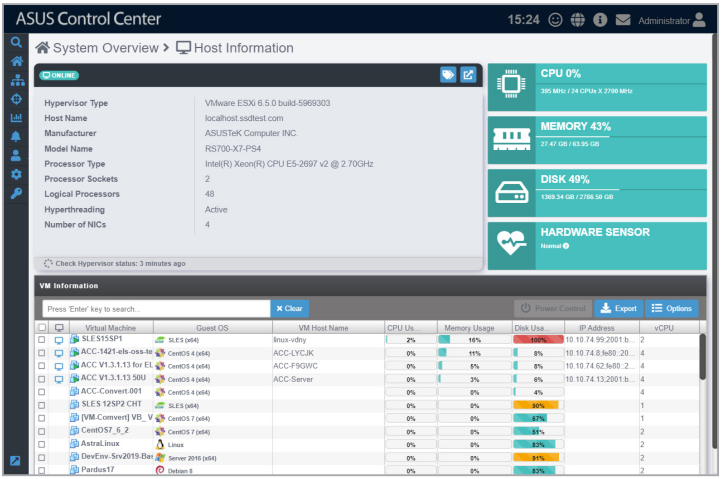
The **Host Information** screen gives you various functions to view the status and manage the selected hypervisor.

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

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

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

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



Hypervisor Type	VMware ESXi 6.5.0 build-5969303
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
Number of NICs	4

Check Hypervisor status: 3 minutes ago

CPU 0%
395 MHz / 24 CPUs X 2700 MHz

MEMORY 43%
27.47 GB / 63.95 GB

DISK 49%
1369.34 GB / 2786.50 GB

HARDWARE SENSOR
Normal

□	🖥	Virtual Machine	Guest OS	VM Host Name	CPU Us...	Memory Usage	Disk Usa...	IP Address	vCPU
□	🖥	SLES15SP1	SLES (x64)	linux-vdny	2%	16%	100%	10.10.74.99;2001:b...	2
□	🖥	ACC-1421-els-oss-te	CentOS 4 (x64)	ACC-LYCJK	0%	11%	8%	10.10.74.8;fe80::20...	4
□	🖥	ACC V1.3.1.13 for EL	CentOS 4 (x64)	ACC-F9GWC	0%	5%	8%	10.10.74.62;fe80::2...	4
□	🖥	ACC V1.3.1.13 50U	CentOS 4 (x64)	ACC-Server	0%	3%	6%	10.10.74.13;2001:b...	4
□		ACC-Convert-001	CentOS 4 (x64)		0%	0%	4%		4
□		SLES 12SP2 CHT	SLES (x64)		0%	0%	90%		1
□		[VM-Comvert] VB_ V	CentOS 7 (x64)		0%	0%	67%		1
□		CentOS7_6_2	CentOS 7 (x64)		0%	0%	51%		2
□		AstraLinux	Linux		0%	0%	83%		2
□		DevEnv-Srv2019-Bas	Server 2016 (x64)		0%	0%	91%		2
□		Pardus17	Debian 8		0%	0%	83%		2

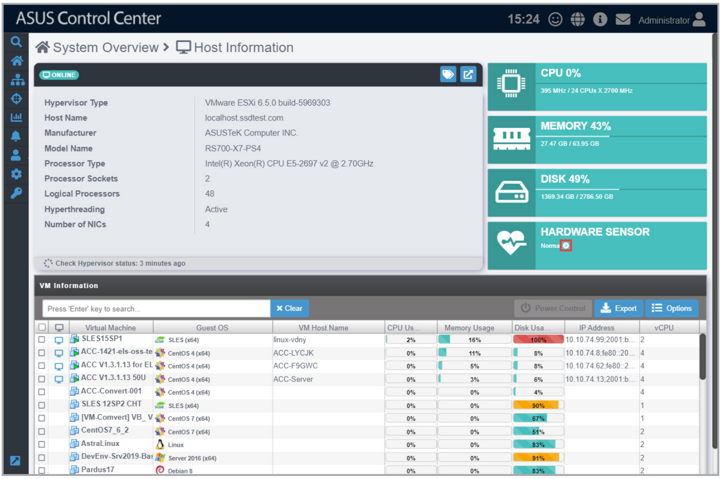
Device Statuses and Quick Buttons

ONLINE	**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.

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

2.5.1 Hardware Sensor

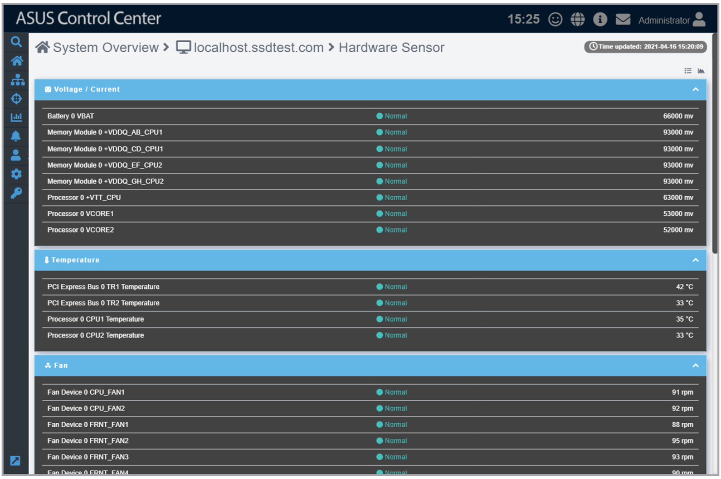
This item allows you to view the details and values for the Voltage / Current, Temperature, Fan, Power Supply, CPU, and Other items. You can view the Hardware Sensor information for the selected device by clicking on the › arrow in the Hardware Sensor block.



Hypervisor Type	VMware ESXi 6.5.0 build-5969303
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
Number of NICs	4

Check Hypervisor status: 3 minutes ago

□		Virtual Machine	Guest OS	VM Host Name	CPU Us...	Memory Usage	Disk Usa...	IP Address	vCPU
□		SLES15SP1	SLES (x64)	linux-vdny	2%	16%	100%	10.10.74.99;2001:b...	2
□		ACC-1421-els-oss-te	CentOS 4 (x64)	ACC-LYCJK	0%	11%	8%	10.10.74.8;fe80::20...	4
□		ACC V1.3.1.13 for EL	CentOS 4 (x64)	ACC-F9GWC	0%	5%	8%	10.10.74.62;fe80::2...	4
□		ACC V1.3.1.13 50U	CentOS 4 (x64)	ACC-Server	0%	3%	6%	10.10.74.13;2001:b...	4
□		ACC-Convert-001	CentOS 4 (x64)		0%	0%	4%		4
□		SLES 12SP2 CHT	SLES (x64)		0%	0%	90%		1
□		[VM-Comvert] VB_ V	CentOS 7 (x64)		0%	0%	67%		1
□		CentOS7_6_2	CentOS 7 (x64)		0%	0%	51%		2
□		AstraLinux	Linux		0%	0%	83%		2
□		DevEnv-Srv2019-Bas	Server 2016 (x64)		0%	0%	91%		2
□		Pardus17	Debian 8		0%	0%	83%		2



System Overview > localhost.ssdtest.com > Hardware Sensor

Time updated: 2021-04-16 15:20:09

Voltage / Current

Battery 0 VBAT	● Normal	66000 mv
Memory Module 0 +VDDQ_AB_CPU1	● Normal	93000 mv
Memory Module 0 +VDDQ_CD_CPU1	● Normal	93000 mv
Memory Module 0 +VDDQ_EF_CPU2	● Normal	93000 mv
Memory Module 0 +VDDQ_GH_CPU2	● Normal	93000 mv
Processor 0 +VTT_CPU	● Normal	63000 mv
Processor 0 VCORE1	● Normal	53000 mv
Processor 0 VCORE2	● Normal	52000 mv

Temperature

PCI Express Bus 0 TR1 Temperature	● Normal	42 °C
PCI Express Bus 0 TR2 Temperature	● Normal	33 °C
Processor 0 CPU1 Temperature	● Normal	35 °C
Processor 0 CPU2 Temperature	● Normal	33 °C

Fan

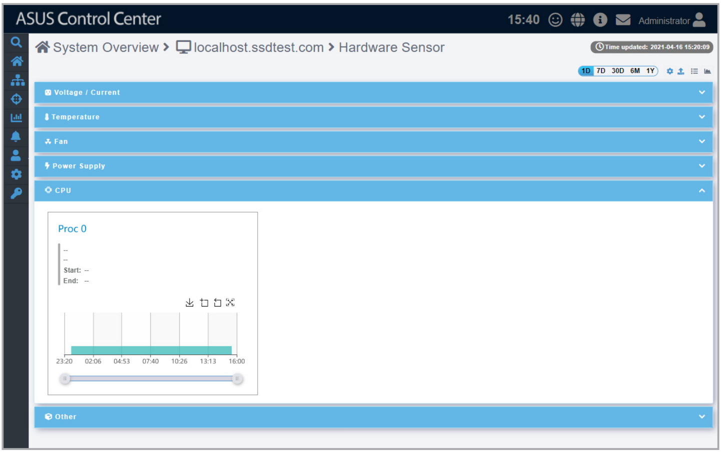
Fan Device 0 CPU_FAN1	● Normal	91 rpm
Fan Device 0 CPU_FAN2	● Normal	92 rpm
Fan Device 0 FRNT_FAN1	● Normal	88 rpm
Fan Device 0 FRNT_FAN2	● Normal	95 rpm
Fan Device 0 FRNT_FAN3	● Normal	93 rpm
Fan Device 0 FRNT_FAN4	● Normal	90 rpm

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

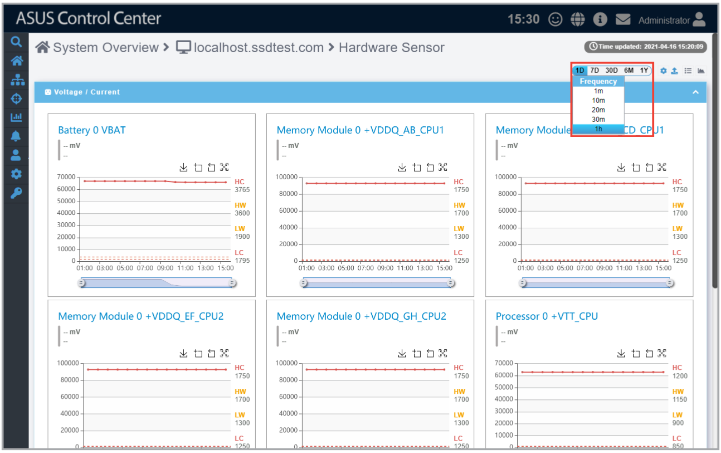
You can toggle the chart view which displays historical data for the Voltage / Current, Temperature, Fan, Power Supply, CPU, and Other sensor events according to different periods of time.



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.


ASUS Control Center
15:30
Administrator
System Overview > localhost.ssdtest.com > Hardware Sensor
Time updated: 2021-04-16 15:20:09
1D 7D 30D 6M 1Y
Frequency
1m
10m
20m
30m
1h
Voltage / Current
Battery 0 VBAT
Memory Module 0 +VDDQ_AB_CPU1
Memory Module 0 +VDDQ_CD_CPU1
Memory Module 0 +VDDQ_EF_CPU2
Memory Module 0 +VDDQ_GH_CPU2
Processor 0 +VTT_CPU
-- mV
HC
HW
LW
LC
01:00 03:00 05:00 07:00 09:00 11:00 13:00 15:00

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

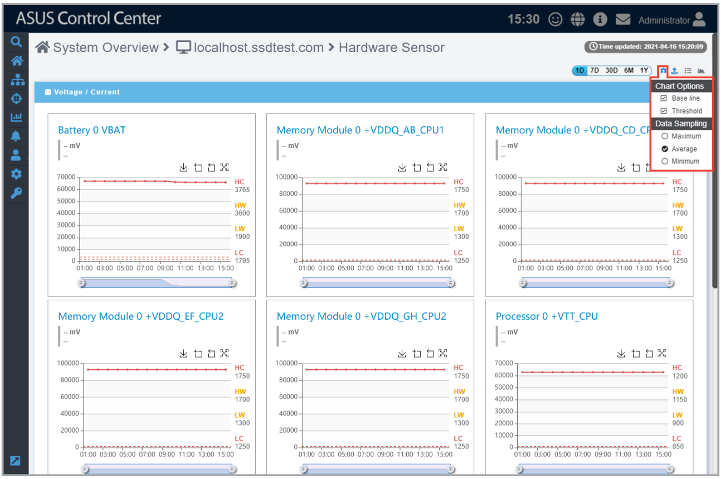


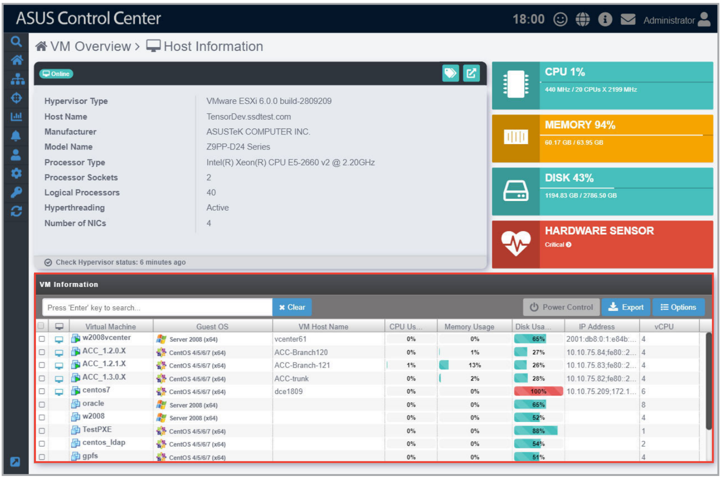
Chart Options
☑ Base line
☑ Threshold

Data Sampling
○ Maximum
● Average
○ Minimum

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

2.5.2 VM Information

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



ASUS Control Center 18:00 Administrator

VM Overview > Host Information

Online

Hypervisor Type	VMware ESXi 6.0.0 build-2809209
Host Name	TensorDev.ssdtest.com
Manufacturer	ASUSTeK COMPUTER INC.
Model Name	Z9PP-D24 Series
Processor Type	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz
Processor Sockets	2
Logical Processors	40
Hyperthreading	Active
Number of NICs	4

Check Hypervisor status: 6 minutes ago

CPU 1%
440 MHz / 20 CPUs X 2199 MHz

MEMORY 94%
60.17 GB / 63.95 GB

DISK 43%
1194.83 GB / 2786.50 GB

HARDWARE SENSOR
Critical

VM Information

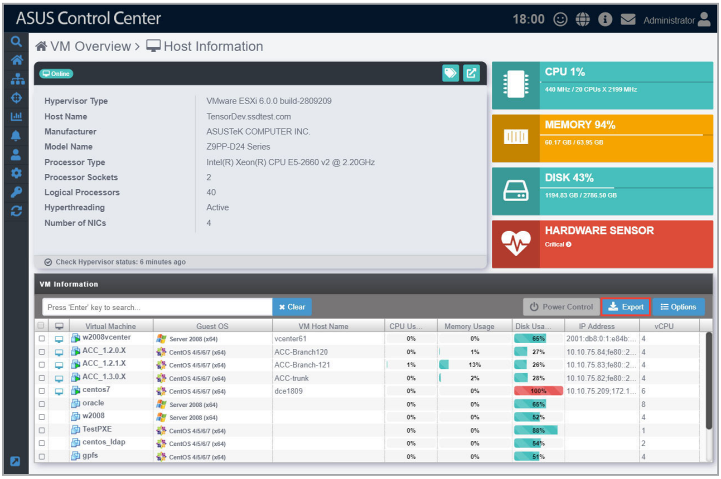
Press 'Enter' key to search... ✖ Clear   Power Control   Export   Options

□		Virtual Machine	Guest OS	VM Host Name	CPU Us...	Memory Usage	Disk Usa...	IP Address	vCPU
□		w2008vcenter	Server 2008 (x64)	vcenter61	0%	0%	65%	2001:db8:0:1:e84b:...	4
□		ACC_1.2.0.X	CentOS 4/5/6/7 (x64)	ACC-Branch120	0%	1%	27%	10.10.75.84;fe80::2...	4
□		ACC_1.2.1.X	CentOS 4/5/6/7 (x64)	ACC-Branch-121	1%	13%	26%	10.10.75.83;fe80::2...	4
□		ACC_1.3.0.X	CentOS 4/5/6/7 (x64)	ACC-trunk	0%	2%	28%	10.10.75.82;fe80::2...	4
□		centos7	CentOS 4/5/6/7 (x64)	dce1809	0%	0%	100%	10.10.75.209;172.1...	6
□		oracle	Server 2008 (x64)		0%	0%	65%		8
□		w2008	Server 2008 (x64)		0%	0%	52%		4
□		TestPXE	CentOS 4/5/6/7 (x64)		0%	0%	88%		1
□		centos_ldap	CentOS 4/5/6/7 (x64)		0%	0%	54%		2
□		gpfs	CentOS 4/5/6/7 (x64)		0%	0%	51%		4

Exporting VM Information

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

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 Center 18:00 Administrator

VM Overview > Host Information

Online

Hypervisor Type	VMware ESXi 6.0.0 build-2809209
Host Name	TensorDev.ssdtest.com
Manufacturer	ASUSTeK COMPUTER INC.
Model Name	Z9PP-D24 Series
Processor Type	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz
Processor Sockets	2
Logical Processors	40
Hyperthreading	Active
Number of NICs	4

Check Hypervisor status: 6 minutes ago

CPU 1%
440 MHz / 20 CPUs X 2199 MHz

MEMORY 94%
60.17 GB / 63.95 GB

DISK 43%
1194.83 GB / 2786.50 GB

HARDWARE SENSOR
Critical

VM Information

Press 'Enter' key to search... ✖ Clear   Power Control   Export   Options

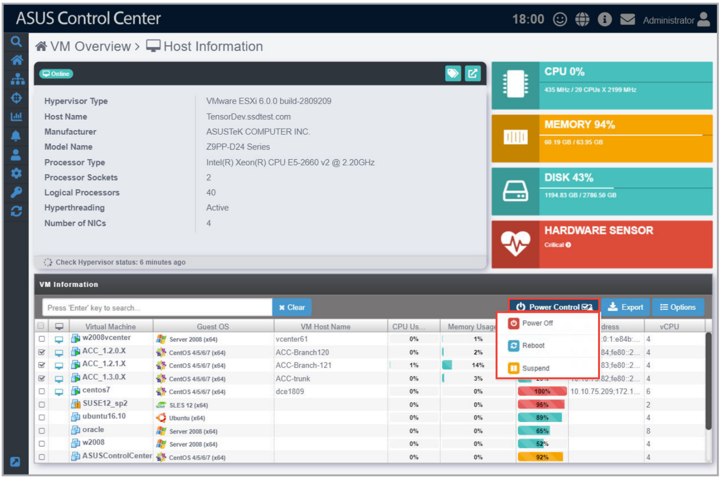
□		Virtual Machine	Guest OS	VM Host Name	CPU Us...	Memory Usage	Disk Usa...	IP Address	vCPU
□		w2008vcenter	Server 2008 (x64)	vcenter61	0%	0%	65%	2001:db8:0:1:e84b:...	4
□		ACC_1.2.0.X	CentOS 4/5/6/7 (x64)	ACC-Branch120	0%	1%	27%	10.10.75.84;fe80::2...	4
□		ACC_1.2.1.X	CentOS 4/5/6/7 (x64)	ACC-Branch-121	1%	13%	26%	10.10.75.83;fe80::2...	4
□		ACC_1.3.0.X	CentOS 4/5/6/7 (x64)	ACC-trunk	0%	2%	28%	10.10.75.82;fe80::2...	4
□		centos7	CentOS 4/5/6/7 (x64)	dce1809	0%	0%	100%	10.10.75.209;172.1...	6
□		oracle	Server 2008 (x64)		0%	0%	65%		8
□		w2008	Server 2008 (x64)		0%	0%	52%		4
□		TestPXE	CentOS 4/5/6/7 (x64)		0%	0%	88%		1
□		centos_ldap	CentOS 4/5/6/7 (x64)		0%	0%	54%		2
□		gpfs	CentOS 4/5/6/7 (x64)		0%	0%	51%		4

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).

> 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.



ASUS Control Center 18:00 Administrator

VM Overview > Host Information

Online

Hypervisor Type	VMware ESXi 6.0.0 build-2809209
Host Name	TensorDev.ssdtest.com
Manufacturer	ASUSTeK COMPUTER INC.
Model Name	Z9PP-D24 Series
Processor Type	Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.20GHz
Processor Sockets	2
Logical Processors	40
Hyperthreading	Active
Number of NICs	4

Check Hypervisor status: 6 minutes ago

CPU 0%
435 MHz / 20 CPUs X 2199 MHz

MEMORY 94%
60.19 GB / 63.95 GB

DISK 43%
1194.83 GB / 2786.50 GB

HARDWARE SENSOR
Critical

VM Information

Press 'Enter' key to search... ✖ Clear | Power Control | Export | Options

Power Off
Reboot
Suspend

☐		Virtual Machine	Guest OS	VM Host Name	CPU Us...	Memory Usage		dress	vCPU
☐		w2008vcenter	Server 2008 (x64)	vcenter61	0%	1%		:0:1:e84b:...	4
☑		ACC_1.2.0.X	CentOS 4/5/6/7 (x64)	ACC-Branch120	0%	2%		84;fe80::2...	4
☑		ACC_1.2.1.X	CentOS 4/5/6/7 (x64)	ACC-Branch-121	1%	14%		83;fe80::2...	4
☑		ACC_1.3.0.X	CentOS 4/5/6/7 (x64)	ACC-trunk	0%	3%		82;fe80::2...	4
☐		centos7	CentOS 4/5/6/7 (x64)	dce1809	0%	0%	100%	10.10.75.209;172.1...	6
☐		SUSE12_sp2	SLES 12 (x64)		0%	0%	95%		2
☐		ubuntu16.10	Ubuntu (x64)		0%	0%	89%		4
☐		oracle	Server 2008 (x64)		0%	0%	65%		8
☐		w2008	Server 2008 (x64)		0%	0%	52%		4
☐		ASUSControlCenter	CentOS 4/5/6/7 (x64)		0%	0%	92%		4

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.

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

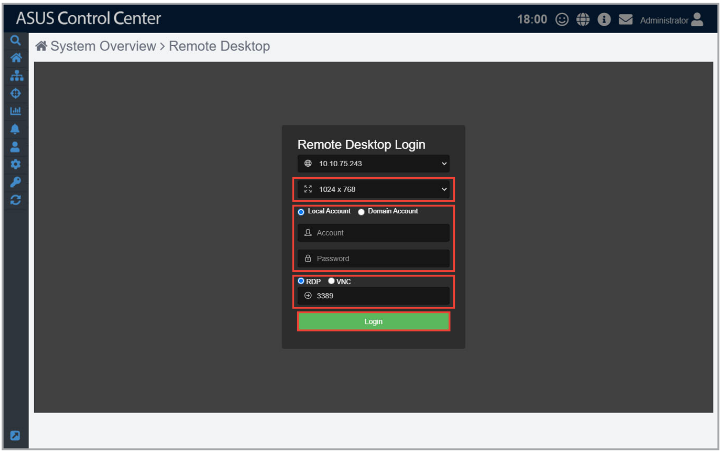
1. Select a VM from the **VM Information** block.
2. Click on the 🖥 icon located next to the VM you wish to view in the **VM Information** block, you should be directed to the **Remote Desktop Login** screen.
3. Select a resolution to display the managed device in the Remote Desktop window.
4. Select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

- **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**.

Linux and Windows® systems use different protocols, ensure the 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.



Remote Desktop Login

10.10.75.243

1024 x 768

◉ Local Account ○ Domain Account

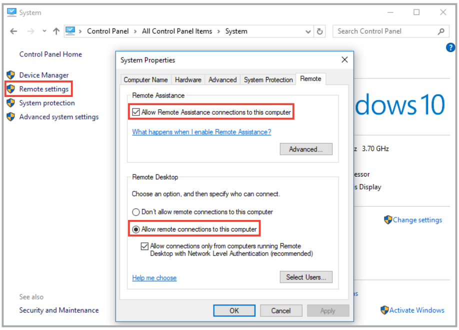
Account

Password

◉ RDP ○ VNC

3389

- 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**.



Remote Assistance

☑ Allow Remote Assistance connections to this computer

Remote Desktop

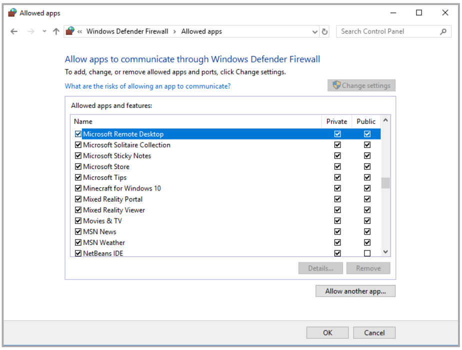
Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

- (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**.



Allow apps to communicate through Windows Defender Firewall

To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ Microsoft Remote Desktop	☑	☑
☑ Microsoft Solitaire Collection	☑	☑
☑ Microsoft Sticky Notes	☑	☑
☑ Microsoft Store	☑	☑
☑ Microsoft Tips	☑	☑
☑ Minecraft for Windows 10	☑	☑
☑ Mixed Reality Portal	☑	☑
☑ Mixed Reality Viewer	☑	☑
☑ Movies & TV	☑	☑
☑ MSN News	☑	☑
☑ MSN Weather	☑	☑
☑ NetBeans IDE	☑	□

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.

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.

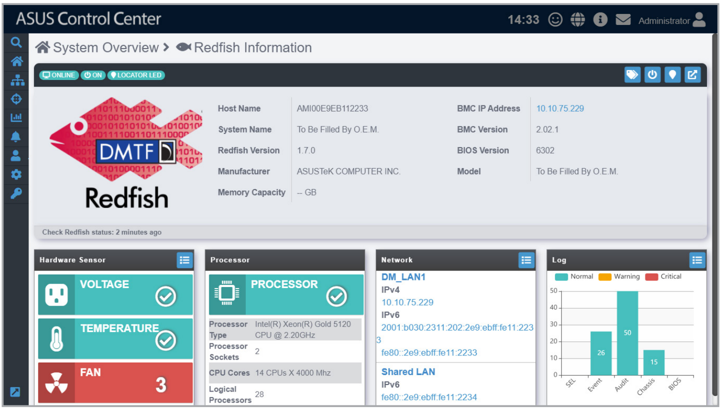
7. Click on the Menu Path at the top of the screen, or click on another menu item from the left menu to end the remote session.

2.6 Redfish Information

- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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**.



Host Name	AMI00E9EB112233	BMC IP Address	10.10.75.229
System Name	To Be Filled By O.E.M.	BMC Version	2.02.1
Redfish Version	1.7.0	BIOS Version	6302
Manufacturer	ASUSTeK COMPUTER INC.	Model	To Be Filled By O.E.M.
Memory Capacity	-- GB		

Check Redfish status: 2 minutes ago

Processor Type	Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Processor Sockets	2
CPU Cores	14 CPUs X 4000 Mhz
Logical Processors	28

Network

DM_LAN1
IPv4
10.10.75.229
IPv6
2001:b030:2311:202:2e9:ebff:fe11:2233
fe80::2e9:ebff:fe11:2233

Shared LAN
IPv6
fe80::2e9:ebff:fe11:2234

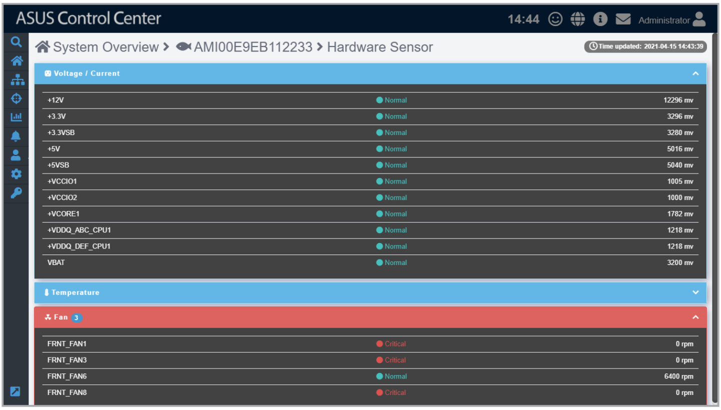
The **Redfish Information** screen will display the **Host Name**, **System Name**, **Redfish Version**, **Manufacturer**, **Memory Capacity**, **BMC IP Address**, **BMC Version**, **BIOS Version** and **Model** of the device. In the blocks located at the bottom of the screen, the **Processor** block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

Redfish device Statuses and Quick Buttons

🖥 ONLINE	**Connection status**	This item displays the connection status of the selected Redfish device.
⏻ ON	**Power Status**	This item displays the power status of the selected Redfish device.
📍 LOCATOR LED	**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 Redfish device by double clicking in the **Value** field.
⏻	**Power Control**	This item allows you to power off or restart a Redfish device.
📍	**Locator LED**	This item allows you to turn on/off the Locator LED.
↗	**BMC**	This item will link to the BMC website.
☰	**Detail**	This item will redirect you to the selected block's (**Hardware Sensor**, **Network**, **Log**) details screen.

2.6.1 Hardware Sensor

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


ASUS Control Center
14:44
Administrator
System Overview > AMI00E9EB112233 > Hardware Sensor
Time updated: 2021-04-15 14:43:39

Voltage / Current

+12V	● Normal	12296 mv
+3.3V	● Normal	3296 mv
+3.3VSB	● Normal	3280 mv
+5V	● Normal	5016 mv
+5VSB	● Normal	5040 mv
+VCCIO1	● Normal	1005 mv
+VCCIO2	● Normal	1000 mv
+VCORE1	● Normal	1782 mv
+VDDQ_ABC_CPU1	● Normal	1218 mv
+VDDQ_DEF_CPU1	● Normal	1218 mv
VBAT	● Normal	3200 mv

Temperature

Fan 3

FRNT_FAN1	● Critical	0 rpm
FRNT_FAN3	● Critical	0 rpm
FRNT_FAN6	● Normal	6400 rpm
FRNT_FAN8	● Critical	0 rpm

Quick Buttons

⌄	Click to expand this block.
⌃	Click to minimize this block.

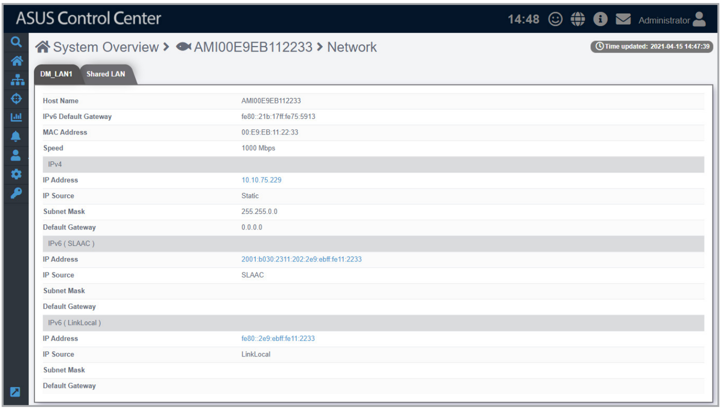
2.6.2 Network

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.

The information entered in this section is for reference only.

DM_LAN

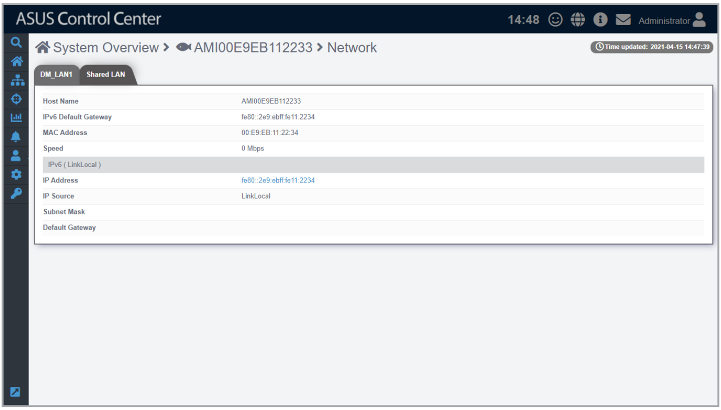
This item is the communication port specifically for BMC, clicking on the BMC IP in the **IP Address** field for **IPv4**, **IPv6 (SLAAC)**, or **IPv6 (LinkLocal)** will redirect you to the ASMB page, allowing you to view the hardware sensor values of the device.


ASUS Control Center
14:48
Administrator
System Overview > AMI00E9EB112233 > Network
Time updated: 2021-04-15 14:47:39
DM_LAN1
Shared LAN

Host Name	AMI00E9EB112233
IPv6 Default Gateway	fe80::21b:17ff:fe75:5913
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:b030:2311:202:2e9:ebff:fe11:2233
IP Source	SLAAC
Subnet Mask	
Default Gateway	
IPv6 (LinkLocal)	
IP Address	fe80::2e9:ebff:fe11:2233
IP Source	LinkLocal
Subnet Mask	
Default Gateway	

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.

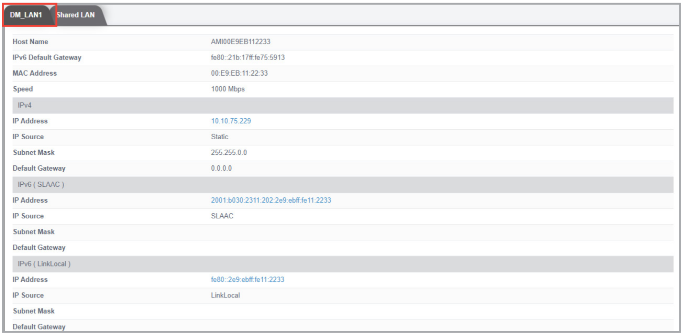

ASUS Control Center
14:48
Administrator
System Overview > AMI00E9EB112233 > Network
Time updated: 2021-04-15 14:47:39
DM_LAN1
Shared LAN

Host Name	AMI00E9EB112233
IPv6 Default Gateway	fe80::2e9:ebff:fe11:2234
MAC Address	00:E9:EB:11:22:34
Speed	0 Mbps
IPv6 (LinkLocal)	
IP Address	fe80::2e9:ebff:fe11:2234
IP Source	LinkLocal
Subnet Mask	
Default Gateway	

Edit BMC using ASMB

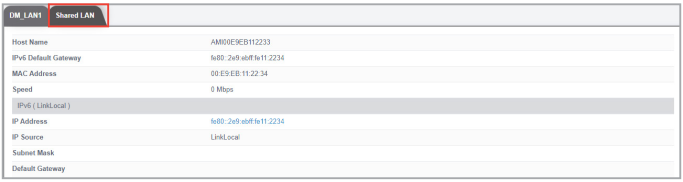
To edit BMC settings using ASMB on the device:

1. Select **DM_LAN1**



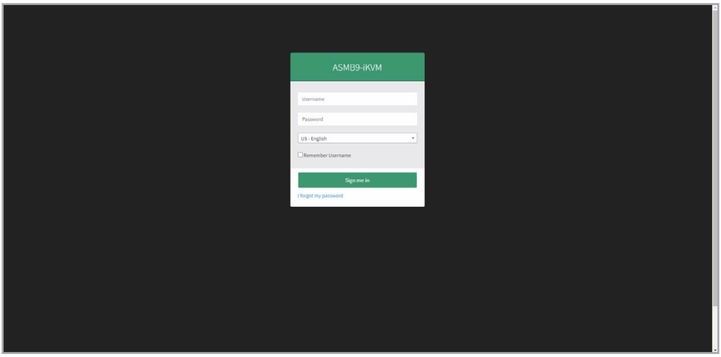
Host Name	AMI00E9EB112233
IPv6 Default Gateway	fe80::21b:17ff:fe75:5913
MAC Address	00:E9:EB:11:22:33
Speed	1000 Mbps
IPv4	
IP Address	10.10.75.229
IP Source	Static
Subnet Mask	255.255.0.0
Default Gateway	0.0.0.0
IPv6 (SLAAC)	
IP Address	2001:b030:2311:202:2e9:ebff:fe11:2233
IP Source	SLAAC
Subnet Mask	
Default Gateway	
IPv6 (LinkLocal)	
IP Address	fe80::2e9:ebff:fe11:2233
IP Source	LinkLocal
Subnet Mask	
Default Gateway	

or **Shared LAN** tab, then click on any of the IP Addresses.



Host Name	AMI00E9EB112233
IPv6 Default Gateway	fe80::2e9:ebff:fe11:2234
MAC Address	00:E9:EB:11:22:34
Speed	0 Mbps
IPv6 (LinkLocal)	
IP Address	fe80::2e9:ebff:fe11:2234
IP Source	LinkLocal
Subnet Mask	
Default Gateway	

2. Login ASMB.

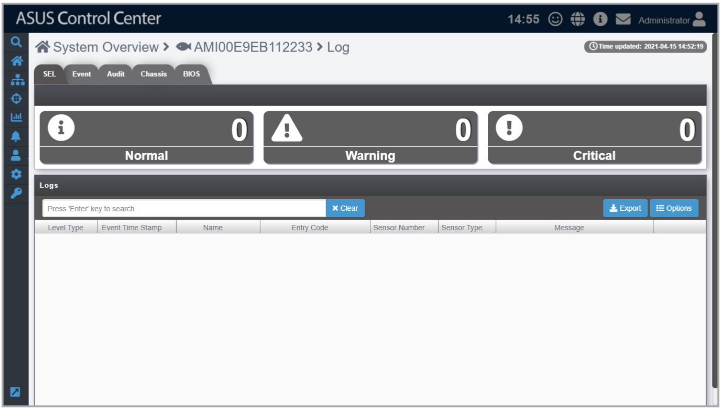


2.6.3 Event Log

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.

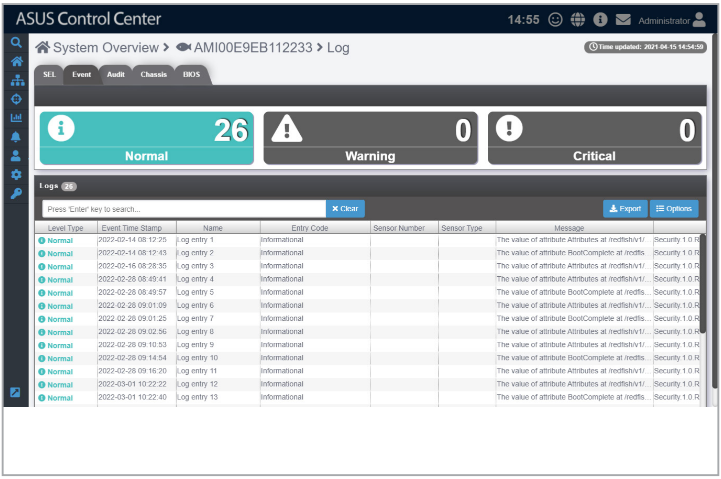
To export the Event Log click the **Export** button, enter a filename, then click **OK**.

SEL tab



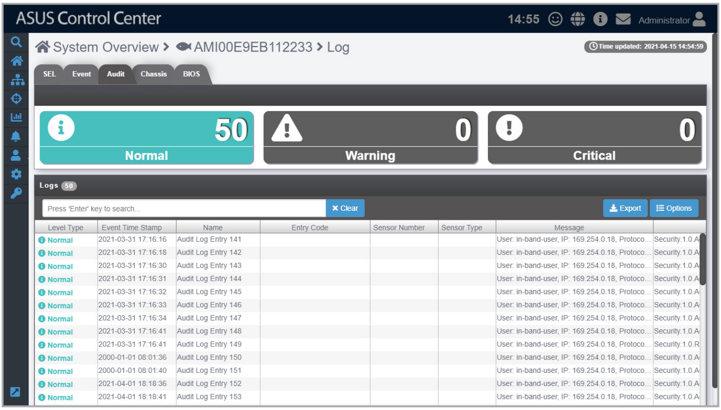
Level Type	Event Time Stamp	Name	Entry Code	Sensor Number	Sensor Type	Message	

Event tab



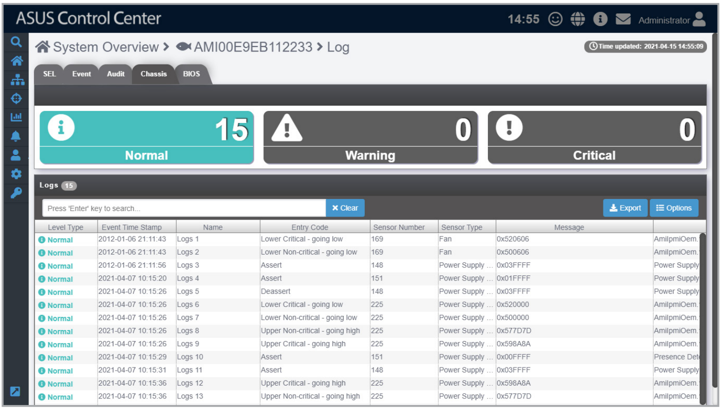
Level Type	Event Time Stamp	Name	Entry Code	Sensor Number	Sensor Type	Message	
Normal	2022-02-14 08:12:25	Log entry 1	Informational			The value of attribute Attributes at /redfish/v1/...	Security.1.0.R
Normal	2022-02-14 08:12:43	Log entry 2	Informational			The value of attribute BootComplete at /redfis...	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 BootComplete at /redfis...	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 BootComplete at /redfis...	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 BootComplete at /redfis...	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 BootComplete at /redfis...	Security.1.0.R

Audit tab



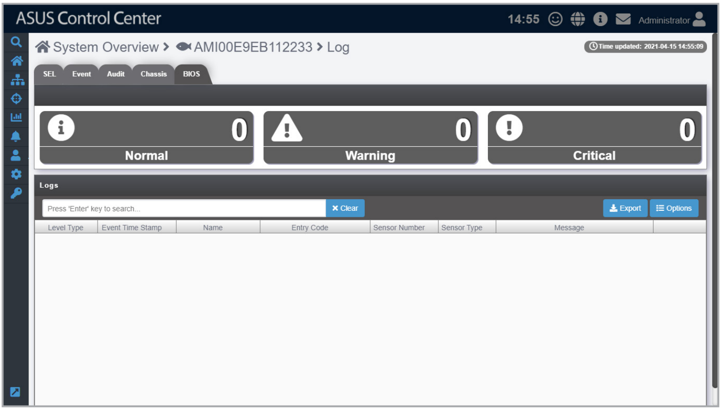
Level Type	Event Time Stamp	Name	Entry Code	Sensor Number	Sensor Type	Message	
Normal	2021-03-31 17:16:16	Audit Log Entry 141				User: in-band-user, IP: 169.254.0.18, Protoco...	Security.1.0.A
Normal	2021-03-31 17:16:18	Audit Log Entry 142				User: in-band-user, IP: 169.254.0.18, Protoco...	Security.1.0.A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

Chassis tab



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	0x520606	AmilpmiOem.
Normal	2012-01-06 21:11:43	Logs 2	Lower Non-critical - going low	169	Fan	0x500606	AmilpmiOem.
Normal	2012-01-06 21:11:56	Logs 3	Assert	148	Power Supply ...	0x03FFFF	Power Supply
Normal	2021-04-07 10:15:20	Logs 4	Assert	151	Power Supply ...	0x01FFFF	Power Supply
Normal	2021-04-07 10:15:26	Logs 5	Deassert	148	Power Supply ...	0x03FFFF	Power Supply
Normal	2021-04-07 10:15:26	Logs 6	Lower Critical - going low	225	Power Supply ...	0x520000	AmilpmiOem.
Normal	2021-04-07 10:15:26	Logs 7	Lower Non-critical - going low	225	Power Supply ...	0x500000	AmilpmiOem.
Normal	2021-04-07 10:15:26	Logs 8	Upper Non-critical - going high	225	Power Supply ...	0x577D7D	AmilpmiOem.
Normal	2021-04-07 10:15:26	Logs 9	Upper Critical - going high	225	Power Supply ...	0x598A8A	AmilpmiOem.
Normal	2021-04-07 10:15:29	Logs 10	Assert	151	Power Supply ...	0x00FFFF	Presence Det
Normal	2021-04-07 10:15:31	Logs 11	Assert	148	Power Supply ...	0x03FFFF	Power Supply
Normal	2021-04-07 10:15:36	Logs 12	Upper Critical - going high	225	Power Supply ...	0x598A8A	AmilpmiOem.
Normal	2021-04-07 10:15:36	Logs 13	Upper Non-critical - going high	225	Power Supply ...	0x577D7D	AmilpmiOem.

BIOS tab



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.

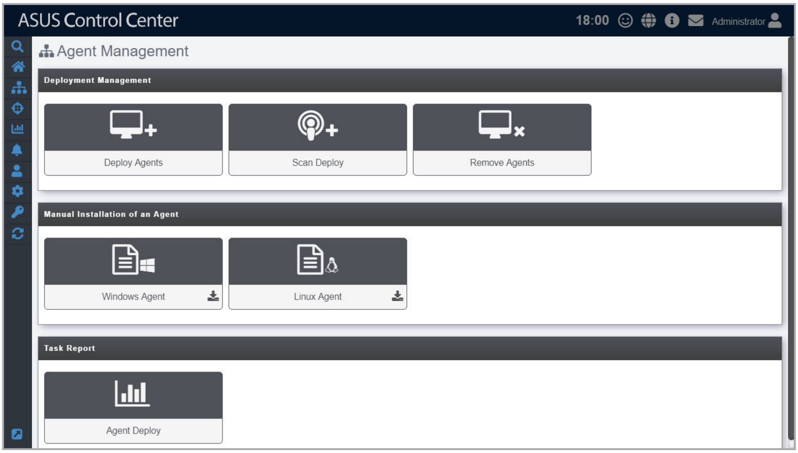
Deployment

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.

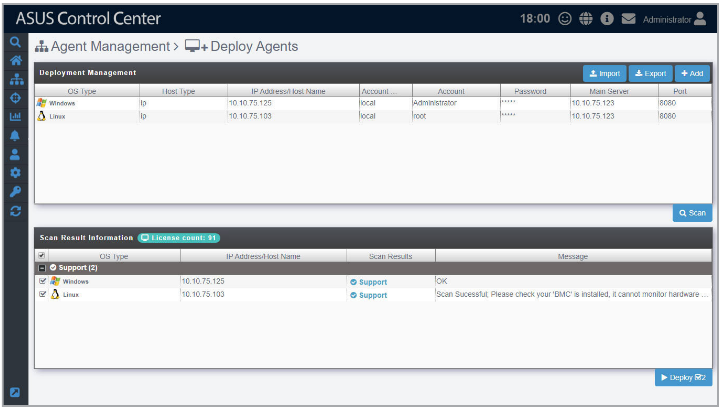
To access **Agent Management**, click 🖧 > **Agent Management** in the left menu.



- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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.



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 License count: 91

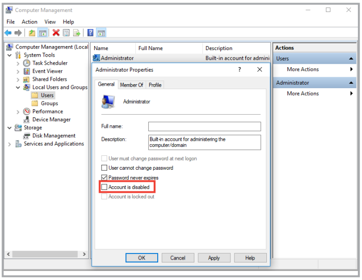
☑	OS Type	IP Address/Host Name	Scan Results	Message
⊟	Support (2)			
☑	Windows	10.10.75.125	Support	OK
☑	Linux	10.10.75.103	Support	Scan Sucessful; Please check your 'BMC' is installed, it cannot monitor hardware ...

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.

> 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**)



Administrator

Full name:

Description: Built-in account for administering the computer/domain

□ User must change password at next logon

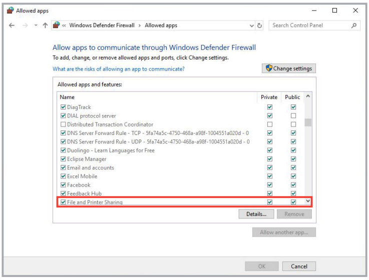
□ User cannot change password

☑ Password never expires

□ Account is disabled

□ Account is locked out

  - **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.



Allow apps to communicate through Windows Defender Firewall

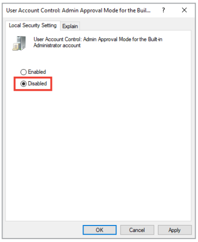
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ DiagTrack	☑	☑
☑ DIAL protocol server	☑	□
□ Distributed Transaction Coordinator	□	□
☑ DNS Server Forward Rule - TCP - 5fa74a5c-4750-468a-a98f-1004551a020d - 0	☑	☑
☑ DNS Server Forward Rule - UDP - 5fa74a5c-4750-468a-a98f-1004551a020d - 0	☑	☑
☑ Duolingo - Learn Languages for Free	☑	☑
☑ Eclipse Manager	☑	☑
☑ Email and accounts	☑	☑
☑ Excel Mobile	☑	☑
☑ Facebook	☑	☑
☑ Feedback Hub	☑	☑
☑ File and Printer Sharing	☑	☑

- **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**.



User Account Control: Admin Approval Mode for the Built-in Administrator account

○ Enabled
● Disabled

- For Debian and Ubuntu clients
  - Enable **SSH**:

    a. Ensure the root account can be logged in through SSH.

    b. Install SSH by executing the following:

    ```
    sudo apt-get install ssh
    ```

    c. 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):

    a. Ensure the root account can be logged in through SSH.

    b. Install SSH by executing the following:

    ```
    sudo apt-get install ssh
    ```

    c. Confirm SSH server by executing the following:

    ```
    systemctl start sshd
    systemctl status sshd
    ```

  - Disable **SELinux**:

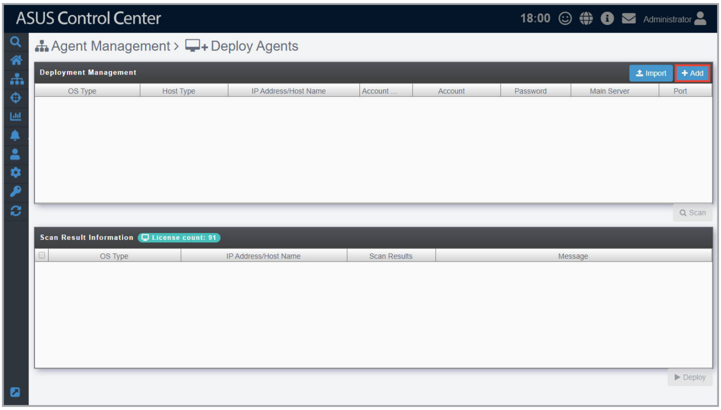
    a. Open */etc/sysconfig/selinux*.

    b. Set **SELINUX=enforcing** to **SELINUX=disabled**.

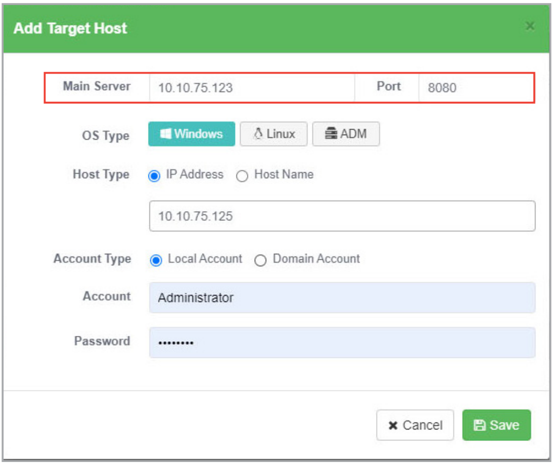
    c. Reboot the system.

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.



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

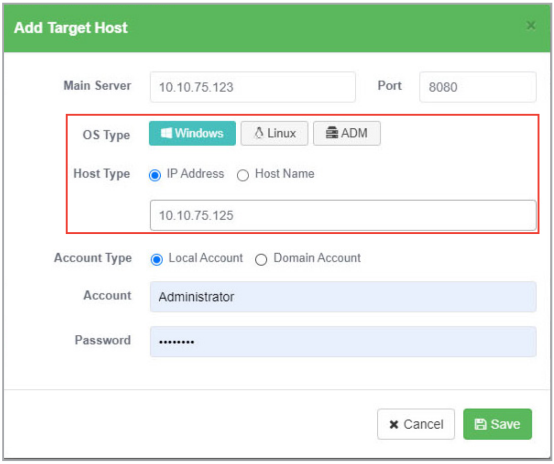
Account: Administrator

Password: •••••••••

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

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

Selecting Windows® system:



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

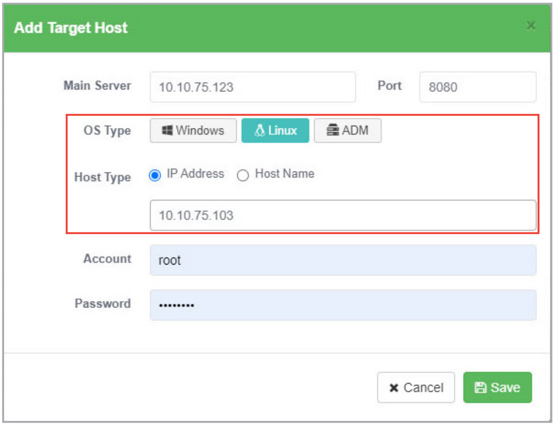
Account Type ● Local Account ○ Domain Account

Account Administrator

Password ••••••••

✖ Cancel Save

Selecting Linux system:



Add Target Host ×

Main Server 10.10.75.123 Port 8080

OS Type Windows [✓ Linux] ADM

Host Type ● IP Address ○ Host Name

10.10.75.103

Account root

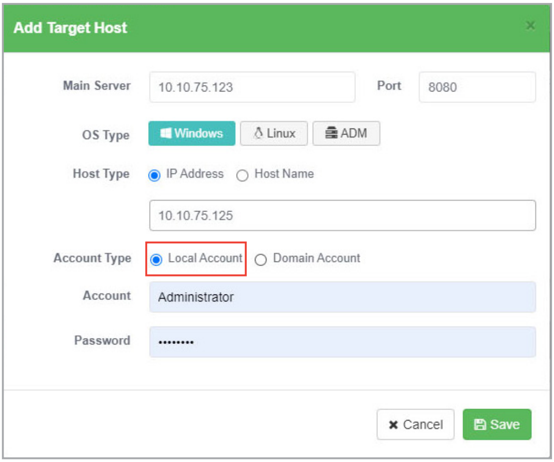
Password ••••••••

✖ Cancel Save

4. Select the **Account Type**.

- **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.

Selecting Local Account:


Add Target Host

Main Server: 10.10.75.123 Port: 8080

OS Type: Windows | Linux | ADM

Host Type: ● IP Address ○ Host Name

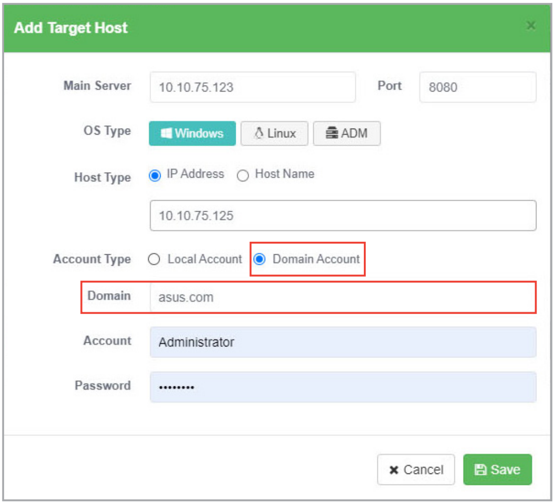
10.10.75.125

Account Type: ● Local Account ○ Domain Account

Account: Administrator

Password: ••••••••

Selecting Domain Account:


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

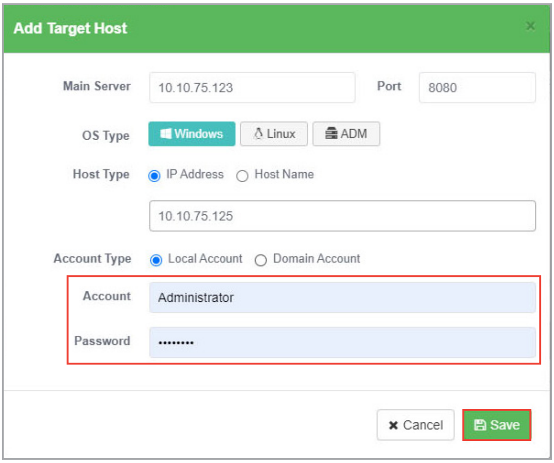
Domain: asus.com

Account: Administrator

Password: ••••••••

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**.

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

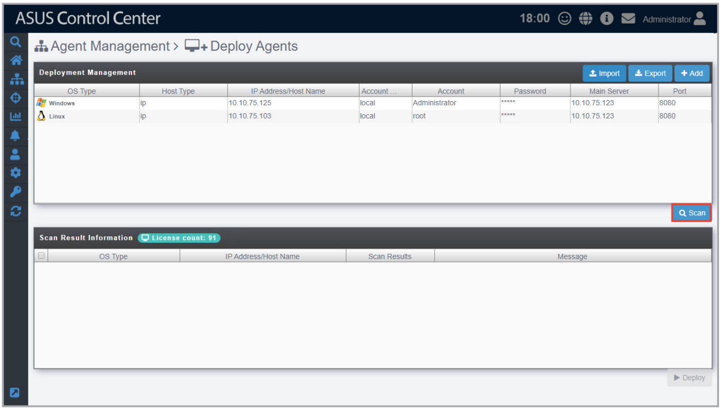


Add Target Host

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	••••••••		

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**.



Deployment Management

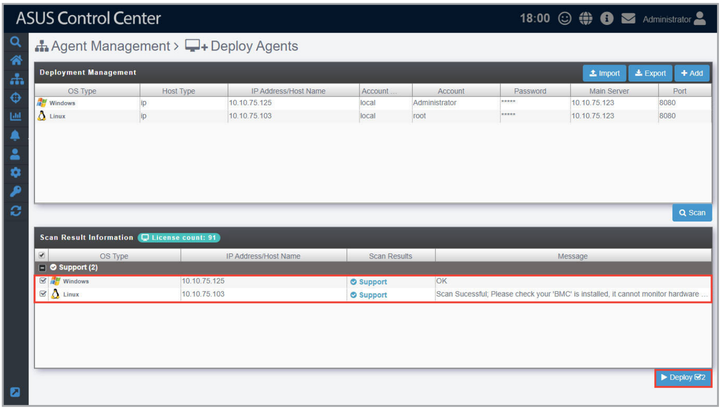
OS Type	Host Type	IP Address/Host Name	Account ...	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	*****	10.10.75.123	8080
Linux	ip	10.10.75.103	local	root	*****	10.10.75.123	8080

Scan Result Information License count: 91

□	OS Type	IP Address/Host Name	Scan Results	Message

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

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



Deployment Management

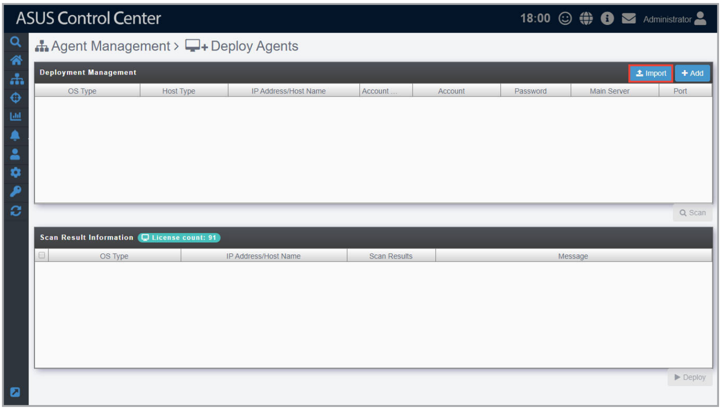
OS Type	Host Type	IP Address/Host Name	Account ...	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	*****	10.10.75.123	8080
Linux	ip	10.10.75.103	local	root	*****	10.10.75.123	8080

Scan Result Information License count: 91

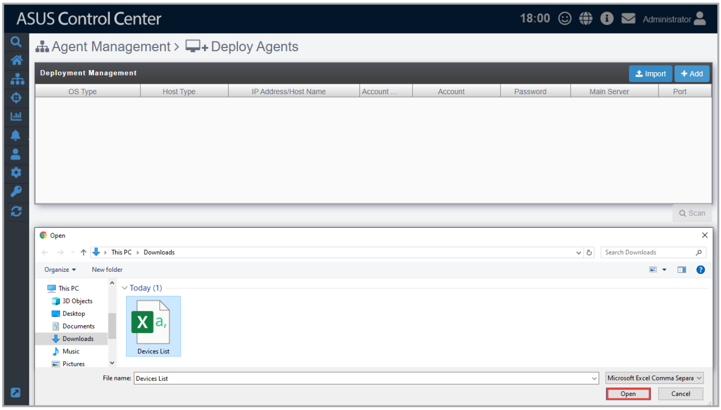
☑	OS Type	IP Address/Host Name	Scan Results	Message
⊟	Support (2)			
☑	Windows	10.10.75.125	Support	OK
☑	Linux	10.10.75.103	Support	Scan Sucessful; Please check your 'BMC' is installed, it cannot monitor hardware ...

Adding devices from CSV file

1. Click on **Import**.

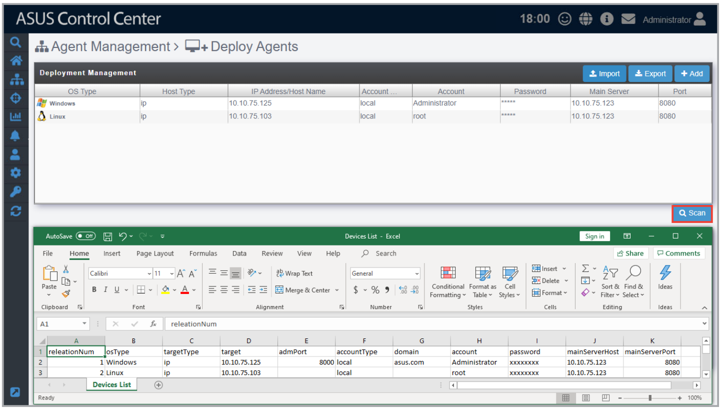


2. Select the CSV file to import and click **Open**.



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

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

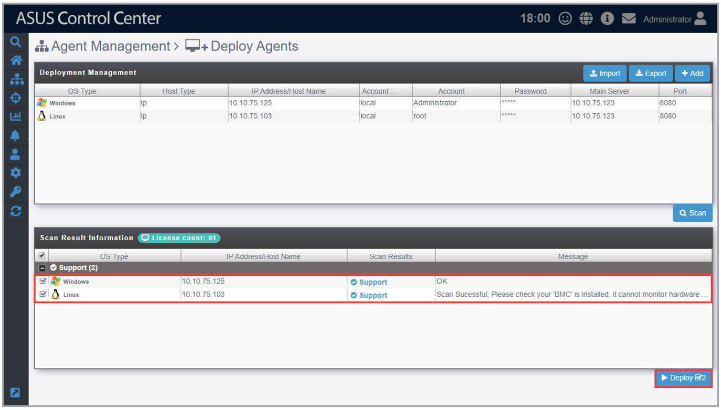


OS Type	Host Type	IP Address/Host Name	Account ...	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	*****	10.10.75.123	8080
Linux	ip	10.10.75.103	local	root	*****	10.10.75.123	8080

	A	B	C	D	E	F	G	H	I	J	K
1	releationNum	osType	targetType	target	admPort	accountType	domain	account	password	mainServerHost	mainServerPort
2	1	Windows	ip	10.10.75.125	8000	local	asus.com	Administrator	xxxxxxxx	10.10.75.123	8080
3	2	Linux	ip	10.10.75.103		local		root	xxxxxxxx	10.10.75.123	8080

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

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

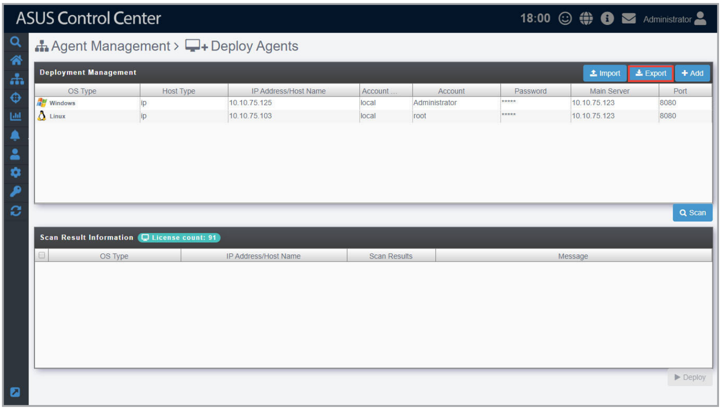


OS Type	Host Type	IP Address/Host Name	Account ...	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	*****	10.10.75.123	8080
Linux	ip	10.10.75.103	local	root	*****	10.10.75.123	8080

☑	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 Sucessful; Please check your 'BMC' is installed, it cannot monitor hardware ...

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.

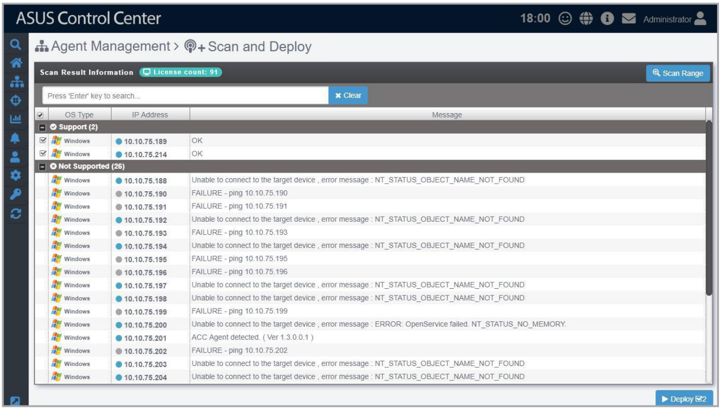


OS Type	Host Type	IP Address/Host Name	Account ...	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	*****	10.10.75.123	8080
Linux	ip	10.10.75.103	local	root	*****	10.10.75.123	8080

□	OS Type	IP Address/Host Name	Scan Results	Message

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.

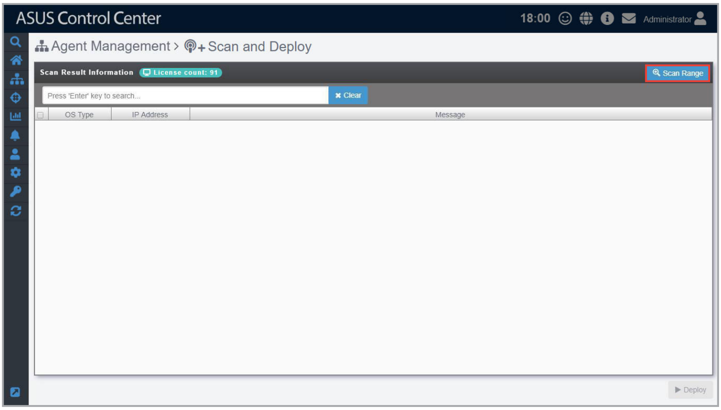


☑	OS Type	IP Address	Message
Support (2)			
☑	Windows	● 10.10.75.189	OK
☑	Windows	● 10.10.75.214	OK
Not Supported (26)			
	Windows	● 10.10.75.188	Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND
	Windows	● 10.10.75.190	FAILURE - ping 10.10.75.190
	Windows	● 10.10.75.191	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

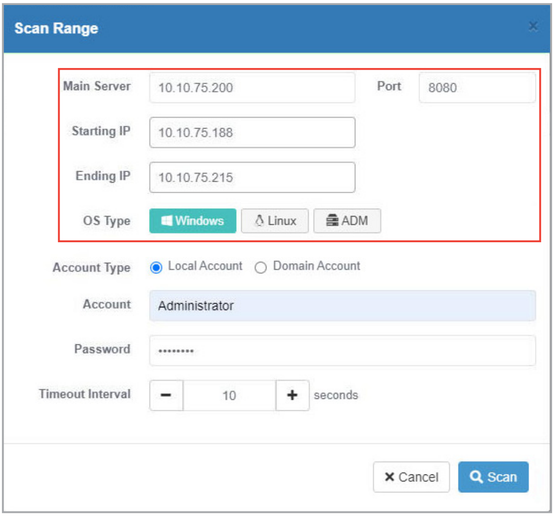
Before using the **Scan and Deploy** function, ensure that the agent deployment conditions and settings are met, for more information please refer to **Agent deployment conditions and settings** in the the **Deploy Agents** section.

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.



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

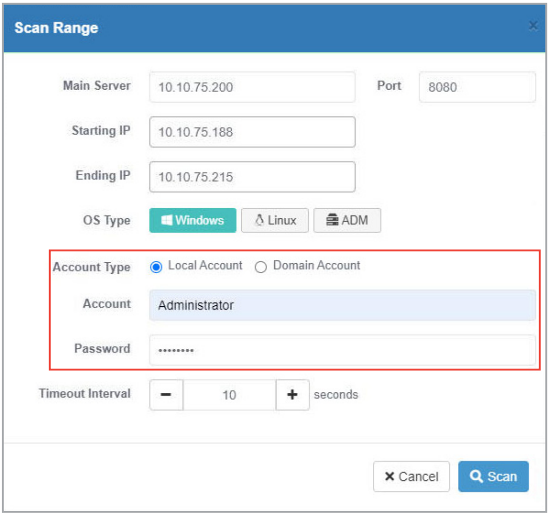
Account Administrator

Password ••••••••

Timeout Interval − 10 + seconds

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.

> 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.



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

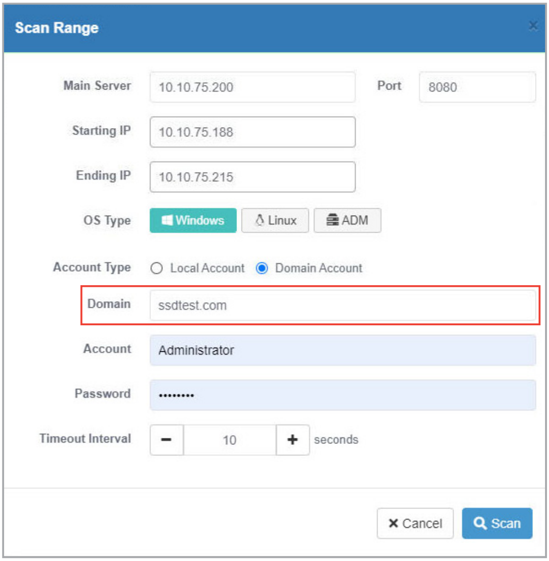
Account Type: ● Local Account ○ Domain Account

Account: Administrator

Password: ••••••••

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.



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

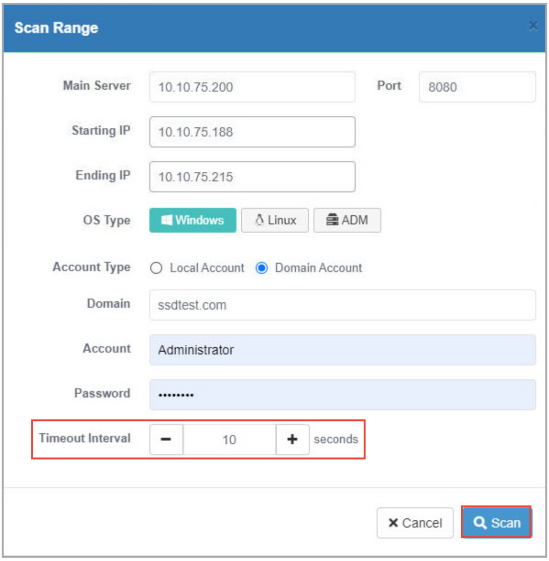
Domain: ssdtest.com

Account: Administrator

Password: ••••••••

Timeout Interval: − 10 + seconds

4. 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**.



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

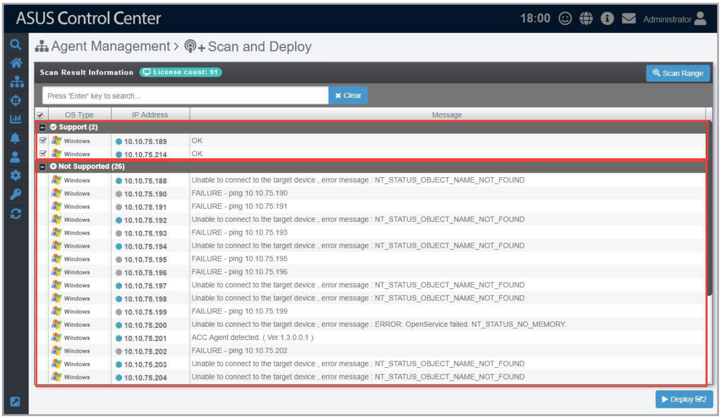
Domain: ssdtest.com

Account: Administrator

Password: ••••••••

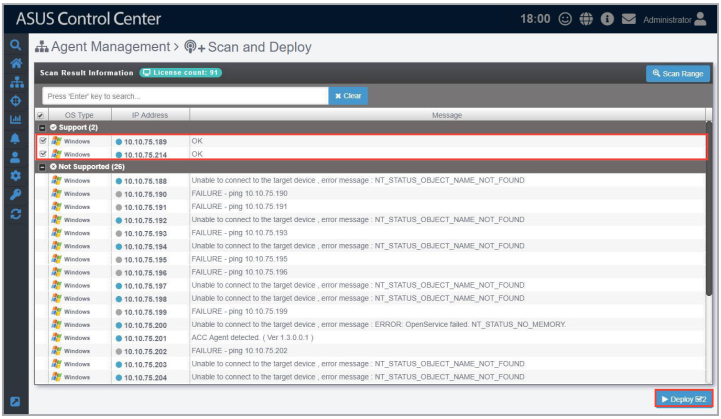
Timeout Interval: − 10 + seconds

5. 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.



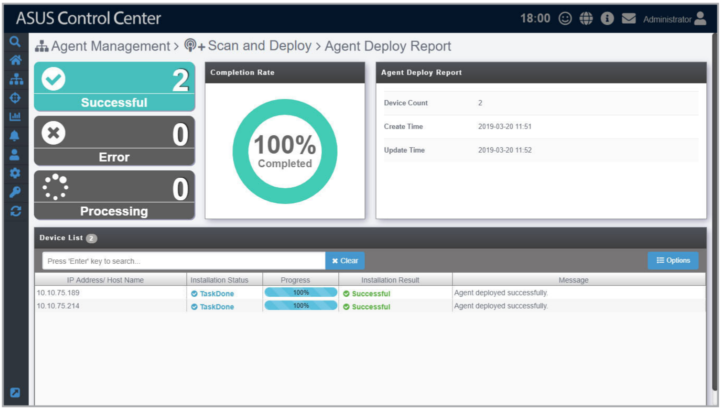
☑	OS Type	IP Address	Message
⊟	Support (2)		
☑	Windows	● 10.10.75.189	OK
☑	Windows	● 10.10.75.214	OK
⊟	Not Supported (26)		
	Windows	● 10.10.75.188	Unable to connect to the target device , error message : NT_STATUS_OBJECT_NAME_NOT_FOUND
	Windows	● 10.10.75.190	FAILURE - ping 10.10.75.190
	Windows	● 10.10.75.191	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**.



☑	OS Type	IP Address	Message
⊟	Support (2)		
☑	Windows	10.10.75.189	OK
☑	Windows	10.10.75.214	OK
⊟	Not Supported (26)		
	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

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.

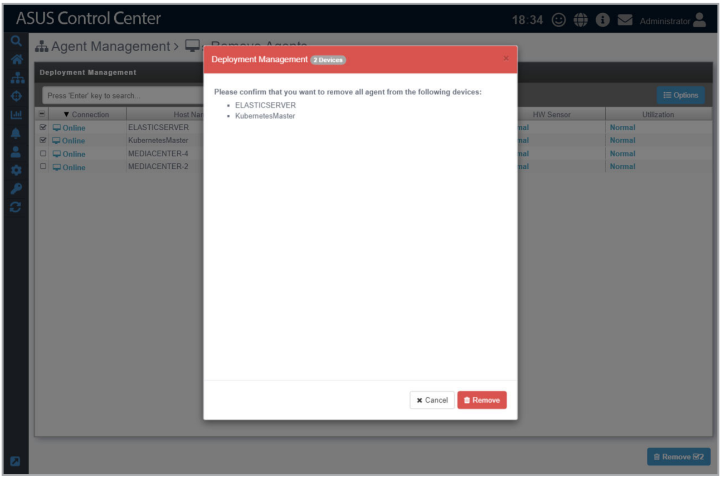


Device Count	2
Create Time	2019-03-20 11:51
Update Time	2019-03-20 11:52

IP Address/ Host Name	Installation Status	Progress	Installation Result	Message
10.10.75.189	TaskDone	100%	Successful	Agent deployed successfully.
10.10.75.214	TaskDone	100%	Successful	Agent deployed successfully.

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.

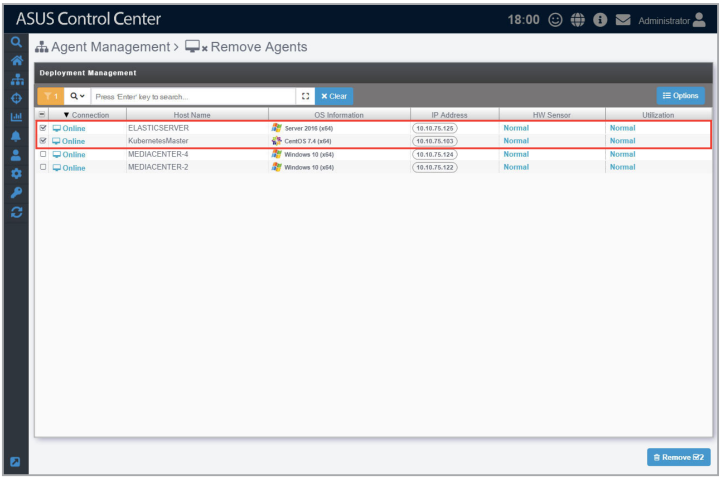


Please confirm that you want to remove all agent from the following devices:

- ELASTICSERVER
- KubernetesMaster

Remove agents using ASUS Control Center

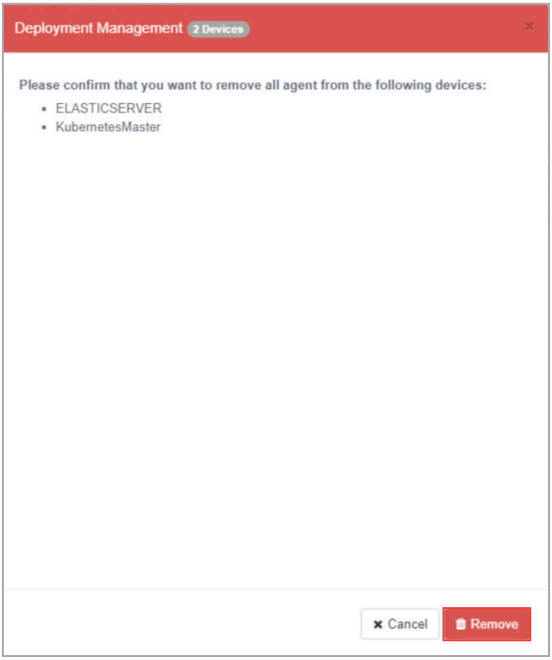
1. Check the devices you wish to remove agents from on the list.



	Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
☑	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	Normal
☑	Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103	Normal	Normal
□	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	Normal	Normal
□	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	Normal	Normal

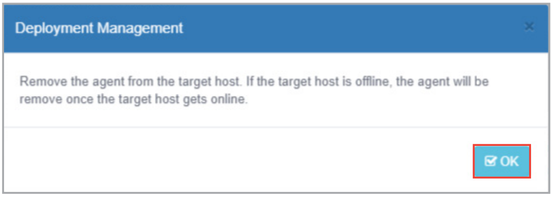
2. A pop-up window should appear, displaying the devices you wish to remove agents from. After confirming the correct managed devices are selected, click on **Remove**, then click on **OK**.

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



Please confirm that you want to remove all agent from the following devices:

- ELASTICSERVER
- KubernetesMaster

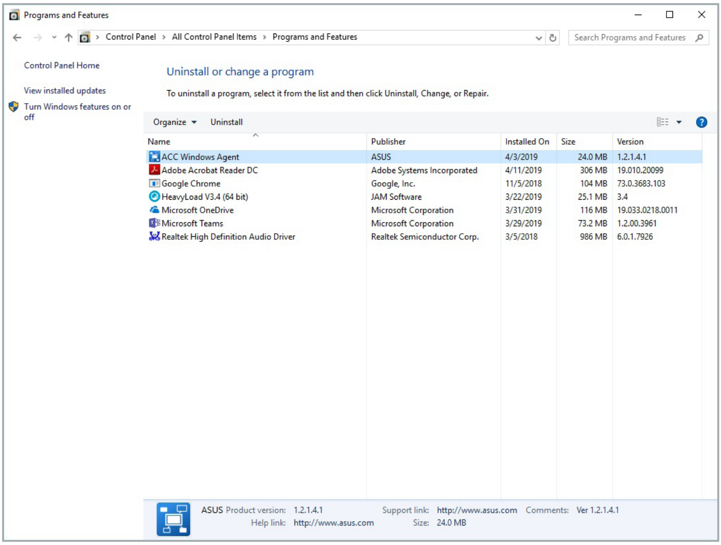


Remove the agent from the target host. If the target host is offline, the agent will be remove once the target host gets online.

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**.

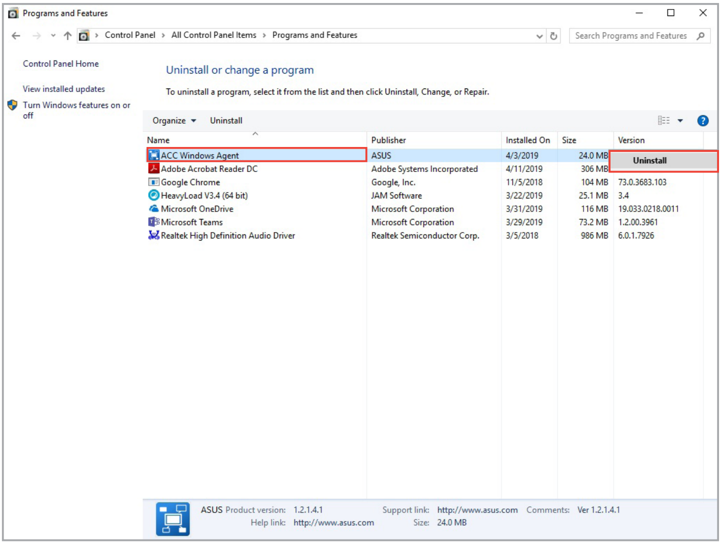

Programs and Features
Control Panel > All Control Panel Items > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
Organize
Uninstall

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
ACC Windows Agent	ASUS	4/3/2019	24.0 MB	1.2.1.4.1
Adobe Acrobat Reader DC	Adobe Systems Incorporated	4/11/2019	306 MB	19.010.20099
Google Chrome	Google, Inc.	11/5/2018	104 MB	73.0.3683.103
HeavyLoad V3.4 (64 bit)	JAM Software	3/22/2019	25.1 MB	3.4
Microsoft OneDrive	Microsoft Corporation	3/31/2019	116 MB	19.033.0218.0011
Microsoft Teams	Microsoft Corporation	3/29/2019	73.2 MB	1.2.00.3961
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	3/5/2018	986 MB	6.0.1.7926

ASUS Product version: 1.2.1.4.1 Support link: http://www.asus.com Comments: Ver 1.2.1.4.1
Help link: http://www.asus.com Size: 24.0 MB

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

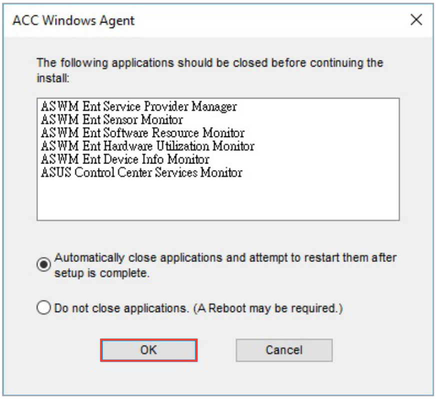

Programs and Features
Control Panel > All Control Panel Items > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
Organize
Uninstall
Uninstall

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
ACC Windows Agent	ASUS	4/3/2019	24.0 MB	
Adobe Acrobat Reader DC	Adobe Systems Incorporated	4/11/2019	306 MB	
Google Chrome	Google, Inc.	11/5/2018	104 MB	73.0.3683.103
HeavyLoad V3.4 (64 bit)	JAM Software	3/22/2019	25.1 MB	3.4
Microsoft OneDrive	Microsoft Corporation	3/31/2019	116 MB	19.033.0218.0011
Microsoft Teams	Microsoft Corporation	3/29/2019	73.2 MB	1.2.00.3961
Realtek High Definition Audio Driver	Realtek Semiconductor Corp.	3/5/2018	986 MB	6.0.1.7926

ASUS Product version: 1.2.1.4.1 Support link: http://www.asus.com Comments: Ver 1.2.1.4.1
Help link: http://www.asus.com Size: 24.0 MB

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.



ACC Windows Agent

The following applications should be closed before continuing the install:

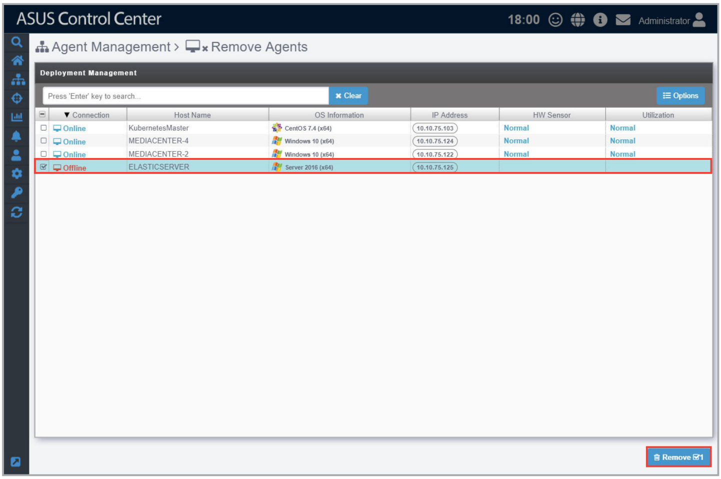
ASWM Ent Service Provider Manager
ASWM Ent Sensor Monitor
ASWM Ent Software Resource Monitor
ASWM Ent Hardware Utilization Monitor
ASWM Ent Device Info Monitor
ASUS Control Center Services Monitor

● Automatically close applications and attempt to restart them after setup is complete.

○ Do not close applications. (A Reboot may be required.)

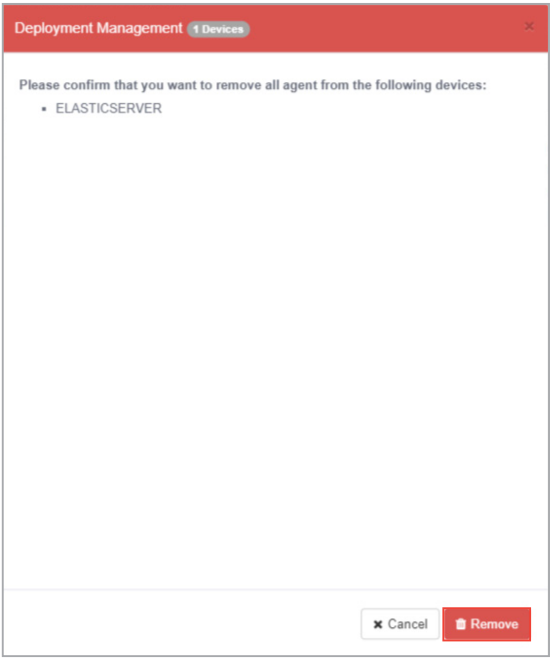
4. Once **ACC Windows Agent** is uninstalled on the managed device, please navigate to the **Remove Agents** menu of your ASUS Control Center (**Deployment** > **Agent Management** > **Remove Agents**).

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.



	▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
□	Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103	Normal	Normal
□	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	Normal	Normal
□	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	Normal	Normal
☑	Offline	ELASTICSERVER	Server 2016 (x64)	10.10.75.125		

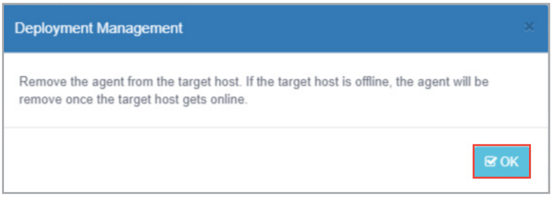
6. A pop-up window should appear, displaying the managed devices you wish to remove agents from. After confirming the correct devices are selected, click on **Remove**, then click on **OK**.



Deployment Management 1 Devices

Please confirm that you want to remove all agent from the following devices:

- ELASTICSERVER



Deployment Management

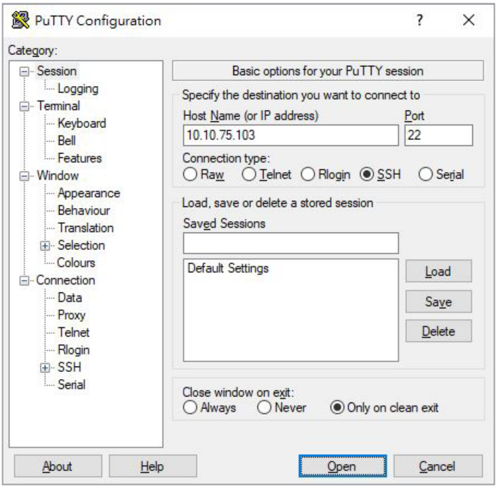
Remove the agent from the target host. If the target host is offline, the agent will be remove once the target host gets online.

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.

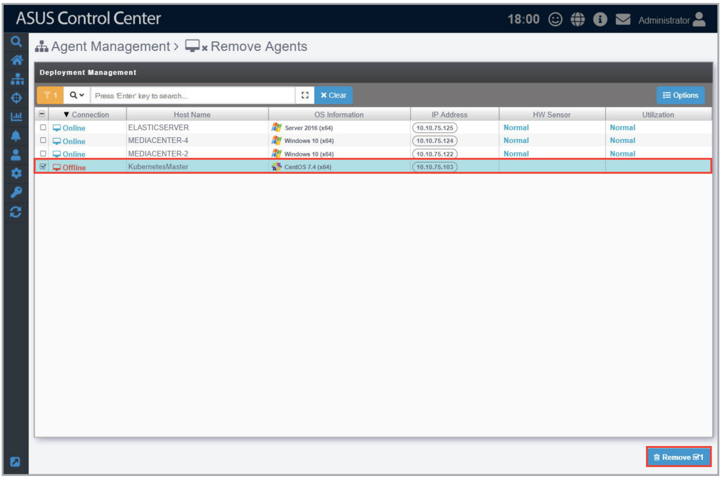
   For this example we will be using PuTTY to log on to the managed Linux device and remove the Linux Agent.



Host Name (or IP address): 10.10.75.103
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Saved Sessions: Default Settings
Close window on exit: ○ Always ○ Never ● Only on clean exit

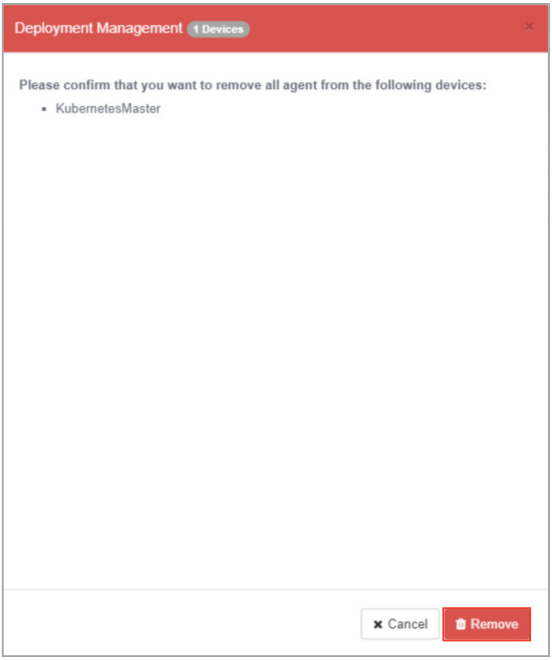
2. Enter the root account and password of the client Linux device.
3. Once you've logged in, execute `bash /root/uninstall.sh` to remove the Linux Agent from the managed device.
4. Once the Linux Agent is removed on the managed device, please navigate to the **Remove Agents** menu of your ASUS Control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



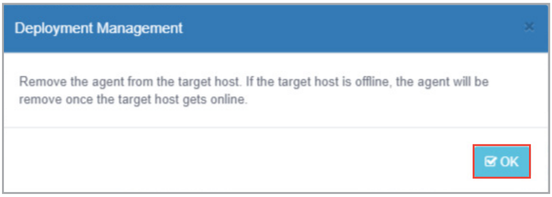
	Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
□	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	Normal
□	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	Normal	Normal
□	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	Normal	Normal
☑	Offline	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103		

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**.



Please confirm that you want to remove all agent from the following devices:

- KubernetesMaster



Remove the agent from the target host. If the target host is offline, the agent will be remove once the target host gets online.

3.1.4 Windows Agent

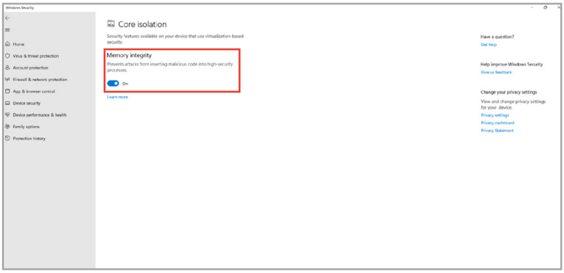
You may install agents manually on the device by downloading the Windows Agent installation files from the ASUS Control Center web console.

CSM products only supports Windows Agents.

The information entered in this section is for reference only.

Install Windows agents manually

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**.



Core isolation

Security features available on your device that use virtualization-based security.

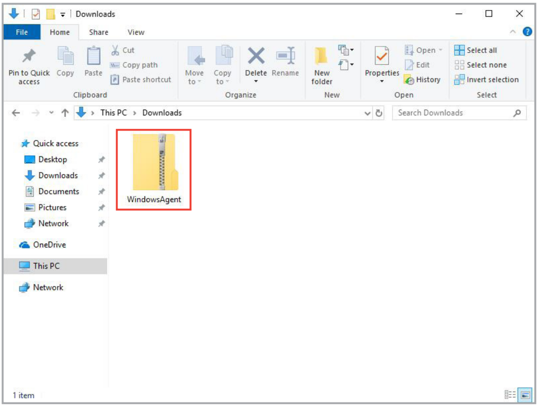
Memory integrity

Prevents attacks from inserting malicious code into high-security processes.

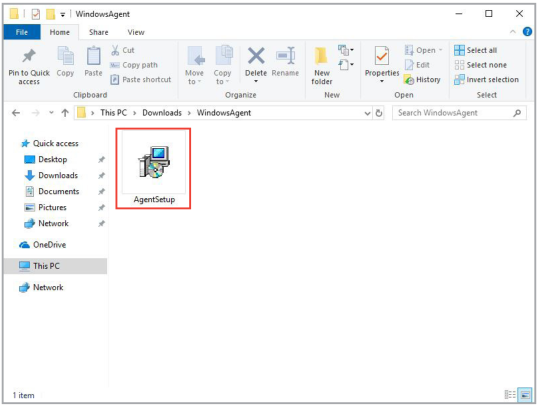
On

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.

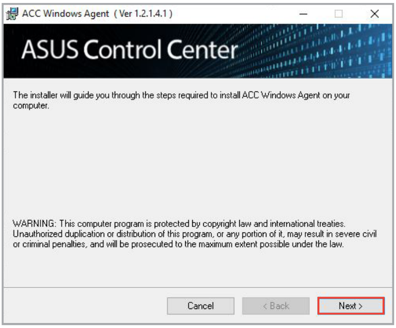
3. Unzip the ZIP file containing the installation files.



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



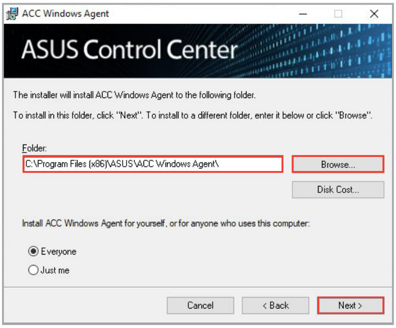
5. Click on **Next** to begin the installation.



The installer will guide you through the steps required to install ACC Windows Agent on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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



ACC Windows Agent

ASUS Control Center

The installer will install ACC Windows Agent to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\ASUS\ACC Windows Agent\

Browse...

Disk Cost...

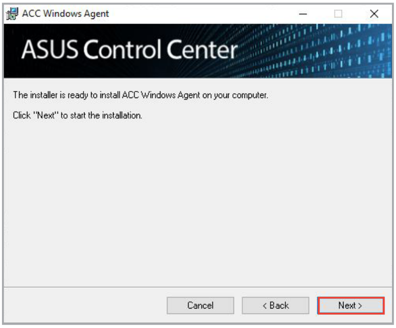
Install ACC Windows Agent for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

Cancel | < Back | Next >

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



ACC Windows Agent

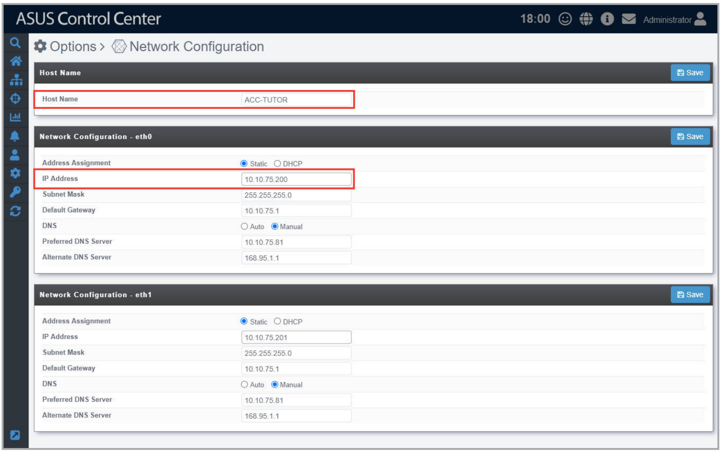
ASUS Control Center

The installer is ready to install ACC Windows Agent on your computer.

Click "Next" to start the installation.

Cancel | < Back | Next >

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



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

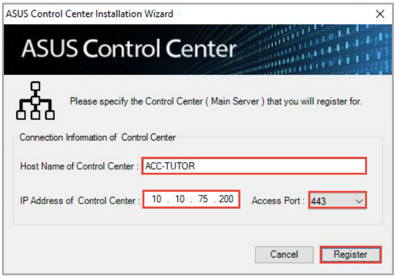
DNS: ○ Auto ● Manual

Preferred DNS Server: 10.10.75.81

Alternate DNS Server: 168.95.1.1

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**.

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


ASUS Control Center Installation Wizard

Please specify the Control Center (Main Server) that you will register for.

Connection Information of Control Center

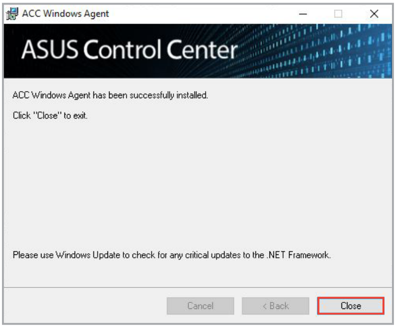
Host Name of Control Center : ACC-TUTOR

IP Address of Control Center : 10 . 10 . 75 . 200

Access Port : 443

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.

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


ACC Windows Agent

ACC Windows Agent has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

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.

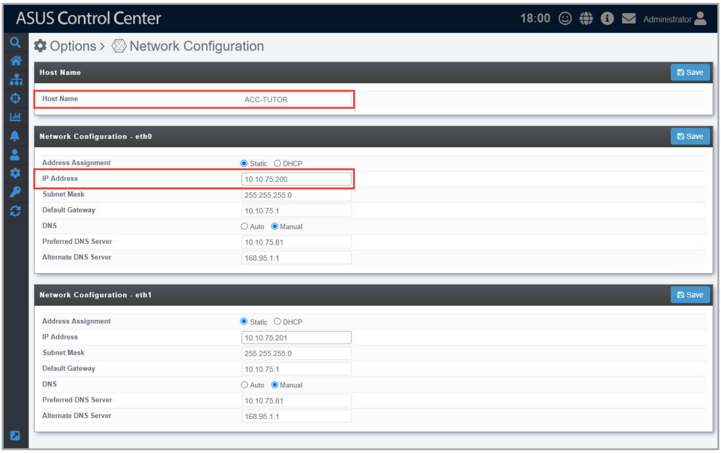
Install Linux agents manually

1. 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			

2. Click on **Linux Agent** to download Linux Agent installation files.

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



Host Name

Host Name: ACC-TUTOR

Network Configuration - eth0

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

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

4. On your client device, create the folder */tmp/ASWMAgentInstallFile*.

5. 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
     ```

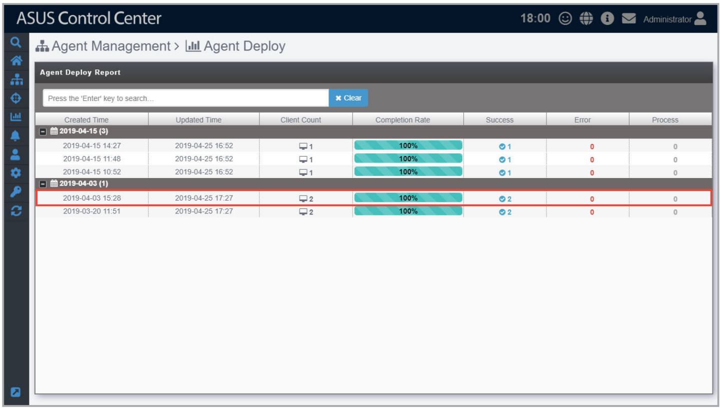
   - For Ubuntu, Debian, Pardus

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

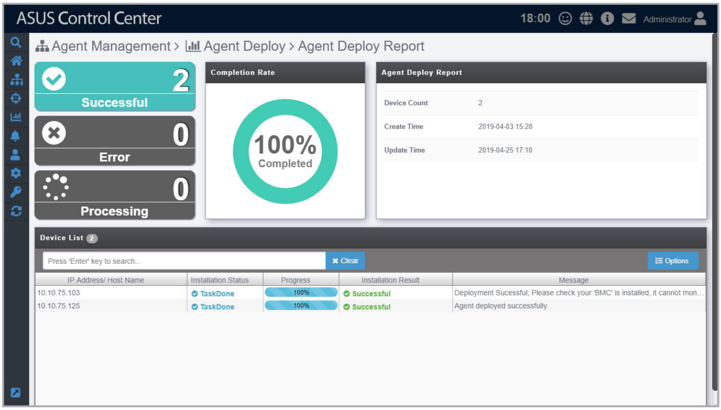
Please replace `XXX.XXX.XXX.XXX` with the actual IP of the ACC main server, for this example, it would be 10.10.75.200.

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...
✖ Clear

Created Time	Updated Time	Client Count	Completion Rate	Success	Error	Process
2019-04-15 (3)						
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



Device Count 2

Create Time 2019-04-03 15:28

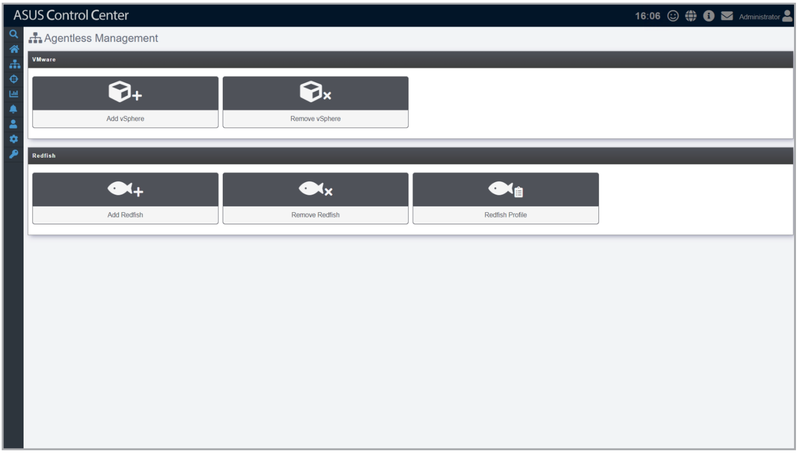
Update Time 2019-04-25 17:10

IP Address/ Host Name	Installation Status	Progress	Installation Result	Message
10.10.75.103	TaskDone	100%	Successful	Deployment Sucessful; Please check your 'BMC' is installed, it cannot mon...
10.10.75.125	TaskDone	100%	Successful	Agent deployed successfully.

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.

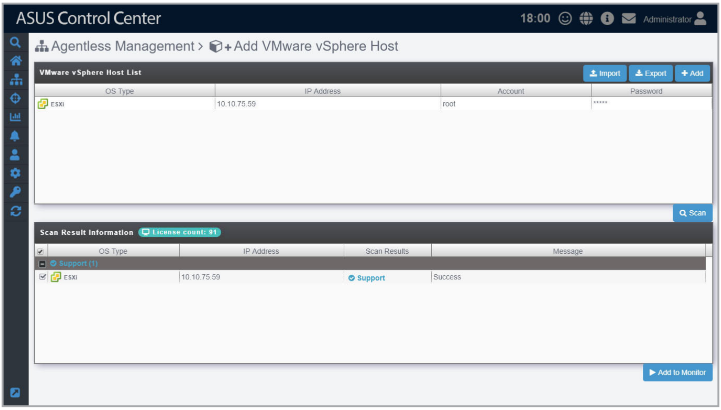


- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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.

> 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.



VMware vSphere Host List

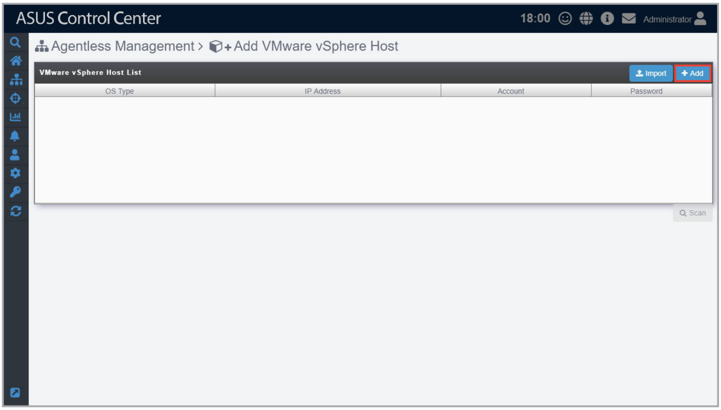
OS Type	IP Address	Account	Password
ESXi	10.10.75.59	root	*****

Scan Result Information License count: 91

☑	OS Type	IP Address	Scan Results	Message
⊟	Support (1)			
☑	ESXi	10.10.75.59	Support	Success

Adding managed vSphere

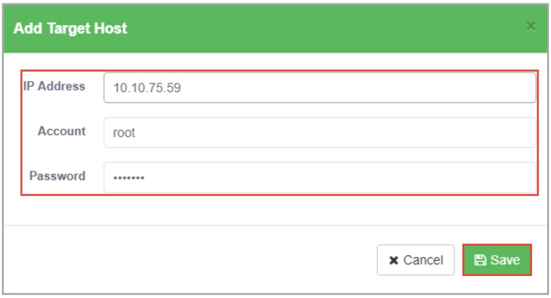
1. Click on **Add**.



VMware vSphere Host List

OS Type	IP Address	Account	Password

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

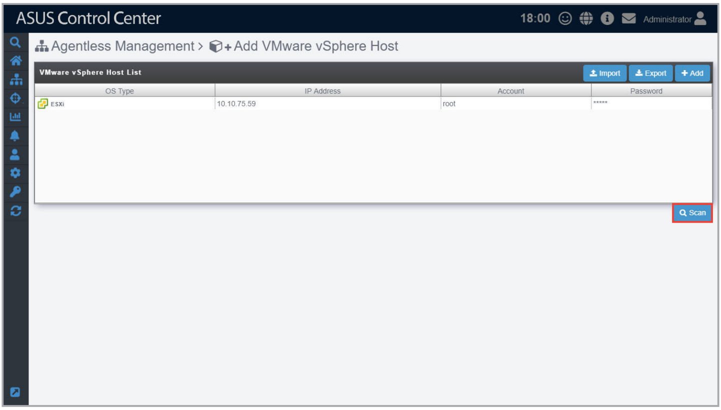


Add Target Host

IP Address	10.10.75.59
Account	root
Password	•••••••

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.

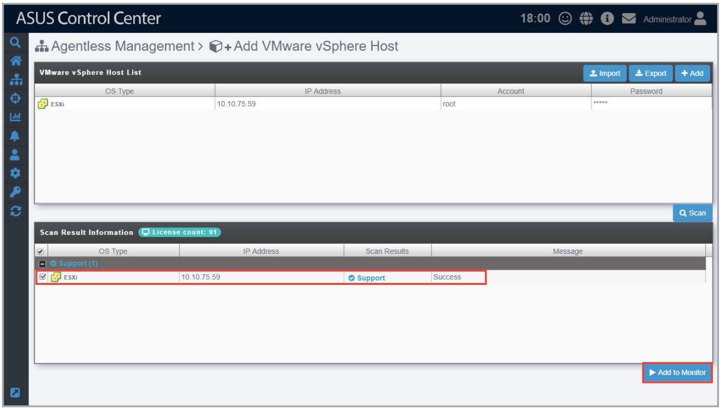
4. Once you have added all the vSpheres you wish to scan, click on **Scan**.



OS Type	IP Address	Account	Password
ESXi	10.10.75.59	root	*****

5. 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.

- 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.



Agentless Management > Add VMware vSphere Host

VMware vSphere Host List

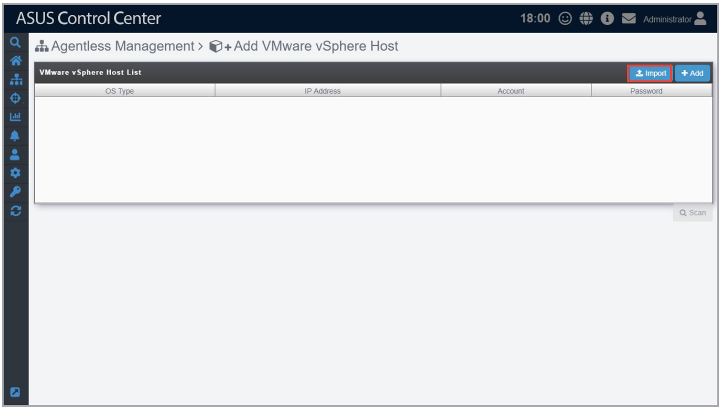
OS Type	IP Address	Account	Password
ESXi	10.10.75.59	root	*****

Scan Result Information License count: 91

☑	OS Type	IP Address	Scan Results	Message
⊟	Support (1)			
☑	ESXi	10.10.75.59	Support	Success

Add vSphere from CSV file

1. Click on **Import**.

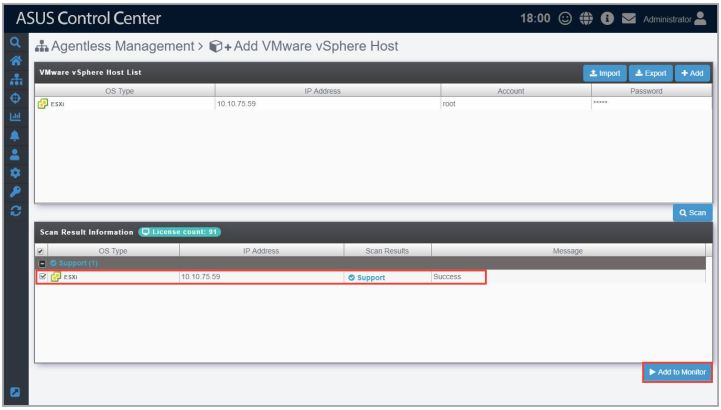


2. Select the CSV file to import and click **Open**.
3. Once the CSV file is successfully imported, click on **Scan**.

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.

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



VMware vSphere Host List

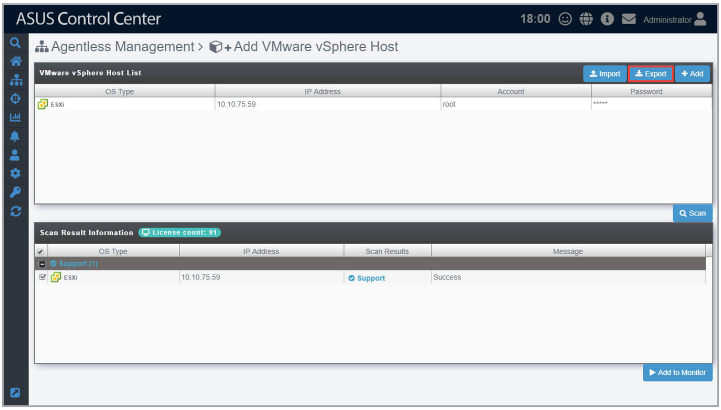
OS Type	IP Address	Account	Password
ESXi	10.10.75.59	root	*****

Scan Result Information License count: 91

☑	OS Type	IP Address	Scan Results	Message
⊟	Support (1)			
☑	ESXi	10.10.75.59	Support	Success

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.



VMware vSphere Host List

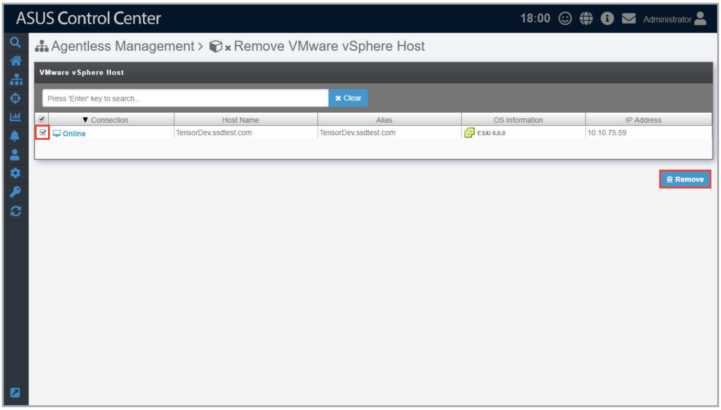
OS Type	IP Address	Account	Password
ESXi	10.10.75.59	root	*****

Scan Result Information License count: 91

☑	OS Type	IP Address	Scan Results	Message
⊟	Support (1)			
☑	ESXi	10.10.75.59	Support	Success

3.2.2 Remove vSphere

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



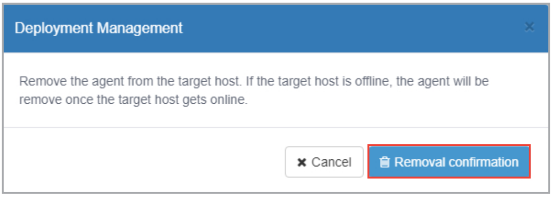
Agentless Management > Remove VMware vSphere Host

VMware vSphere Host

☑	▼ Connection	Host Name	Alias	OS Information	IP Address
☑	Online	TensorDev.ssdtest.com	TensorDev.ssdtest.com	ESXi 6.0.0	10.10.75.59

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

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



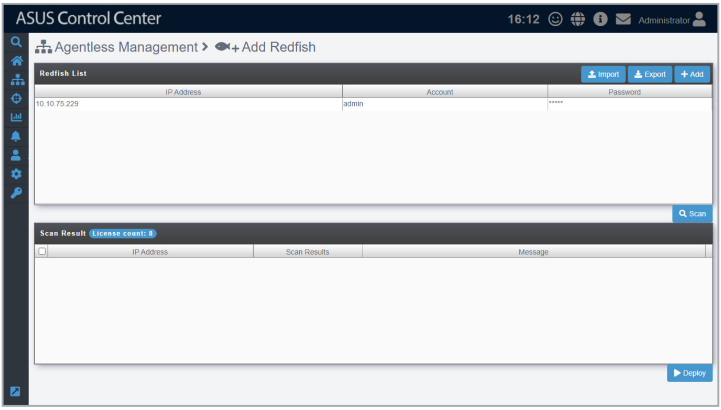
Deployment Management

Remove the agent from the target host. If the target host is offline, the agent will be remove once the target host gets 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.

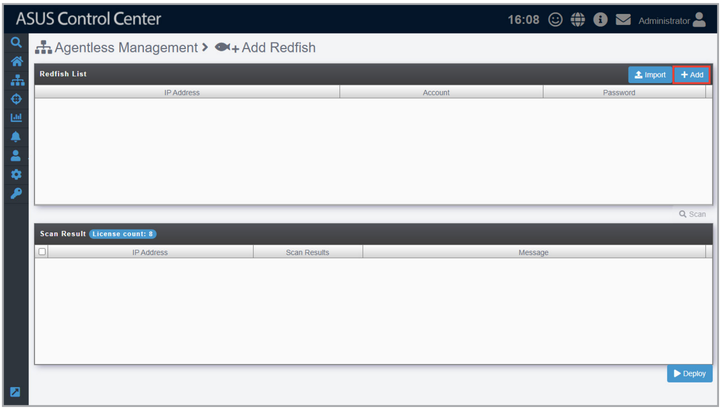
> Ensure to register the License keys before adding the Redfish device you wish to manage to ASUS Control Center. For more information on registering license keys, please refer to the **License** chapter.



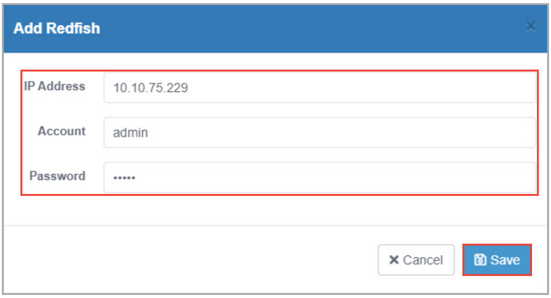
IP Address	Account	Password
10.10.75.229	admin	*****

Adding managed Redfish device

1. Click on **Add**.



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



Add Redfish

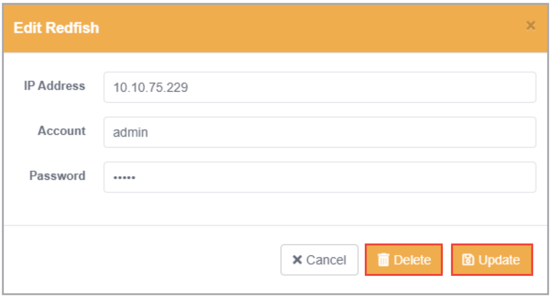
IP Address: 10.10.75.229

Account: admin

Password: •••••

3. Repeat steps 1 and 2 to add additional Redfish devicees 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**.



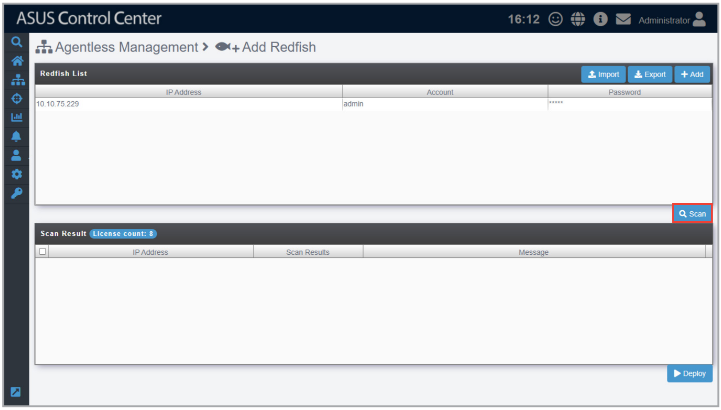
Edit Redfish

IP Address: 10.10.75.229

Account: admin

Password: •••••

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



ASUS Control Center 16:12 Administrator

Agentless Management > Add Redfish

Redfish List

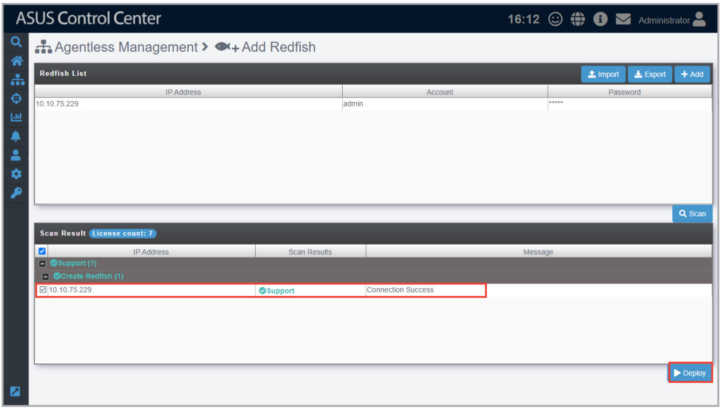
IP Address	Account	Password
10.10.75.229	admin	*****

Scan Result License count: 8

□	IP Address	Scan Results	Message

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

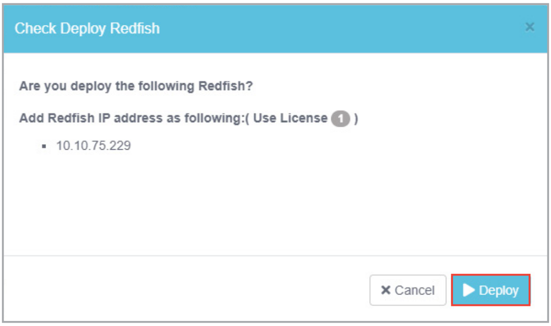
Unavailable Redfish devices will be listed as **Not Support**. You may click on the Redfish device to view details on why it is unavailable.



IP Address	Account	Password
10.10.75.229	admin	*****

☑	IP Address	Scan Results	Message
⊟	Support (1)		
⊟	Create Redfish (1)		
☑	10.10.75.229	Support	Connection Success

7. 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**.



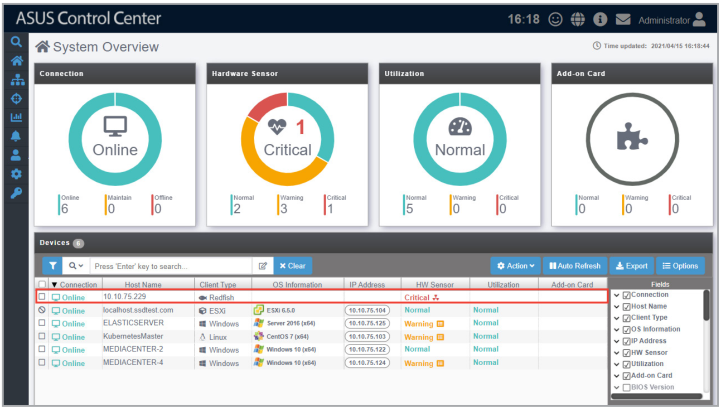
Are you deploy the following Redfish?

Add Redfish IP address as following:(Use License 1)

- 10.10.75.229

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

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

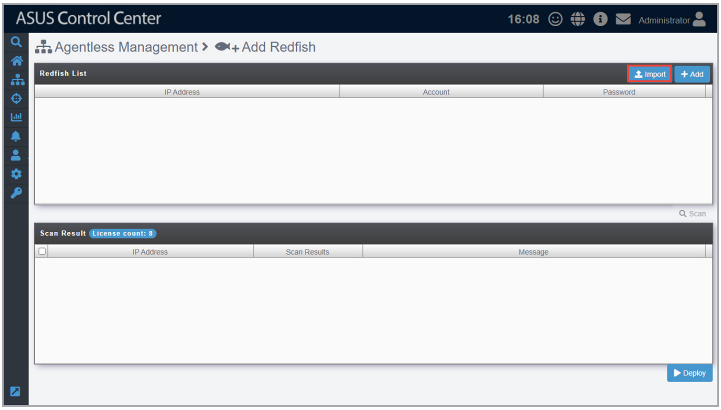


☐	▼ Connection	Host Name	Client Type	OS Information	IP Address	HW Sensor	Utilization	Add-on Card
☐	Online	10.10.75.229	Redfish			Critical		
⊘	Online	localhost.ssdtest.com	ESXi	ESXi 6.5.0	10.10.75.104	Normal	Normal	
☐	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.75.125	Warning	Normal	
☐	Online	KubernetesMaster	Linux	CentOS 7 (x64)	10.10.75.103	Warning	Normal	
☐	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.75.122	Normal	Normal	
☐	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.75.124	Warning	Normal	

Fields
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- ☑ HW Sensor
- ☑ Utilization
- ☑ Add-on Card
- ☐ BIOS Version

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**.

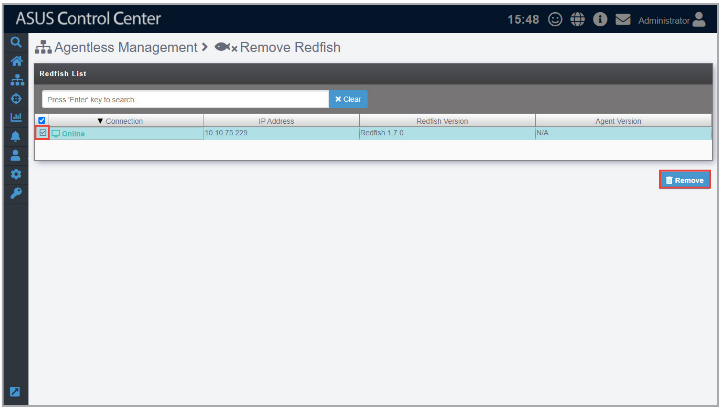
You may edit items added by clicking on it before scanning.

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.

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**.

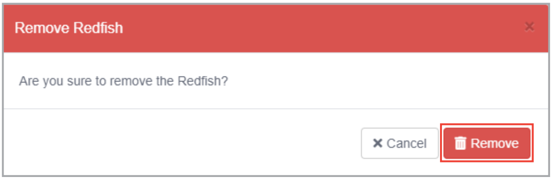


ASUS Control Center
15:48
Administrator
Agentless Management > Remove Redfish
Redfish List
Press 'Enter' key to search...
Clear
Remove

☑	Connection	IP Address	Redfish Version	Agent Version
☑	Online	10.10.75.229	Redfish 1.7.0	N/A

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

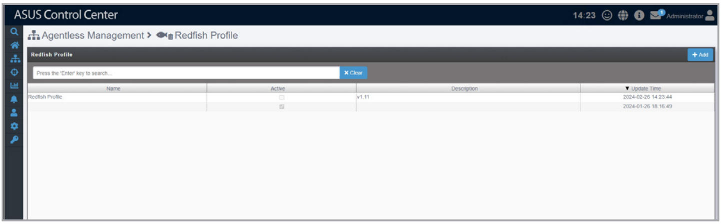
If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.



Are you sure to remove the Redfish?

3.2.5 Redfish Profile

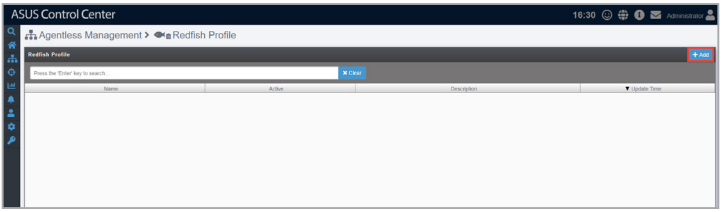
The **Redfish Profile** function allows you to add, edit, or delete Redfish profiles.


ASUS Control Center
14:23
Administrator
Agentless Management > Redfish Profile
Redfish Profile
+ Add
Press the 'Enter' key to search...
✖ Clear

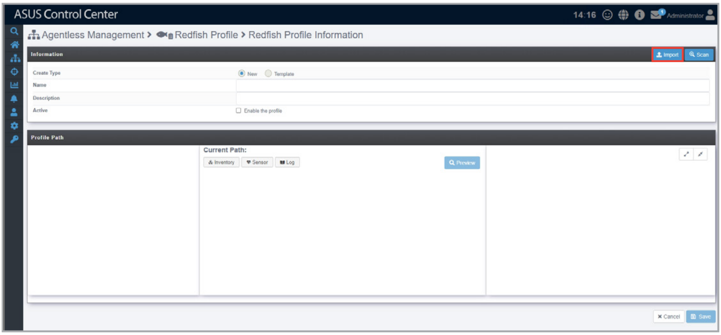
Name	Active	▼ Update Time	Description
Redfish Profile	☐	v1.11	2024-02-26 14:23:44
	☑		2024-01-26 18:16:49

Adding a Redfish profile by importing a profile file

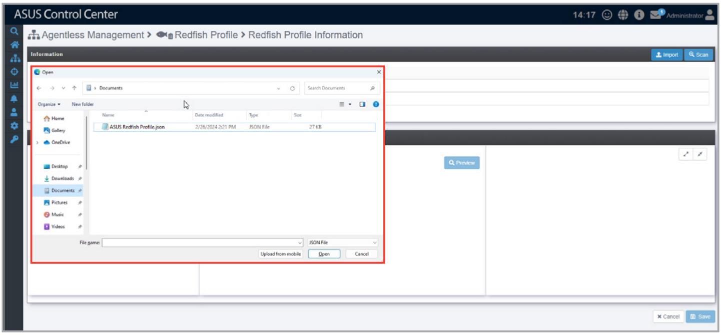
1. Click **Add**.



2. Click **Import**.

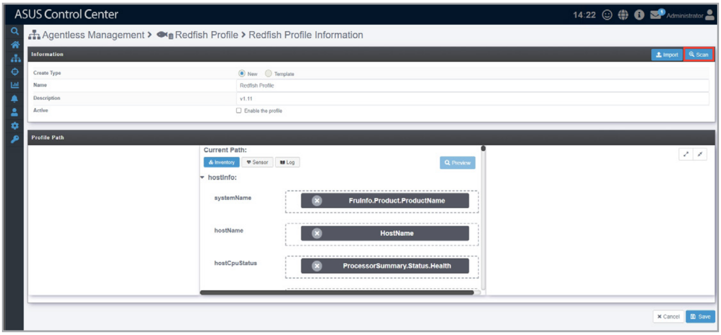


3. Select a Redfish profile JSON file, then click **Open**.



Name	Date modified	Type	Size
ASUS Redfish Profile.json	2/26/2024 2:21 PM	JSON File	27 KB

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

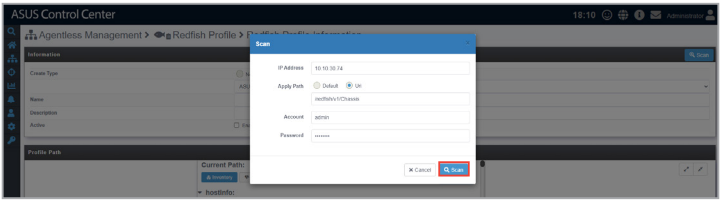


Create Type ● New ○ Template
Name Redfish Profile
Description v1.11
Active □ Enable the profile

hostInfo:
systemName FruInfo.Product.ProductName
hostName HostName
hostCpuStatus ProcessorSummary.Status.Health

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

> 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.



Scan

IP Address: 10.10.30.74

Apply Path: ○ Default ● Uri

/redfish/v1/Chassis

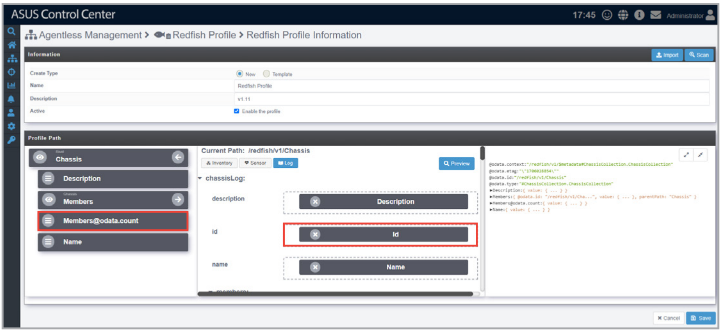
Account: admin

Password: ••••••••

✕ Cancel | Scan

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.



Create Type: ● New ○ Template

Name: Redfish Profile

Description: v1.11

Active: ☑ Enable the profile

Current Path: /redfish/v1/Chassis

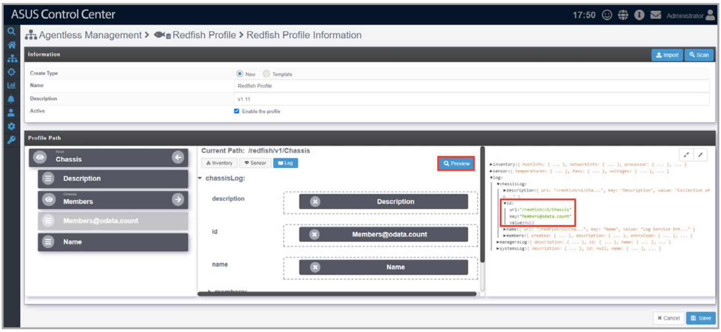
description: Description

id: Id

name: Name

```
@odata.context:"/redfish/v1/$metadata#ChassisCollection.ChassisCollection"
@odata.etag:"\"1706028854\""
@odata.id:"/redfish/v1/Chassis"
@odata.type:"#ChassisCollection.ChassisCollection"
▶Description:{ value: { ... } }
▶Members:{ @odata.id: "/redfish/v1/Cha...", value: { ... }, parentPath: "Chassis" }
▶Members@odata.count:{ value: { ... } }
▶Name:{ value: { ... } }
```

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



Create Type: ● New ○ Template

Name: Redfish Profile

Description: v1.11

Active: ☑ Enable the profile

Current Path: /redfish/v1/Chassis

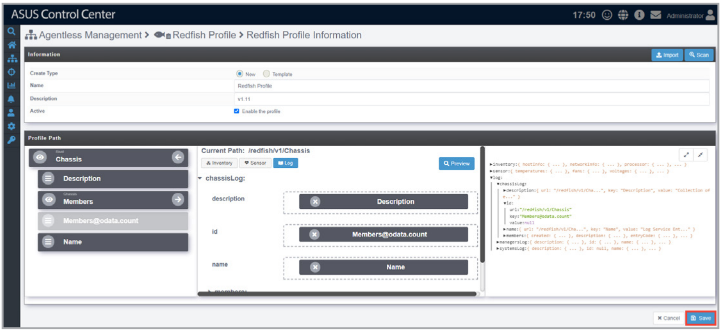
description: Description

id: Members@odata.count

name: Name

```
▶inventory:{ hostInfo: { ... }, networkInfo: { ... }, processor: { ... }, ... }
▶sensor:{ temperatures: { ... }, fans: { ... }, voltages: { ... }, ... }
▼log:
  ▼chassisLog:
    ▶description:{ url: "/redfish/v1/Cha...", key: "Description", value: "Collection of
e..." }
    ▼id:
      url:"/redfish/v1/Chassis"
      key:"Members@odata.count"
      value:null
    ▶name:{ url: "/redfish/v1/Cha...", key: "Name", value: "Log Service Ent..." }
    ▶members:{ created: { ... }, description: { ... }, entryCode: { ... }, ... }
  ▶managersLog:{ description: { ... }, id: { ... }, name: { ... }, ... }
  ▶systemsLog:{ description: { ... }, id: null, name: { ... }, ... }
```

7. Click **Save**.



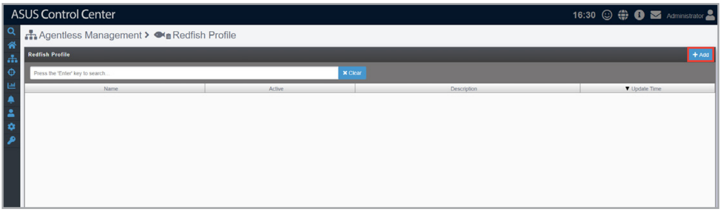
Create Type	● New ○ Template
Name	Redfish Profile
Description	v1.11
Active	☑ Enable the profile

Current Path: /redfish/v1/Chassis

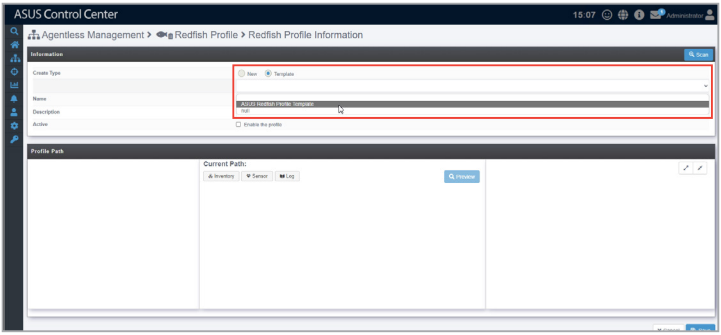
```
▸inventory:{ hostInfo: { ... }, networkInfo: { ... }, processor: { ... }, ... }
▸sensor:{ temperatures: { ... }, fans: { ... }, voltages: { ... }, ... }
▾log:
  ▾chassisLog:
    ▸description:{ url: "/redfish/v1/Cha...", key: "Description", value: "Collection of
    e..." }
    ▾id:
      url:"/redfish/v1/Chassis"
      key:"Members@odata.count"
      value:null
    ▸name:{ url: "/redfish/v1/Cha...", key: "Name", value: "Log Service Ent..." }
    ▸members:{ created: { ... }, description: { ... }, entryCode: { ... }, ... }
  ▸managersLog:{ description: { ... }, id: { ... }, name: { ... }, ... }
  ▸systemsLog:{ description: { ... }, id: null, name: { ... }, ... }
```

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.



Create Type: ○ New ● Template

ASUS Redfish Profile Template

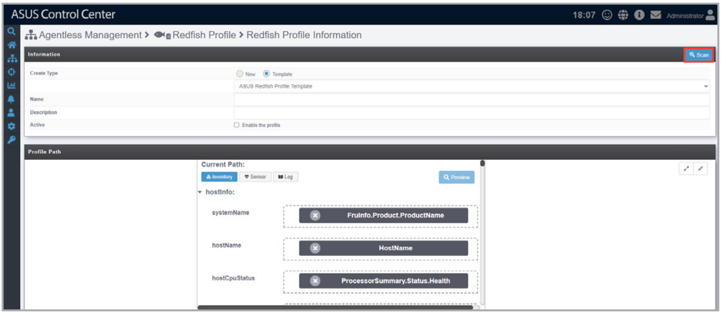
null

Name

Description

Active: □ Enable the profile

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



Create Type: ○ New ● Template

ASUS Redfish Profile Template

Name

Description

Active: □ Enable the profile

hostInfo:

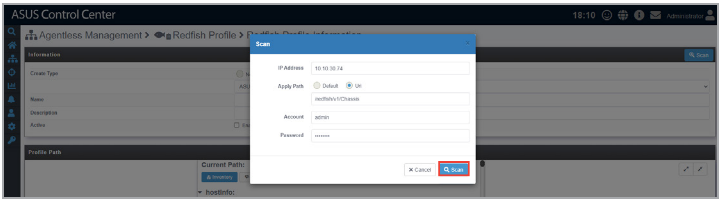
systemName FruInfo.Product.ProductName

hostName HostName

hostCpuStatus ProcessorSummary.Status.Health

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

> 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.



Scan

IP Address: 10.10.30.74

Apply Path: ○ Default ● Uri

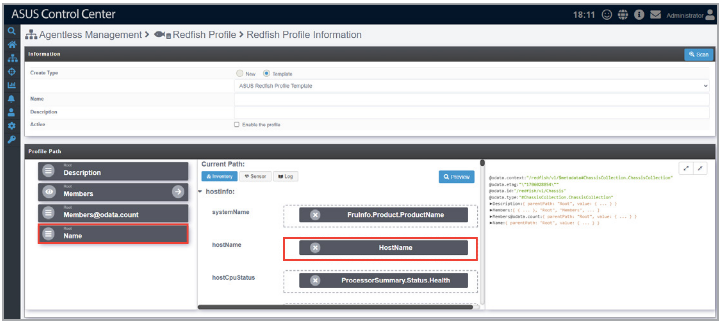
/redfish/v1/Chassis

Account: admin

Password: ••••••••

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.



Create Type: ○ New ● Template

ASUS Redfish Profile Template

Name:

Description:

Active: □ Enable the profile

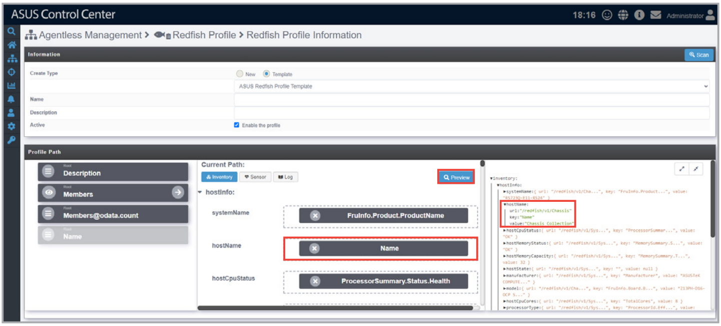
systemName: FruInfo.Product.ProductName

hostName: HostName

hostCpuStatus: ProcessorSummary.Status.Health

```
@odata.context:"/redfish/v1/$metadata#ChassisCollection.ChassisCollection"
@odata.etag:"\"1706028854\""
@odata.id:"/redfish/v1/Chassis"
@odata.type:"#ChassisCollection.ChassisCollection"
▶Description:{ parentPath: "Root", value: { ... } }
▶Members:[ { ... }, "Root", "Members", ... ]
▶Members@odata.count:{ parentPath: "Root", value: { ... } }
▶Name:{ parentPath: "Root", value: { ... } }
```

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



Create Type: ○ New ● Template

ASUS Redfish Profile Template

Name:

Description:

Active: ☑ Enable the profile

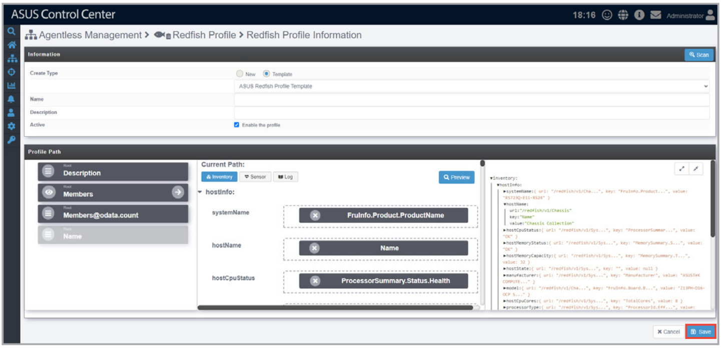
systemName: FruInfo.Product.ProductName

hostName: Name

hostCpuStatus: ProcessorSummary.Status.Health

```
▼inventory:
  ▼hostInfo:
    ▶systemName:{ url: "/redfish/v1/Cha...", key: "FruInfo.Product...", value:
    "RS723Q-E11-RS24" }
    ▼hostName:
      url:"/redfish/v1/Chassis"
      key:"Name"
      value:"Chassis Collection"
    ▶hostCpuStatus:{ url: "/redfish/v1/Sys...", key: "ProcessorSummar...", value:
    "OK" }
    ▶hostMemoryStatus:{ url: "/redfish/v1/Sys...", key: "MemorySummary.S...", value:
    "OK" }
    ▶hostMemoryCapacity:{ url: "/redfish/v1/Sys...", key: "MemorySummary.T...",
    value: 32 }
    ▶hostState:{ url: "/redfish/v1/Sys...", key: "", value: null }
    ▶manufacturer:{ url: "/redfish/v1/Sys...", key: "Manufacturer", value: "ASUSTeK
    COMPUTE..." }
    ▶model:{ url: "/redfish/v1/Cha...", key: "FruInfo.Board.B...", value: "Z13PH-D16-
    OCP S..." }
    ▶hostCpuCores:{ url: "/redfish/v1/Sys...", key: "TotalCores", value: 8 }
    ▶processorType:{ url: "/redfish/v1/Sys...", key: "ProcessorId.Eff...", value:
```

6. Click **Save**.



ASUS Control Center
18:16
Administrator
Agentless Management > Redfish Profile > Redfish Profile Information
Information
Scan

Create Type: ○ New ● Template

ASUS Redfish Profile Template

Name:

Description:

Active: ☑ Enable the profile

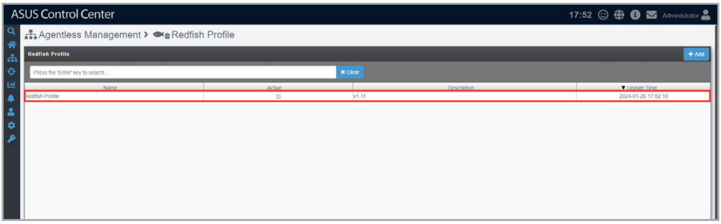
hostInfo:

systemName	FruInfo.Product.ProductName
hostName	Name
hostCpuStatus	ProcessorSummary.Status.Health

```
▾inventory:
  ▾hostInfo:
    ▸systemName:{ url: "/redfish/v1/Cha...", key: "FruInfo.Product...", value:
    "RS723Q-E11-RS24" }
    ▾hostName:
      url:"/redfish/v1/Chassis"
      key:"Name"
      value:"Chassis Collection"
    ▸hostCpuStatus:{ url: "/redfish/v1/Sys...", key: "ProcessorSummar...", value:
    "OK" }
    ▸hostMemoryStatus:{ url: "/redfish/v1/Sys...", key: "MemorySummary.S...", value:
    "OK" }
    ▸hostMemoryCapacity:{ url: "/redfish/v1/Sys...", key: "MemorySummary.T...",
    value: 32 }
    ▸hostState:{ url: "/redfish/v1/Sys...", key: "", value: null }
    ▸manufacturer:{ url: "/redfish/v1/Sys...", key: "Manufacturer", value: "ASUSTeK
    COMPUTE..." }
    ▸model:{ url: "/redfish/v1/Cha...", key: "FruInfo.Board.B...", value: "Z13PH-D16-
    OCP S..." }
    ▸hostCpuCores:{ url: "/redfish/v1/Sys...", key: "TotalCores", value: 8 }
    ▸processorType:{ url: "/redfish/v1/Sys...", key: "ProcessorId.Eff...", value:
```

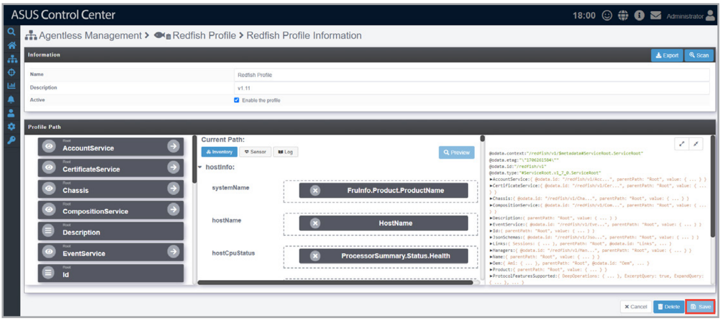
Editing an existing Redfish profile

1. Select an existing Redfish profile.


ASUS Control Center
17:52
Administrator
Agentless Management > Redfish Profile
Redfish Profile
+ Add
Press the 'Enter' key to search...
✖ Clear

Name	Active	Description	▼ Update Time
Redfish Profile	☑	v1.11	2024-01-26 17:52:10

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



Name: Redfish Profile
Description: v1.11
Active: ☑ Enable the profile

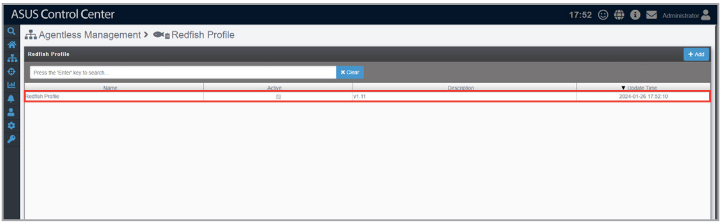
hostInfo:

systemName: FruInfo.Product.ProductName
hostName: HostName
hostCpuStatus: ProcessorSummary.Status.Health

```
@odata.context:"/redfish/v1/$metadata#ServiceRoot.ServiceRoot"
@odata.etag:"\"1706261584\""
@odata.id:"/redfish/v1"
@odata.type:"#ServiceRoot.v1_7_0.ServiceRoot"
▸AccountService:{ @odata.id: "/redfish/v1/Acc...", parentPath: "Root", value: { ... } }
▸CertificateService:{ @odata.id: "/redfish/v1/Cer...", parentPath: "Root", value: { ...
} }
▸Chassis:{ @odata.id: "/redfish/v1/Cha...", parentPath: "Root", value: { ... } }
▸CompositionService:{ @odata.id: "/redfish/v1/Com...", parentPath: "Root", value: { ...
} }
▸Description:{ parentPath: "Root", value: { ... } }
▸EventService:{ @odata.id: "/redfish/v1/Eve...", parentPath: "Root", value: { ... } }
▸Id:{ parentPath: "Root", value: { ... } }
▸JsonSchemas:{ @odata.id: "/redfish/v1/Jso...", parentPath: "Root", value: { ... } }
▸Links:{ Sessions: { ... }, parentPath: "Root", @odata.id: "Links", ... }
▸Managers:{ @odata.id: "/redfish/v1/Man...", parentPath: "Root", value: { ... } }
▸Name:{ parentPath: "Root", value: { ... } }
▸Oem:{ Ami: { ... }, parentPath: "Root", @odata.id: "Oem", ... }
▸Product:{ parentPath: "Root", value: { ... } }
▸ProtocolFeaturesSupported:{ DeepOperations: { ... }, ExcerptQuery: true, ExpandQuery:
{ ... }, ... }
```

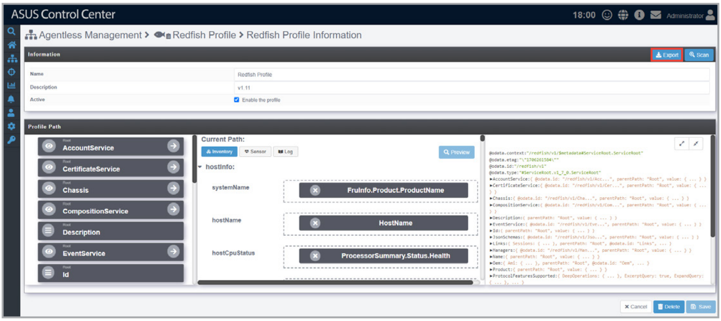
Exporting an existing Redfish profile

1. Select an existing Redfish profile.


ASUS Control Center
17:52
Administrator
Agentless Management > Redfish Profile
Redfish Profile
+ Add
Press the 'Enter' key to search...
✖ Clear

Name	Active	Description	▼ Update Time
Redfish Profile	□	v1.11	2024-01-26 17:52:10

2. Click **Export**.

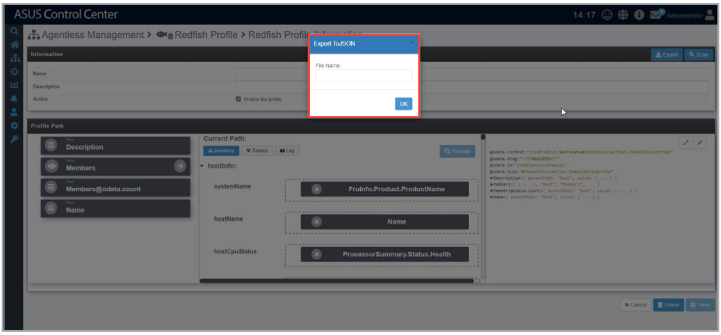


Name: Redfish Profile

Description: v1.11

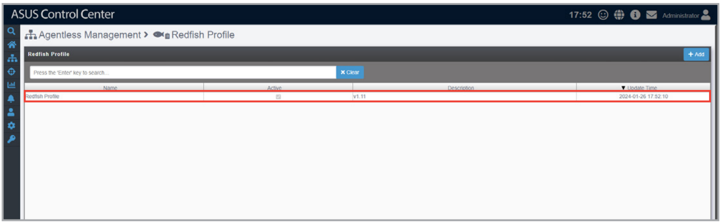
Active: ☑ Enable the profile

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



Deleting an existing Redfish profile

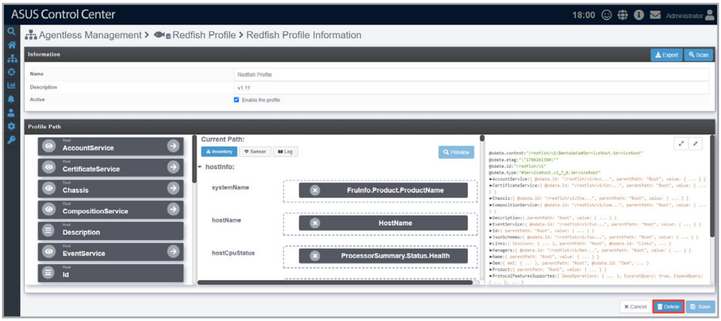
1. Select an existing Redfish profile.



ASUS Control Center
17:52
Administrator
Agentless Management > Redfish Profile
Redfish Profile
+ Add
Press the 'Enter' key to search...
✖ Clear

Name	Active	Description	▼ Update Time
Redfish Profile	☐	v1.11	2024-01-26 17:52:10

2. Click **Delete**.



Name	Redfish Profile
Description	v1.11
Active	☑ Enable the profile

```
@odata.context:"/redfish/v1/$metadata#ServiceRoot.ServiceRoot"
@odata.etag:"\"1706261584\""
@odata.id:"/redfish/v1"
@odata.type:"#ServiceRoot.v1_7_0.ServiceRoot"
▶AccountService:{ @odata.id: "/redfish/v1/Acc...", parentPath: "Root", value: { ... } }
▶CertificateService:{ @odata.id: "/redfish/v1/Cer...", parentPath: "Root", value: { ...
} }
▶Chassis:{ @odata.id: "/redfish/v1/Cha...", parentPath: "Root", value: { ... } }
▶CompositionService:{ @odata.id: "/redfish/v1/Com...", parentPath: "Root", value: { ...
} }
▶Description:{ parentPath: "Root", value: { ... } }
▶EventService:{ @odata.id: "/redfish/v1/Eve...", parentPath: "Root", value: { ... } }
▶Id:{ parentPath: "Root", value: { ... } }
▶JsonSchemas:{ @odata.id: "/redfish/v1/Jso...", parentPath: "Root", value: { ... } }
▶Links:{ Sessions: { ... }, parentPath: "Root", @odata.id: "Links", ... }
▶Managers:{ @odata.id: "/redfish/v1/Man...", parentPath: "Root", value: { ... } }
▶Name:{ parentPath: "Root", value: { ... } }
▶Oem:{ Ami: { ... }, parentPath: "Root", @odata.id: "Oem", ... }
▶Product:{ parentPath: "Root", value: { ... } }
▶ProtocolFeaturesSupported:{ DeepOperations: { ... }, ExcerptQuery: true, ExpandQuery:
{ ... }, ... }
```

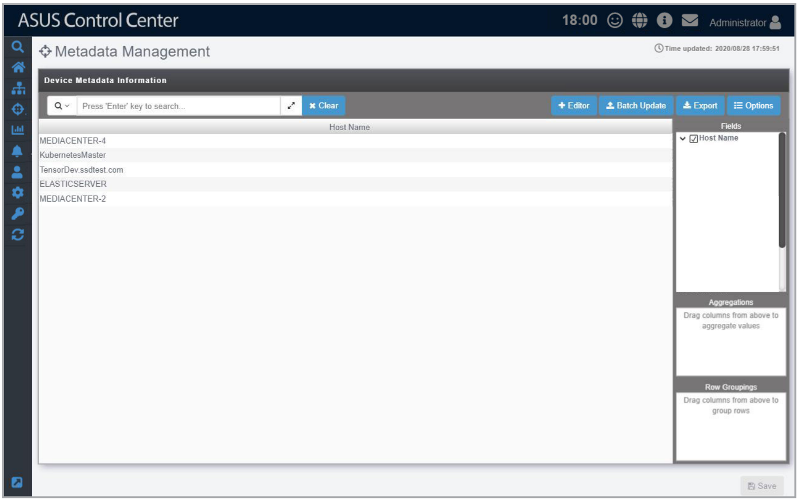
Chapter 4

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

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.



ASUS Control Center
18:00
Administrator
Metadata Management
Time updated: 2020/08/28 17:59:51
Device Metadata Information
Press 'Enter' key to search...
Clear
Editor
Batch Update
Export
Options
Fields
☑ Host Name
Aggregations
Drag columns from above to aggregate values
Row Groupings
Drag columns from above to group rows
Save

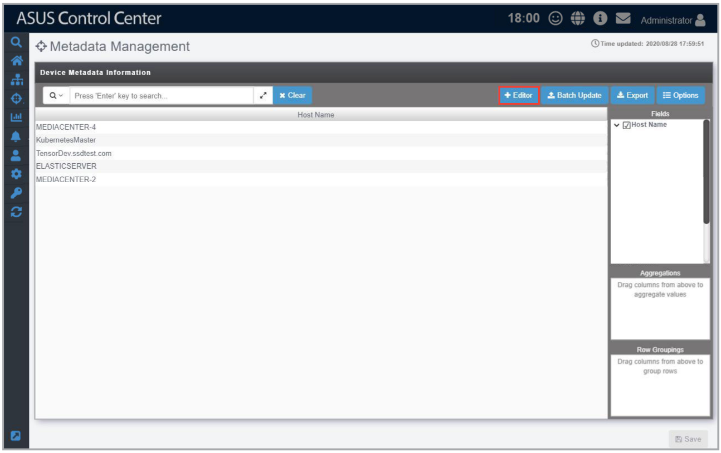
Host Name
MEDIACENTER-4
KubernetesMaster
TensorDev.ssdtest.com
ELASTICSERVER
MEDIACENTER-2

- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

Adding metadata fields

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

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

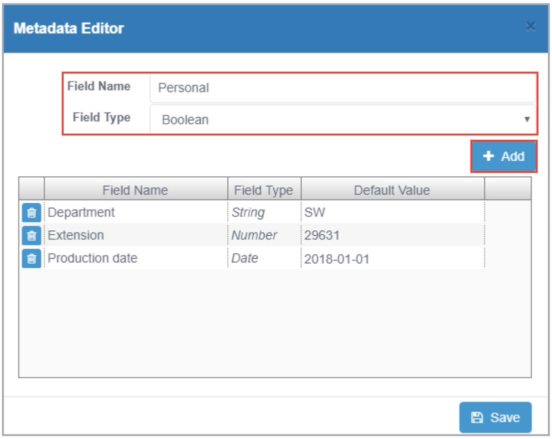

ASUS Control Center
18:00
Administrator
Metadata Management
Time updated: 2020/08/28 17:59:51
Device Metadata Information
Press 'Enter' key to search...
Clear
Editor
Batch Update
Export
Options
Fields
Host Name
Aggregations
Drag columns from above to aggregate values
Row Groupings
Drag columns from above to group rows
Save

Host Name
MEDIACENTER-4
KubernetesMaster
TensorDev.ssdtest.com
ELASTICSERVER
MEDIACENTER-2

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

- **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.

3. Click on **Add** to add the field.



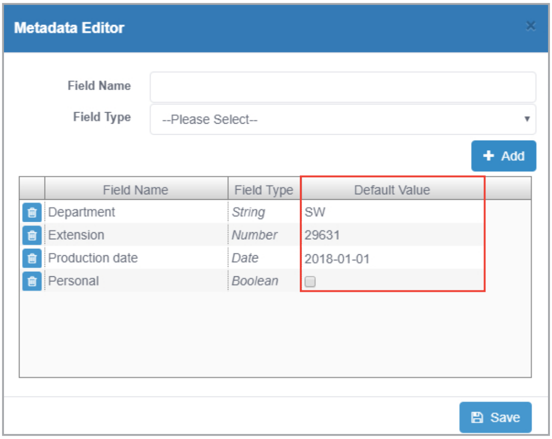
Field Name: Personal

Field Type: Boolean

Field Name	Field Type	Default Value
Department	String	SW
Extension	Number	29631
Production date	Date	2018-01-01

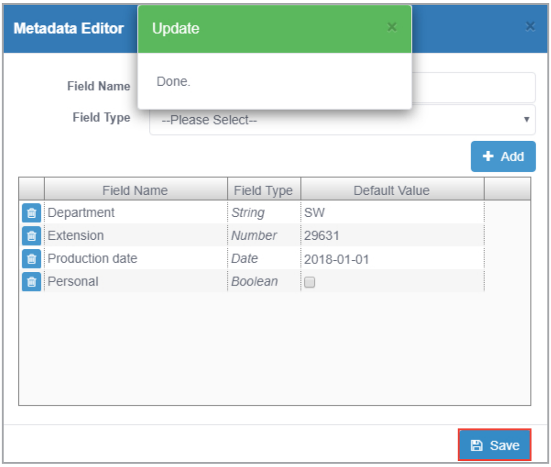
4. (optional) You may set or edit the default value of the new field by double-clicking in the **Default Value** cell and then entering the new default value.

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



	Field Name	Field Type	Default Value
🗑	Department	*String*	SW
🗑	Extension	*Number*	29631
🗑	Production date	*Date*	2018-01-01
🗑	Personal	*Boolean*	□

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

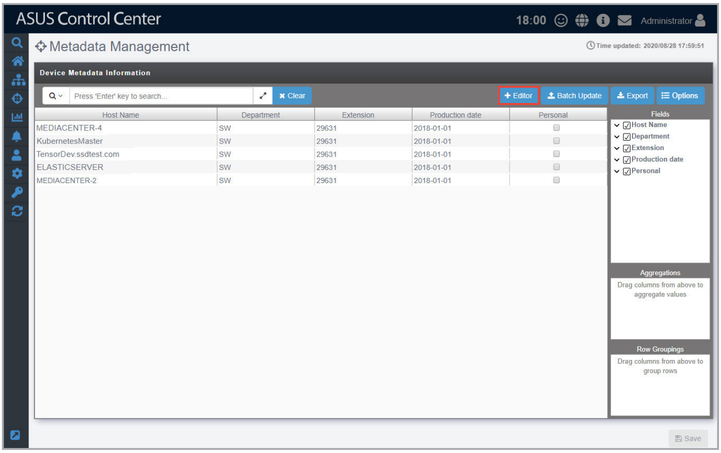


Done.

	Field Name	Field Type	Default Value
🗑	Department	*String*	SW
🗑	Extension	*Number*	29631
🗑	Production date	*Date*	2018-01-01
🗑	Personal	*Boolean*	□

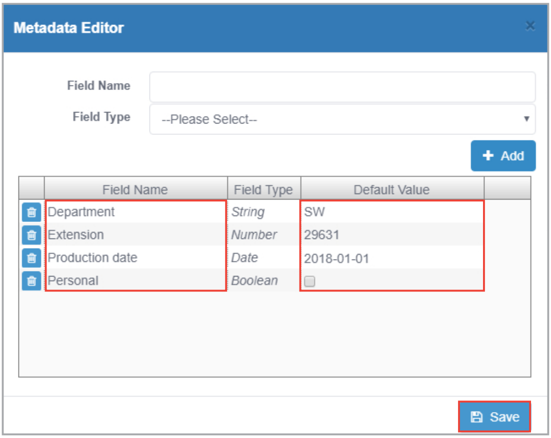
Editing metadata fields

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



Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	□
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	SW	29631	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	SW	29631	2018-01-01	□

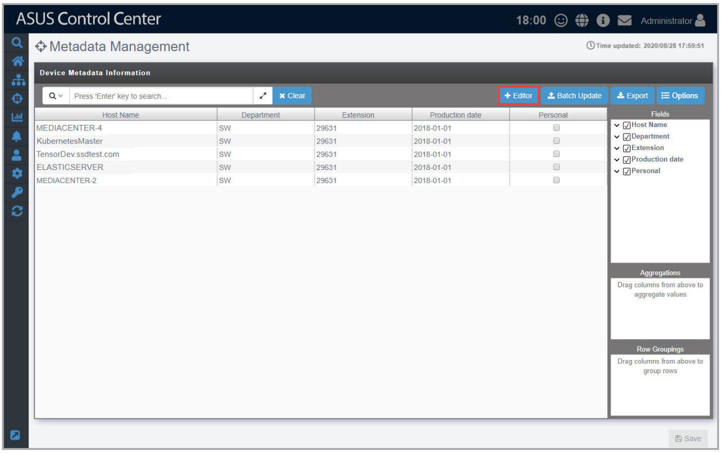
2. You can edit the **Field Name** and **Default Value** of existing metadata fields. When you are finished editing, click on **Save** to save the changes made.



Field Name	Field Type	Default Value
Department	String	SW
Extension	Number	29631
Production date	Date	2018-01-01
Personal	Boolean	□

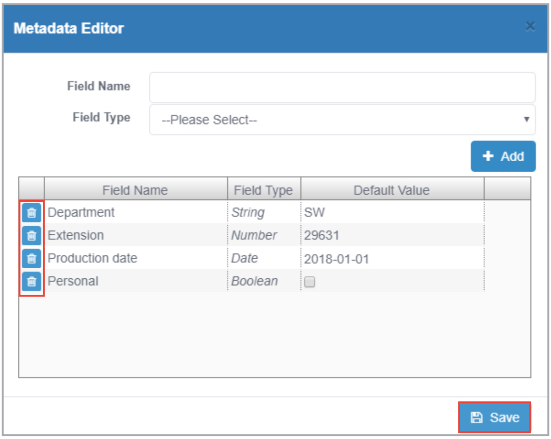
Deleting metadata fields

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



Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	□
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	SW	29631	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	SW	29631	2018-01-01	□

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



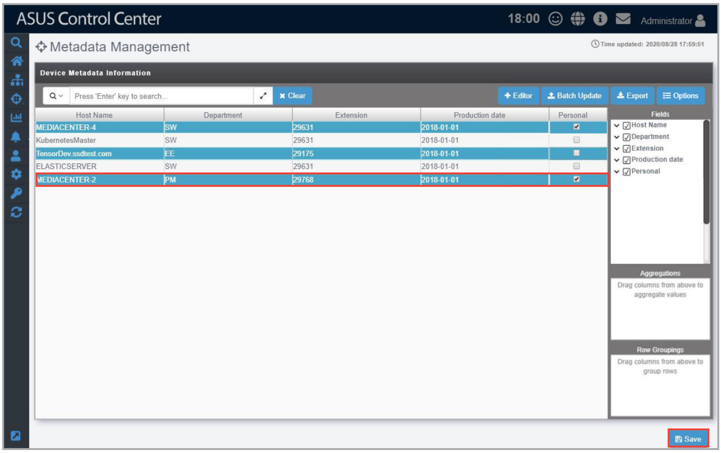
	Field Name	Field Type	Default Value
🗑	Department	*String*	SW
🗑	Extension	*Number*	29631
🗑	Production date	*Date*	2018-01-01
🗑	Personal	*Boolean*	□

Editing the metadata value of a single device

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

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

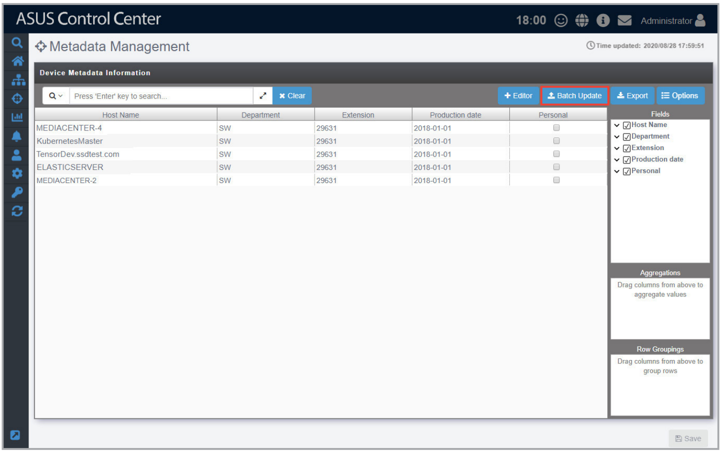
2. Click on **Save** once you have finished making changes to the metadata.



Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	☑
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	EE	29175	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	PM	29768	2018-01-01	☑

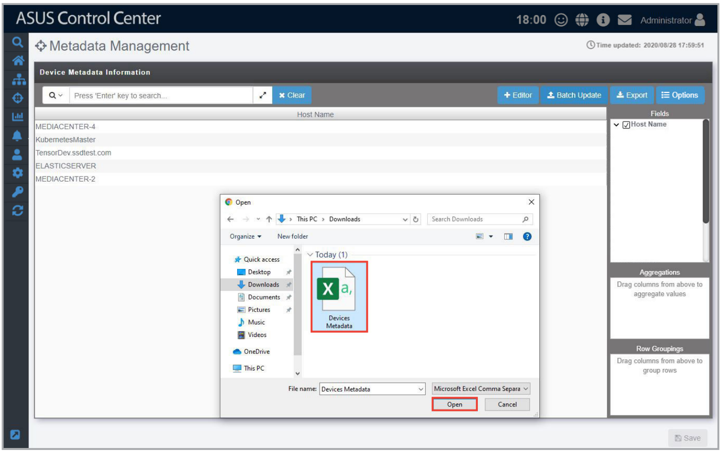
Editing the metadata value of multiple devices

1. Click on **Batch Update**.



Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	□
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	SW	29631	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	SW	29631	2018-01-01	□

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

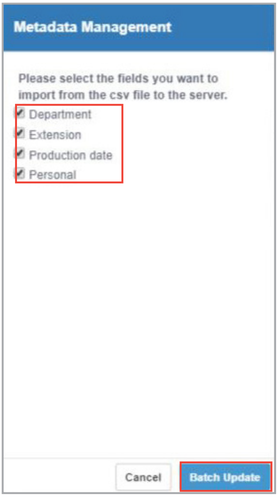


Host Name
MEDIACENTER-4
KubernetesMaster
TensorDev.ssdtest.com
ELASTICSERVER
MEDIACENTER-2

File name: Devices Metadata

Microsoft Excel Comma Separa

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

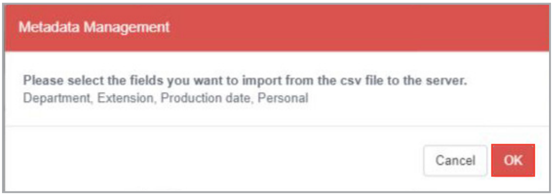


Metadata Management

Please select the fields you want to import from the csv file to the server.

☑ Department
☑ Extension
☑ Production date
☑ Personal

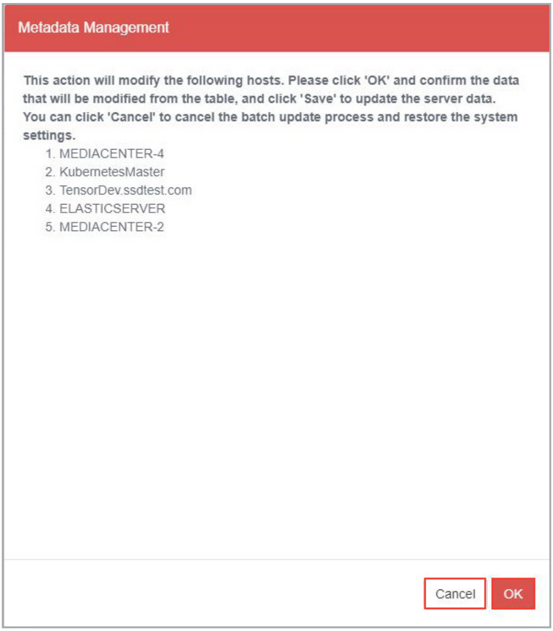
4. A confirmation window should pop-up, click **OK**.



Metadata Management

Please select the fields you want to import from the csv file to the server.
Department, Extension, Production date, Personal

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.

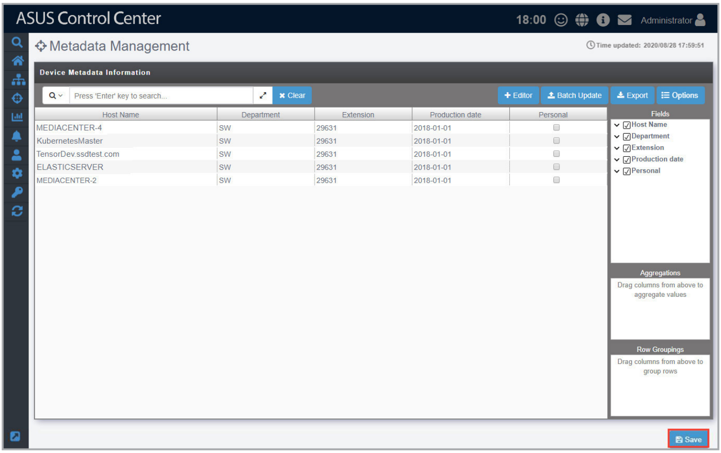


Metadata Management

This action will modify the following hosts. Please click 'OK' and confirm the data that will be modified from the table, and click 'Save' to update the server data. You can click 'Cancel' to cancel the batch update process and restore the system settings.

1. MEDIACENTER-4
2. KubernetesMaster
3. TensorDev.ssdtest.com
4. ELASTICSERVER
5. MEDIACENTER-2

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

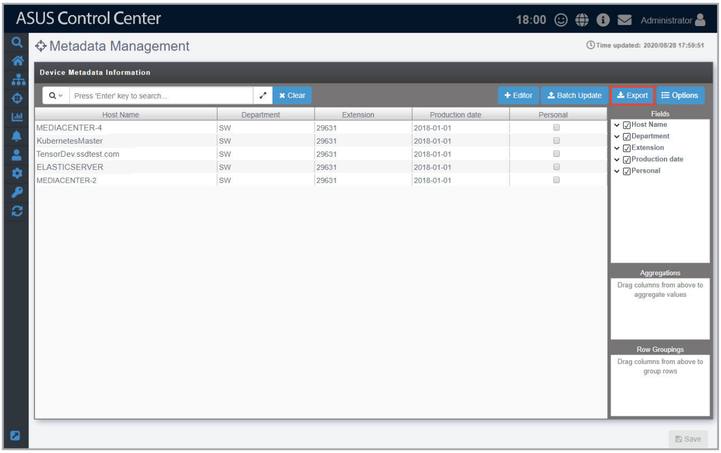


Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	□
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	SW	29631	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	SW	29631	2018-01-01	□

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**.



Host Name	Department	Extension	Production date	Personal
MEDIACENTER-4	SW	29631	2018-01-01	□
KubernetesMaster	SW	29631	2018-01-01	□
TensorDev.ssdtest.com	SW	29631	2018-01-01	□
ELASTICSERVER	SW	29631	2018-01-01	□
MEDIACENTER-2	SW	29631	2018-01-01	□

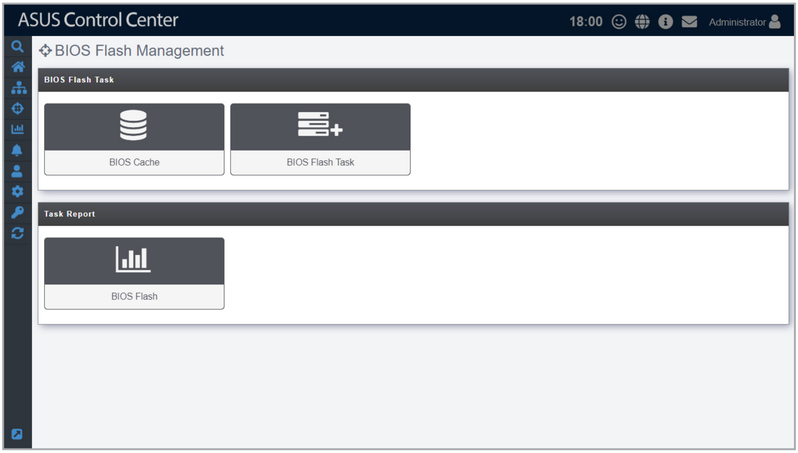
2. Enter a filename for the CSV file, then click **OK**.

- 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.

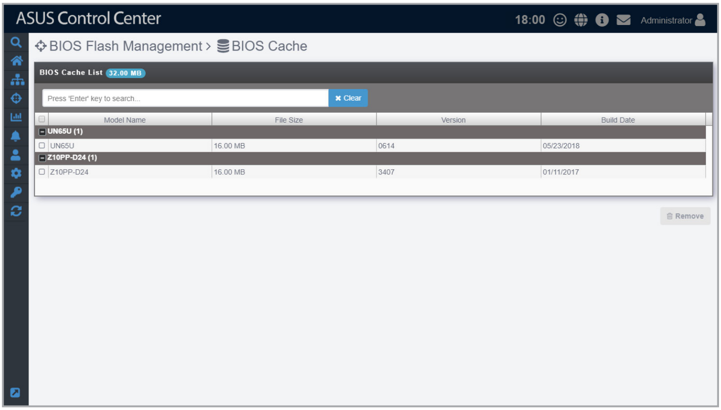
To access **BIOS Flash Management**, click ⌖ > **BIOS Flash Management** in the left menu.



- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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.



□	Model Name	File Size	Version	Build Date
⊟	UN65U (1)			
□	UN65U	16.00 MB	0614	05/23/2018
⊟	Z10PP-D24 (1)			
□	Z10PP-D24	16.00 MB	3407	01/11/2017

Adding a BIOS cap file to the BIOS Cache

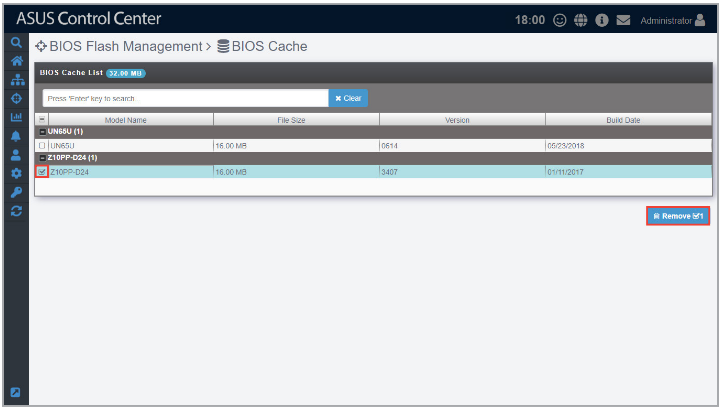
The BIOS cap file is automatically added to the BIOS Cache when you manually upload a BIOS cap file when flashing the BIOS from **Device Information**, or when you manually upload a BIOS cap file when using the **BIOS Flash Task** function.

- 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

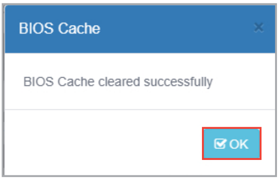
You can remove BIOS cap files from the BIOS Cache List when you need to, such as when the BIOS version is outdated.

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



☐	Model Name	File Size	Version	Build Date
UN65U (1)				
☐	UN65U	16.00 MB	0614	05/23/2018
Z10PP-D24 (1)				
☑	Z10PP-D24	16.00 MB	3407	01/11/2017

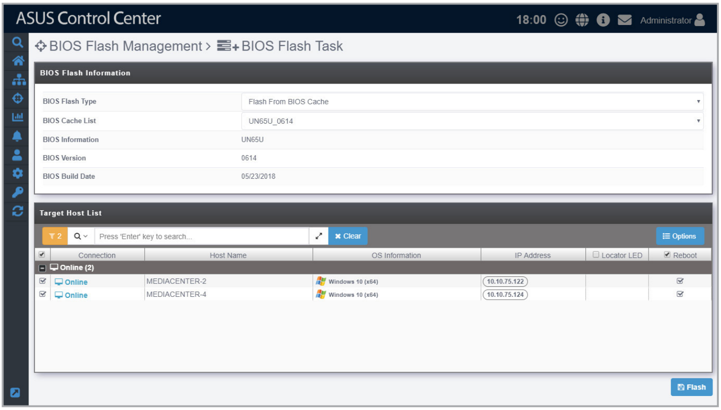
2. When the BIOS cap file(s) have been successfully removed, click **OK**.



BIOS Cache cleared successfully

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.



BIOS Flash Information

BIOS Flash Type	Flash From BIOS Cache
BIOS Cache List	UN65U_0614
BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018

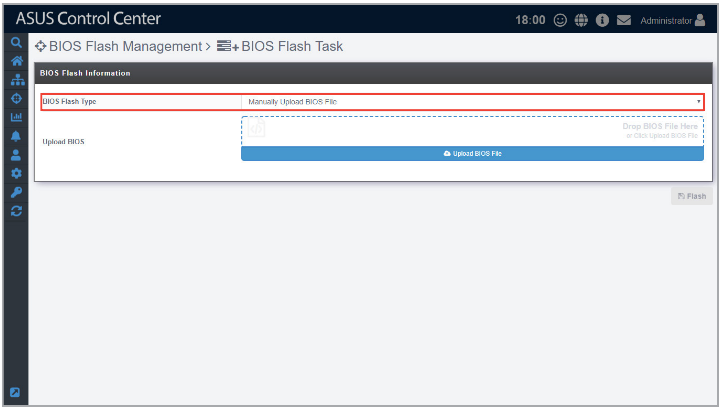
Target Host List

Press 'Enter' key to search...

☑	Connection	Host Name	OS Information	IP Address	□ Locator LED	☑ Reboot
⊟	Online (2)					
☑	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		☑
☑	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		☑

Manually uploading the BIOS cap file

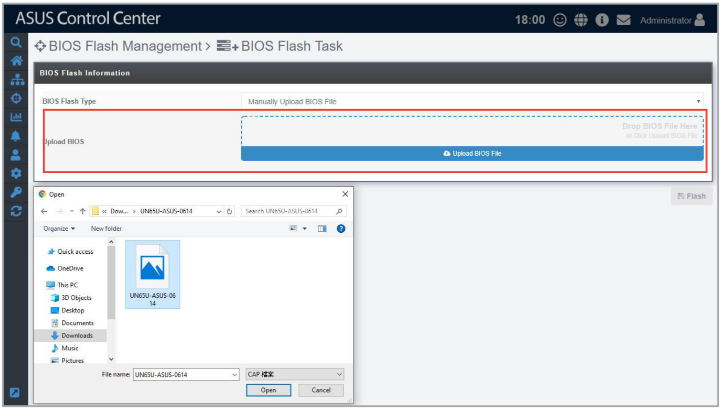
1. Select **Manually Upload BIOS File** from the drop down menu in the **BIOS Flash Type** field.



BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	

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.



ASUS Control Center 18:00 Administrator

BIOS Flash Management > BIOS Flash Task

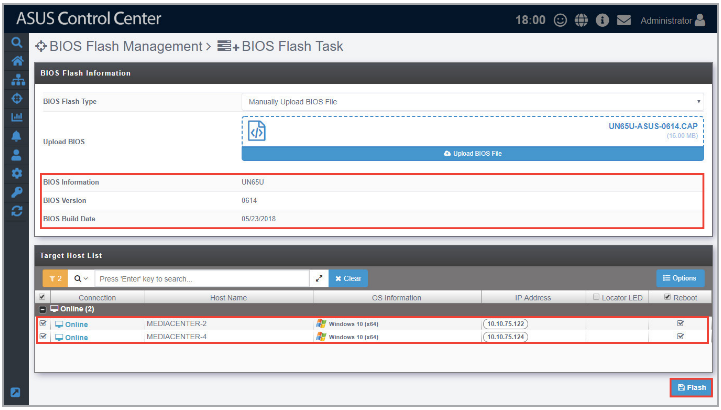
BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	Drop BIOS File Here or Click Upload BIOS File Upload BIOS File

File name: UN65U-ASUS-0614

CAP 檔案

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.



ASUS Control Center 18:00 Administrator

BIOS Flash Management > BIOS Flash Task

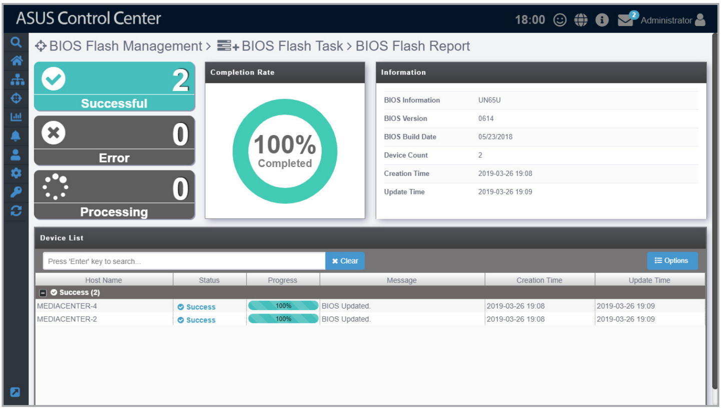
BIOS Flash Information

BIOS Flash Type	Manually Upload BIOS File
Upload BIOS	UN65U-ASUS-0614.CAP (16.00 MB) Upload BIOS File
BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018

Target Host List

☑	Connection	Host Name	OS Information	IP Address	□ Locator LED	☑ Reboot
⊟	Online (2)					
☑	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		☑
☑	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		☑

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.

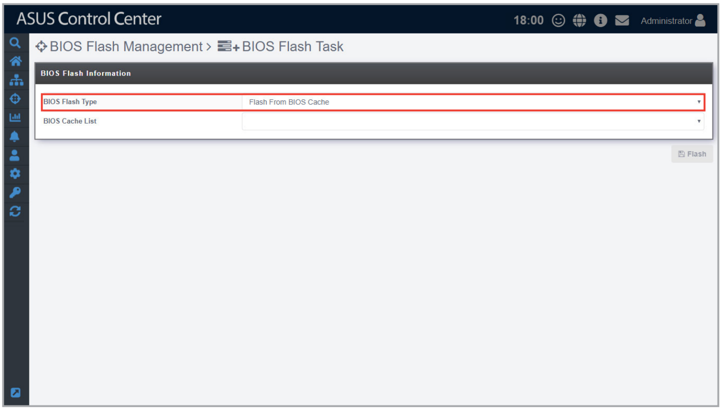


BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018
Device Count	2
Creation Time	2019-03-26 19:08
Update Time	2019-03-26 19:09

Host Name	Status	Progress	Message	Creation Time	Update Time
Success (2)					
MEDIACENTER-4	Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09
MEDIACENTER-2	Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09

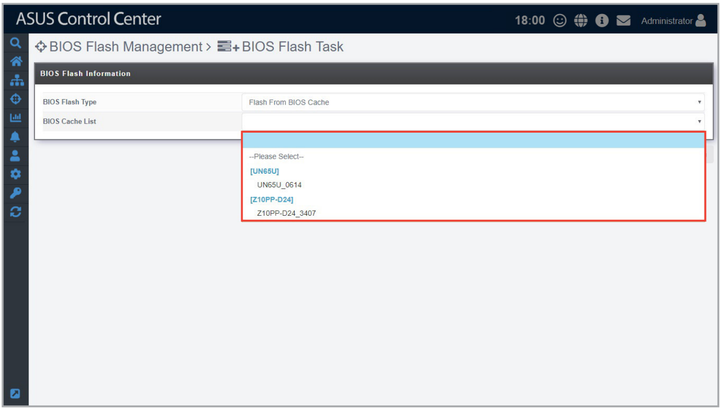
Selecting the BIOS cap file from the BIOS cache

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



BIOS Flash Type	Flash From BIOS Cache
BIOS Cache List	

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



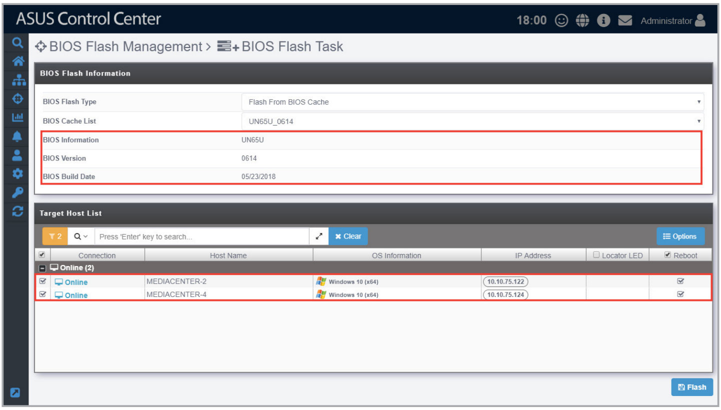
BIOS Flash Management > BIOS Flash Task

BIOS Flash Information

BIOS Flash Type	Flash From BIOS Cache
BIOS Cache List	

--Please Select--
[UN65U]
UN65U_0614
[Z10PP-D24]
Z10PP-D24_3407

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.



BIOS Flash Management > BIOS Flash Task

BIOS Flash Information

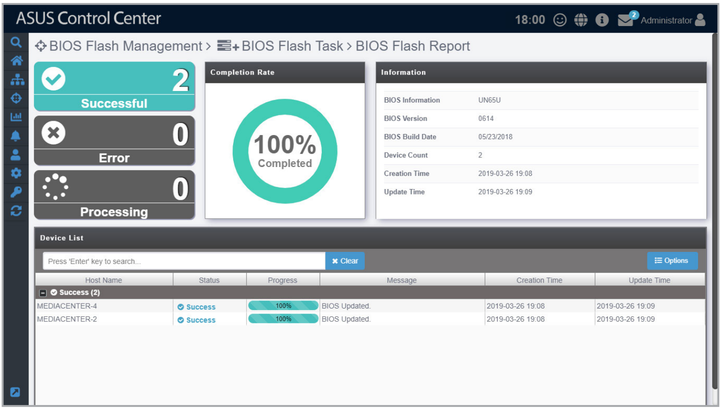
BIOS Flash Type	Flash From BIOS Cache
BIOS Cache List	UN65U_0614
BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018

Target Host List

Press 'Enter' key to search...

☑	Connection	Host Name	OS Information	IP Address	□ Locator LED	☑ Reboot
Online (2)						
☑	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		☑
☑	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		☑

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.



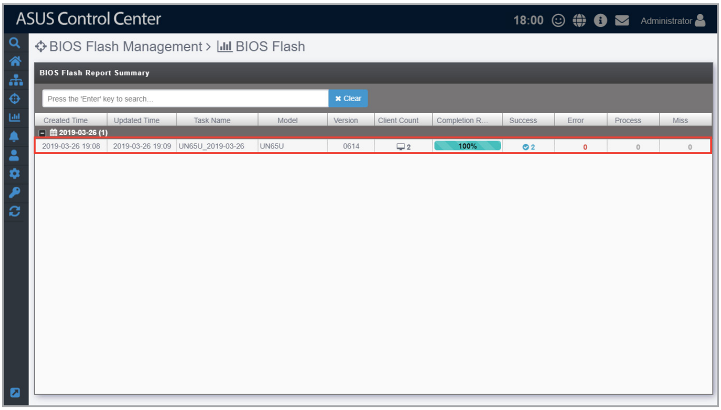
Information	
BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018
Device Count	2
Creation Time	2019-03-26 19:08
Update Time	2019-03-26 19:09

Host Name	Status	Progress	Message	Creation Time	Update Time
Success (2)					
MEDIACENTER-4	Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09
MEDIACENTER-2	Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09

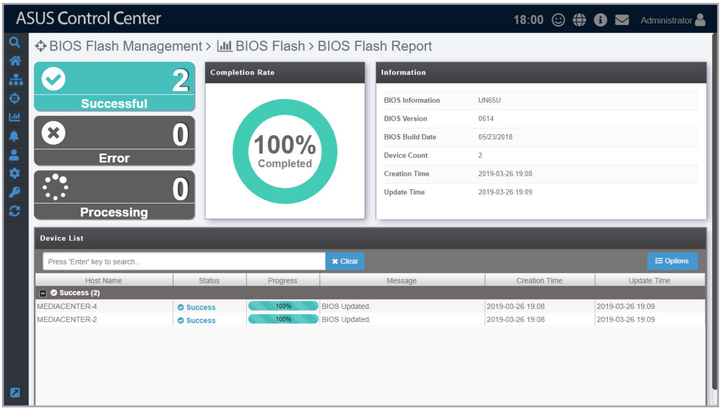
If the device is using Windows 11 or Server 2022 and the BIOS flash is failing, please navigate to **Start** > **Settings** > **Update & Security** > **Windows Security** > **Device Security**, then select **Core Isolation details** and set **Memory integrity** to **Off** on the device.

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.


ASUS Control Center
18:00
Administrator
BIOS Flash Management > BIOS Flash
BIOS Flash Report Summary
Press the 'Enter' key to search...
✖ Clear

Created Time	Updated Time	Task Name	Model	Version	Client Count	Completion R...	Success	Error	Process	Miss
⊟ 2019-03-26 (1)										
2019-03-26 19:08	2019-03-26 19:09	UN65U_2019-03-26	UN65U	0614	2	100%	✓ 2	0	0	0



Information

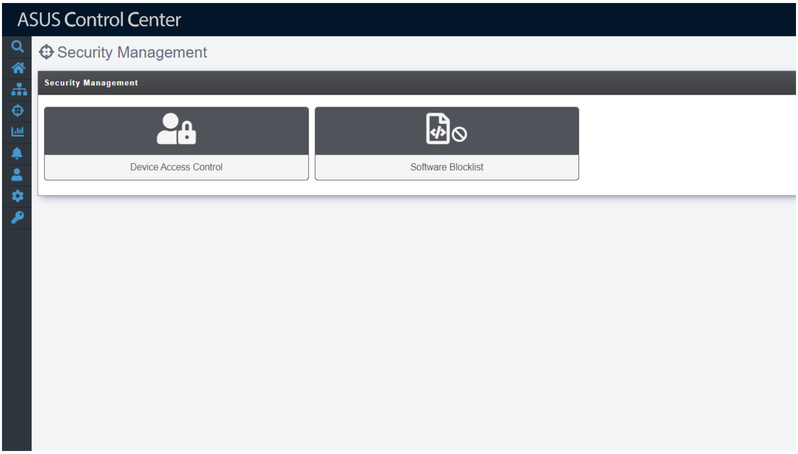
BIOS Information	UN65U
BIOS Version	0614
BIOS Build Date	05/23/2018
Device Count	2
Creation Time	2019-03-26 19:08
Update Time	2019-03-26 19:09

Host Name	Status	Progress	Message	Creation Time	Update Time
⊟ ✓ Success (2)					
MEDIACENTER-4	✓ Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09
MEDIACENTER-2	✓ Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09

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.

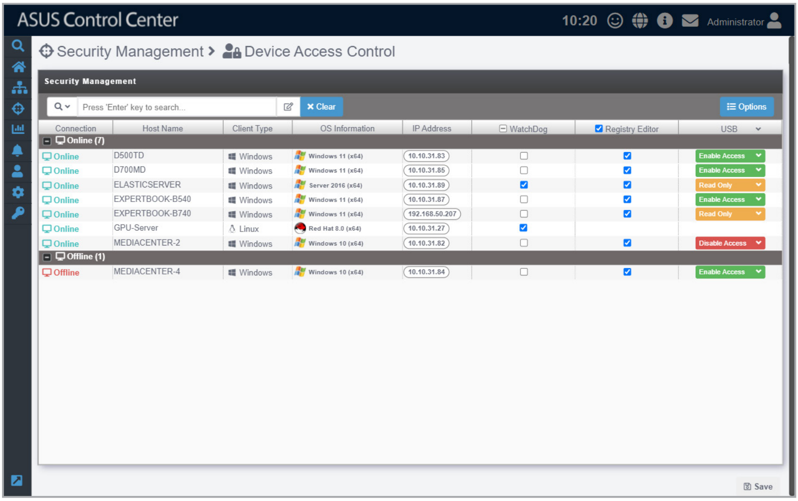
To access **Security Management**, click ⌖ > **Security Management** in the left menu.



- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.
- **Registry Editor** and **USB** configurations are only available for Windows system managed devices.

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.


ASUS Control Center
10:20
Administrator
Security Management > Device Access Control
Security Management
Press 'Enter' key to search...
Clear
Options
Save

Connection	Host Name	Client Type	OS Information	IP Address	⊟ WatchDog	☑ Registry Editor	USB
⊟ Online (7)							
Online	D500TD	Windows	Windows 11 (x64)	10.10.31.83	☐	☑	Enable Access
Online	D700MD	Windows	Windows 11 (x64)	10.10.31.85	☐	☑	Enable Access
Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.89	☑	☑	Read Only
Online	EXPERTBOOK-B540	Windows	Windows 11 (x64)	10.10.31.87	☐	☑	Enable Access
Online	EXPERTBOOK-B740	Windows	Windows 11 (x64)	192.168.50.207	☐	☑	Read Only
Online	GPU-Server	Linux	Red Hat 8.0 (x64)	10.10.31.27	☑		
Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.31.82	☐	☑	Disable Access
⊟ Offline (1)							
Offline	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.31.84	☐	☑	Enable Access

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.

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.

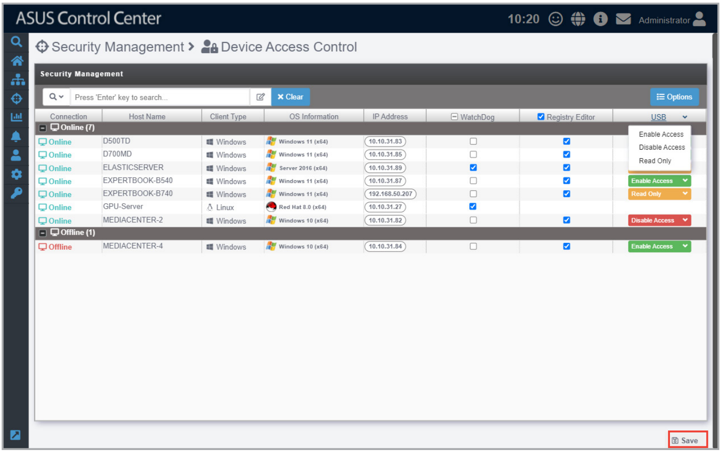
- **Registry Editor (Windows only)**

  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.

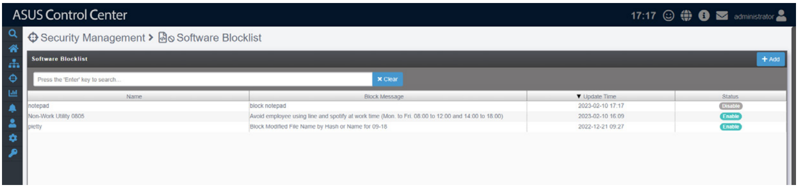
2. Click on **Save** once you have finished making changes to save the changes made.



Connection	Host Name	Client Type	OS Information	IP Address	WatchDog	☑ Registry Editor	USB
Online (7)							
Online	D500TD	Windows	Windows 11 (x64)	10.10.31.83	☐	☑	
Online	D700MD	Windows	Windows 11 (x64)	10.10.31.85	☐	☑	
Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.89	☑	☑	
Online	EXPERTBOOK-B540	Windows	Windows 11 (x64)	10.10.31.87	☐	☑	Enable Access
Online	EXPERTBOOK-B740	Windows	Windows 11 (x64)	192.168.50.207	☐	☑	Read Only
Online	GPU-Server	Linux	Red Hat 8.0 (x64)	10.10.31.27	☑		
Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.31.82	☐	☑	Disable Access
Offline (1)							
Offline	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.31.84	☐	☑	Enable Access

4.3.2 Software Blocklist

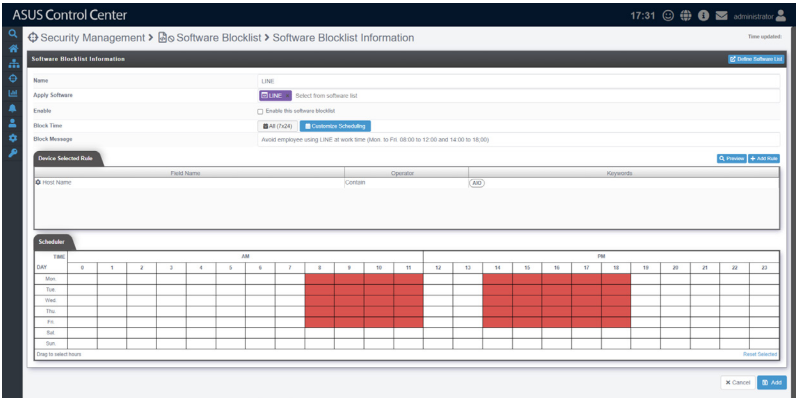
Software Blocklist allows you to create or manage rules to prevent selected software applications from running on the managed device during specified time periods.


ASUS Control Center
17:17
administrator
Security Management > Software Blocklist
Software Blocklist
+ Add
Press the 'Enter' key to search...
✕ Clear

Name	Block Message	▼ Update Time	Status
notepad	block notepad	2023-02-10 17:17	Disable
Non-Work Utility 0805	Avoid employee using line and spotify at work time (Mon. to Fri. 08:00 to 12:00 and 14:00 to 18:00)	2023-02-10 16:09	Enable
pletty	Block Modified File Name by Hash or Name for 09-18	2022-12-21 09:27	Enable

Adding a new software blocklist rule

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



Name: LINE

Apply Software: LINE ✕ Select from software list

Enable: □ Enable this software blocklist

Block Time: All (7x24) | Customize Scheduling

Block Message: Avoid employee using LINE at work time (Mon. to Fri. 08:00 to 12:00 and 14:00 to 18:00)

Field Name	Operator	Keywords
Host Name	Contain	AIO

TIME	AM												PM											
DAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon.									🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥					
Tue.									🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥					
Wed.									🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥					
Thu.									🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥					
Fri.									🟥	🟥	🟥	🟥			🟥	🟥	🟥	🟥	🟥					
Sat.																								
Sun.																								

Drag to select hours

Reset Selected

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

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

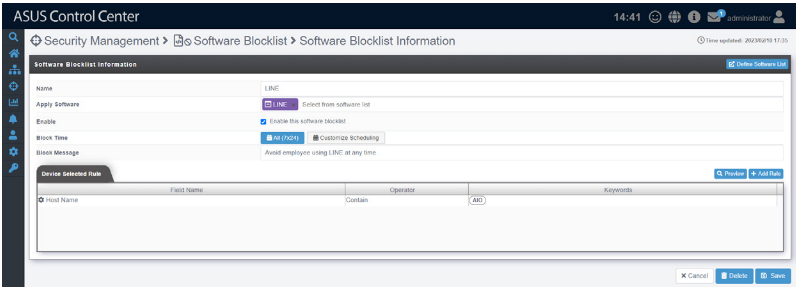
3. Tick **Enable** to enable the software blocklist rule.
4. Select **All (7x24)** in the **Block Time** field to enable the software block list rule at all times, or select **Customize Scheduling** to specify a custom schedule using the **Scheduler**.
5. Fill in the **Block Message** field with a brief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

6. 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**.

7. Click **Add** to save the software blocklist rule.

Editing a software blocklist rule

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



ASUS Control Center
14:41
administrator
Security Management > Software Blocklist > Software Blocklist Information
Time updated: 2023/02/10 17:35
Software Blocklist Information
Define Software List

Name	LINE
Apply Software	LINE × Select from software list
Enable	☑ Enable this software blocklist
Block Time	All (7x24) Customize Scheduling
Block Message	Avoid employee using LINE at any time

Device Selected Rule
Preview
+ Add Rule

Field Name	Operator	Keywords
Host Name	Contain	AIO

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

Deleting a software blocklist rule

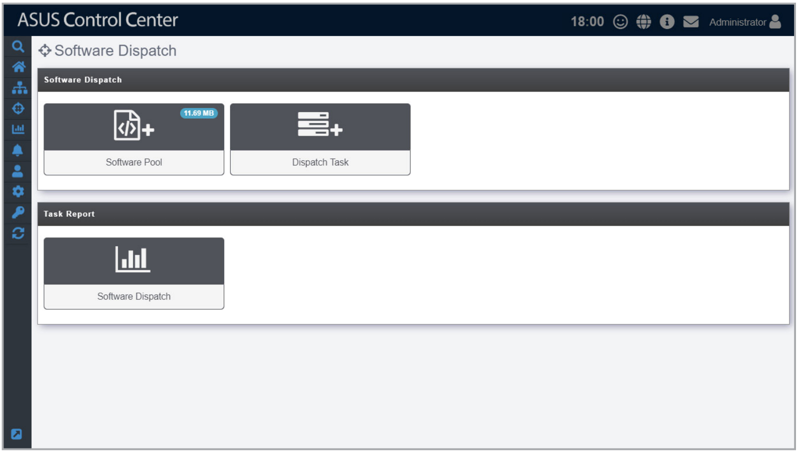
1. Click an existing rule from the Software Blocklist rule list to open the rule editor.

2. Click **Delete** to delete the software blocklist rule.

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.

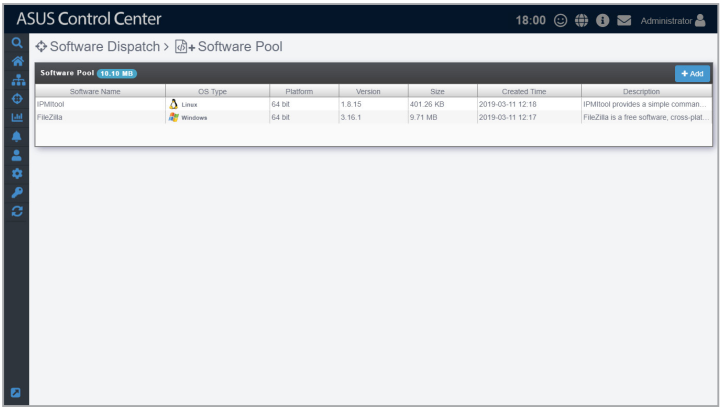
To access **Software Dispatch**, click ⊕ > **Software Dispatch** in the left menu.



- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

4.4.1 Software Pool

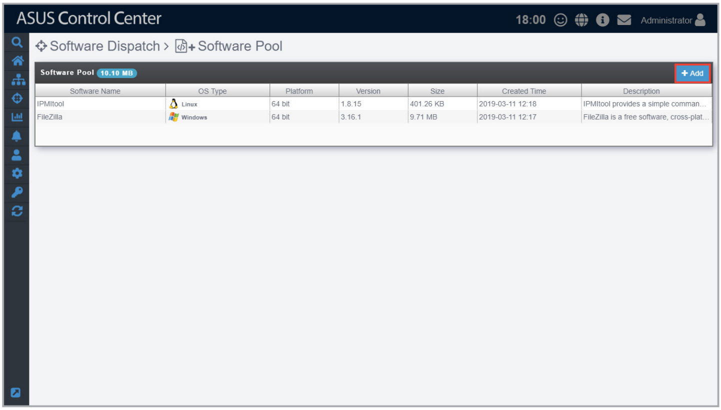
The Software Pool allows you to view all uploaded software packages. You may also add additional software packages or remove existing software packages from the Software Pool. The uploaded software packages will allow you to easily select and dispatch software to selected managed devices.



Software Name	OS Type	Platform	Version	Size	Created Time	Description
IPMItool	Linux	64 bit	1.8.15	401.26 KB	2019-03-11 12:18	IPMItool provides a simple comman...
FileZilla	Windows	64 bit	3.16.1	9.71 MB	2019-03-11 12:17	FileZilla is a free software, cross-plat...

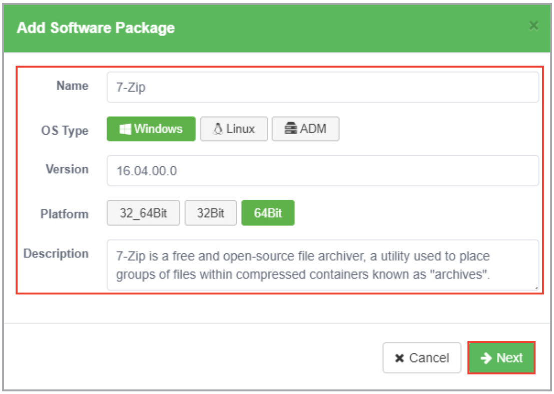
Adding software packages to the Software Pool

1. Click on **Add**.



Software Name	OS Type	Platform	Version	Size	Created Time	Description
IPMItool	Linux	64 bit	1.8.15	401.26 KB	2019-03-11 12:18	IPMItool provides a simple comman...
FileZilla	Windows	64 bit	3.16.1	9.71 MB	2019-03-11 12:17	FileZilla is a free software, cross-plat...

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

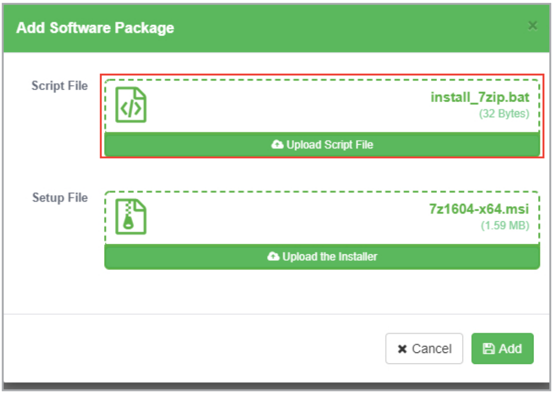
Version: 16.04.00.0

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".

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.

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

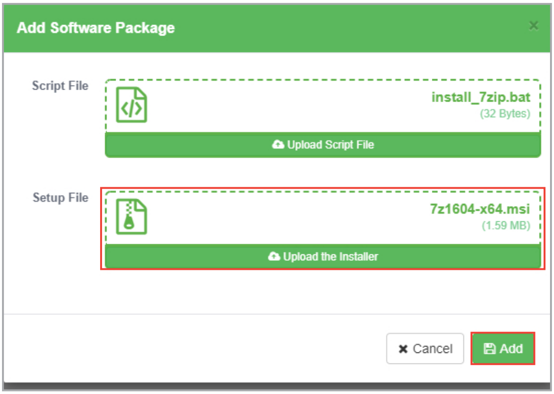


Add Software Package

Script File: install_7zip.bat (32 Bytes)

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

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**.

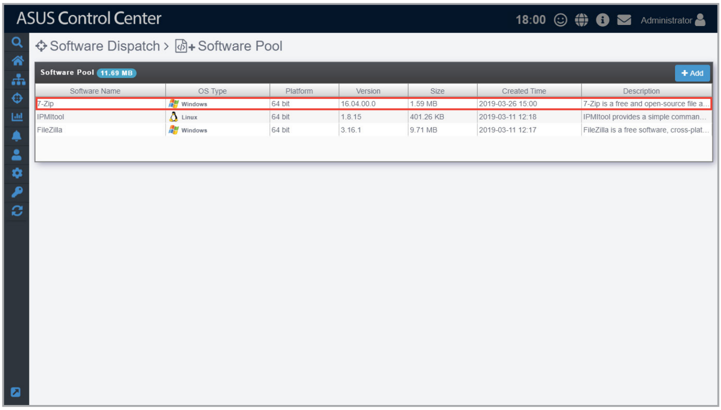


Add Software Package

Script File: install_7zip.bat (32 Bytes)

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

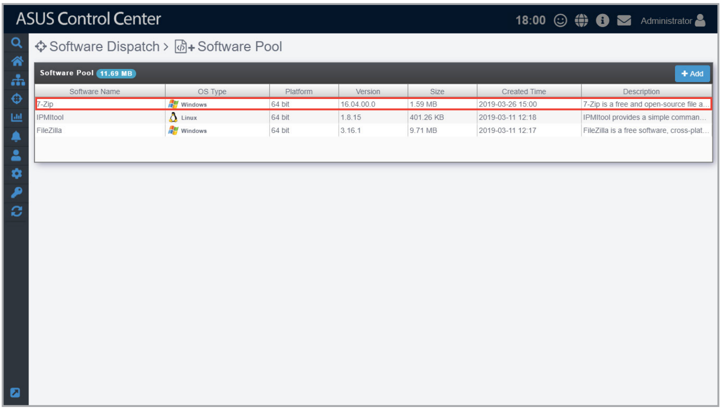
5. The newly added software package will appear in the Software Pool list.



Software Name	OS Type	Platform	Version	Size	Created Time	Description
7-Zip	Windows	64 bit	16.04.00.0	1.59 MB	2019-03-26 15:00	7-Zip is a free and open-source file a...
IPMItool	Linux	64 bit	1.8.15	401.26 KB	2019-03-11 12:18	IPMItool provides a simple comman...
FileZilla	Windows	64 bit	3.16.1	9.71 MB	2019-03-11 12:17	FileZilla is a free software, cross-plat...

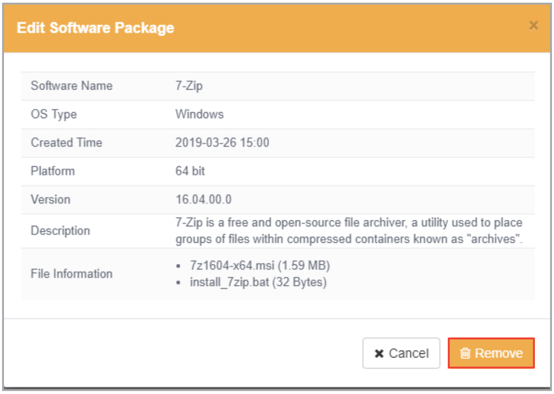
Removing software packages from the Software Pool

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



Software Name	OS Type	Platform	Version	Size	Created Time	Description
7-Zip	Windows	64 bit	16.04.00.0	1.59 MB	2019-03-26 15:00	7-Zip is a free and open-source file a...
IPMItool	Linux	64 bit	1.8.15	401.26 KB	2019-03-11 12:18	IPMItool provides a simple comman...
FileZilla	Windows	64 bit	3.16.1	9.71 MB	2019-03-11 12:17	FileZilla is a free software, cross-plat...

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

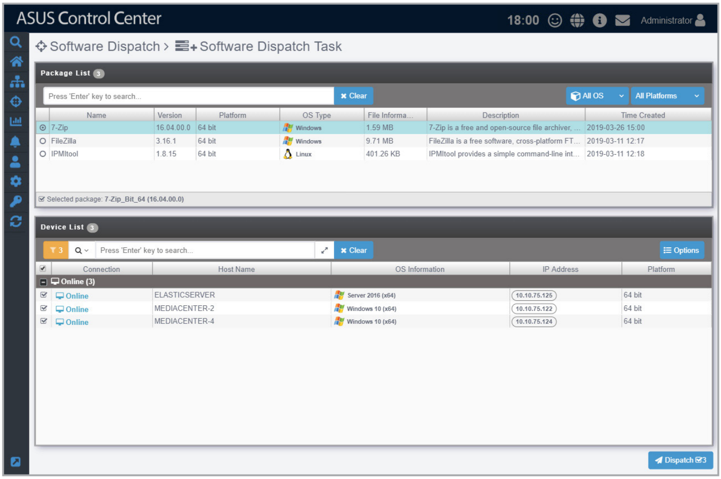


Software Name	7-Zip
OS Type	Windows
Created Time	2019-03-26 15:00
Platform	64 bit
Version	16.04.00.0
Description	7-Zip is a free and open-source file archiver, a utility used to place groups of files within compressed containers known as "archives".
File Information	• 7z1604-x64.msi (1.59 MB) • install_7zip.bat (32 Bytes)

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.

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


ASUS Control Center
18:00
Administrator
Software Dispatch > Software Dispatch Task

Package List 3

Press 'Enter' key to search...
✖ Clear
All OS
All Platforms

	Name	Version	Platform	OS Type	File Informa...	Description	Time Created
●	7-Zip	16.04.00.0	64 bit	Windows	1.59 MB	7-Zip is a free and open-source file archiver, ...	2019-03-26 15:00
○	FileZilla	3.16.1	64 bit	Windows	9.71 MB	FileZilla is a free software, cross-platform FT...	2019-03-11 12:17
○	IPMItool	1.8.15	64 bit	Linux	401.26 KB	IPMItool provides a simple command-line int...	2019-03-11 12:18

☑ Selected package: 7-Zip_Bit_64 (16.04.00.0)

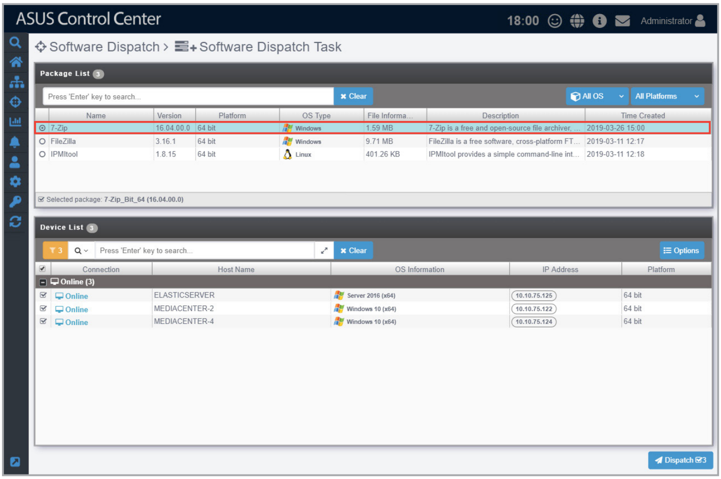
Device List 3

☑	Connection	Host Name	OS Information	IP Address	Platform
⊟	Online (3)				
☑	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	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

Dispatching software packages to devices

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

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 3

Press 'Enter' key to search... ✖ Clear All OS All Platforms

	Name	Version	Platform	OS Type	File Informa...	Description	Time Created
●	7-Zip	16.04.00.0	64 bit	Windows	1.59 MB	7-Zip is a free and open-source file archiver, ...	2019-03-26 15:00
○	FileZilla	3.16.1	64 bit	Windows	9.71 MB	FileZilla is a free software, cross-platform FT...	2019-03-11 12:17
○	IPMItool	1.8.15	64 bit	Linux	401.26 KB	IPMItool provides a simple command-line int...	2019-03-11 12:18

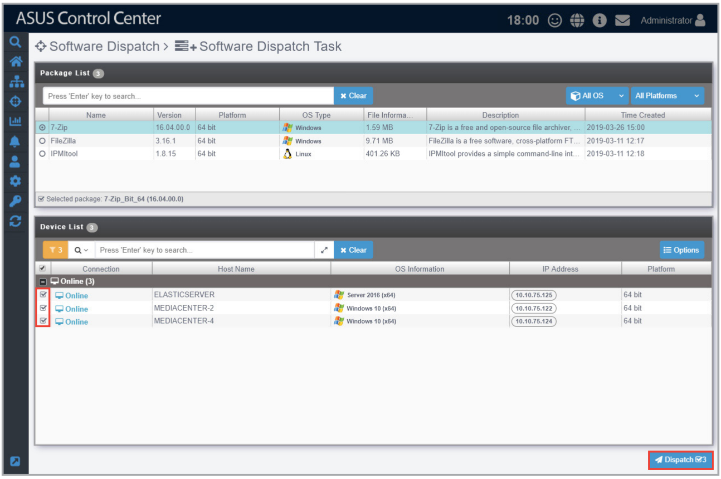
☑ Selected package: 7-Zip_Bit_64 (16.04.00.0)

Device List 3

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

☑	Connection	Host Name	OS Information	IP Address	Platform
⊟	Online (3)				
☑	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	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

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 3

Press 'Enter' key to search... ✖ Clear All OS All Platforms

	Name	Version	Platform	OS Type	File Informa...	Description	Time Created
●	7-Zip	16.04.00.0	64 bit	Windows	1.59 MB	7-Zip is a free and open-source file archiver, ...	2019-03-26 15:00
○	FileZilla	3.16.1	64 bit	Windows	9.71 MB	FileZilla is a free software, cross-platform FT...	2019-03-11 12:17
○	IPMItool	1.8.15	64 bit	Linux	401.26 KB	IPMItool provides a simple command-line int...	2019-03-11 12:18

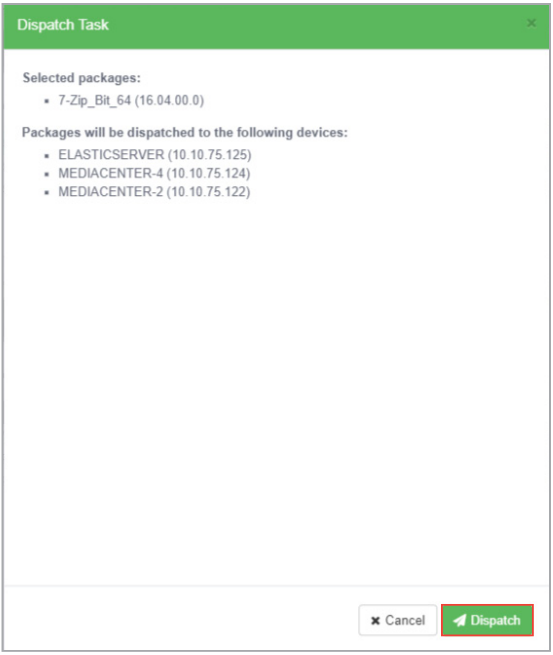
☑ Selected package: 7-Zip_Bit_64 (16.04.00.0)

Device List 3

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

☑	Connection	Host Name	OS Information	IP Address	Platform
⊟	Online (3)				
☑	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	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

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.



Selected packages:

- 7-Zip_Bit_64 (16.04.00.0)

Packages will be dispatched to the following devices:

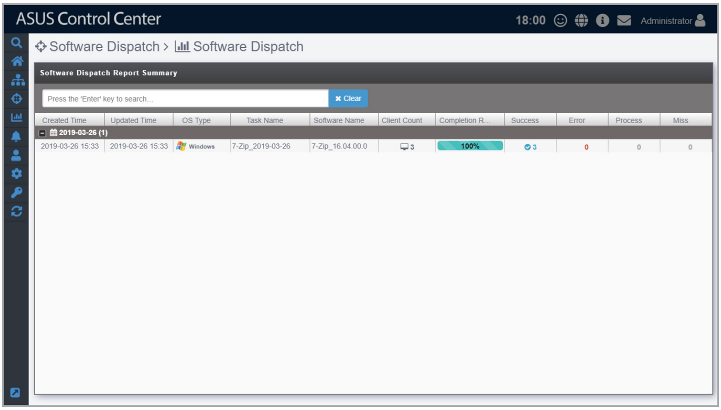
- ELASTICSERVER (10.10.75.125)
- MEDIACENTER-4 (10.10.75.124)
- MEDIACENTER-2 (10.10.75.122)

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

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

4.4.3 Software Dispatch Task Report

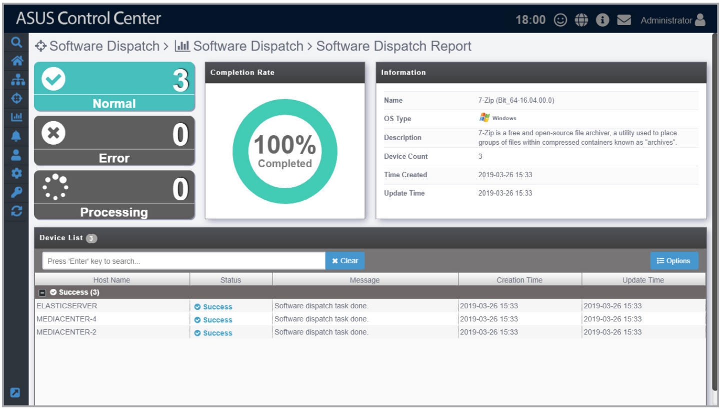
The **Software Dispatch Task Report** function will display a history of all software dispatch tasks performed using ASUS Control Center. Selecting a software dispatch task listed in the Software Dispatch Report Summary will allow you to view information on the software, which devices the software was 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.



Software Dispatch Report Summary

Press the 'Enter' key to search... ✖ Clear

Created Time	Updated Time	OS Type	Task Name	Software Name	Client Count	Completion R...	Success	Error	Process	Miss
2019-03-26 (1)										
2019-03-26 15:33	2019-03-26 15:33	Windows	7-Zip_2019-03-26	7-Zip_16.04.00.0	3	100%	3	0	0	0



Information

Name	7-Zip (Bit_64-16.04.00.0)
OS Type	Windows
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".
Device Count	3
Time Created	2019-03-26 15:33
Update Time	2019-03-26 15:33

Device List 3

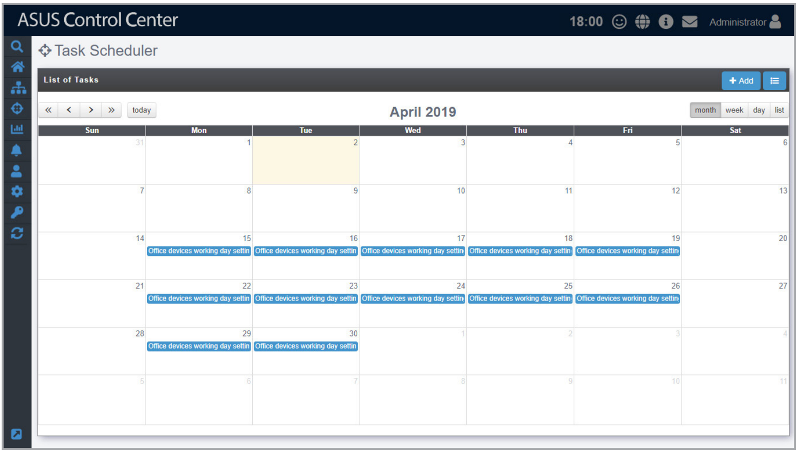
Press 'Enter' key to search... ✖ Clear ☰ Options

Host Name	Status	Message	Creation Time	Update Time
Success (3)				
ELASTICSERVER	Success	Software dispatch task done.	2019-03-26 15:33	2019-03-26 15:33
MEDIACENTER-4	Success	Software dispatch task done.	2019-03-26 15:33	2019-03-26 15:33
MEDIACENTER-2	Success	Software dispatch task done.	2019-03-26 15:33	2019-03-26 15:33

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.



April 2019

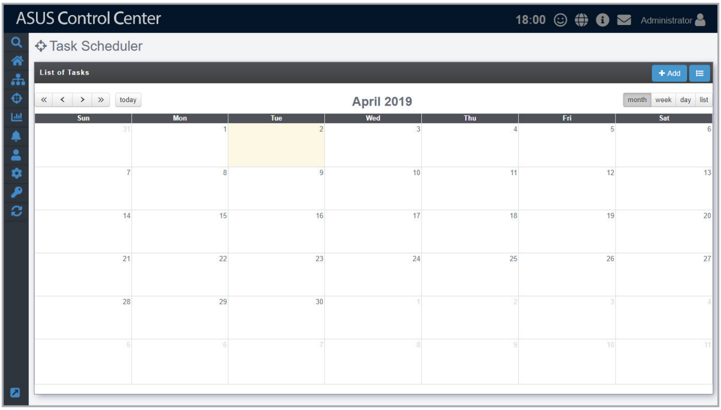
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15 Office devices working day settin	16 Office devices working day settin	17 Office devices working day settin	18 Office devices working day settin	19 Office devices working day settin	20
21	22 Office devices working day settin	23 Office devices working day settin	24 Office devices working day settin	25 Office devices working day settin	26 Office devices working day settin	27
28	29 Office devices working day settin	30 Office devices working day settin	1	2	3	4
5	6	7	8	9	10	11

- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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.

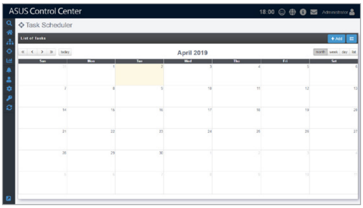
📅 : Calendar view displays the tasks and the dates when they will be executed.



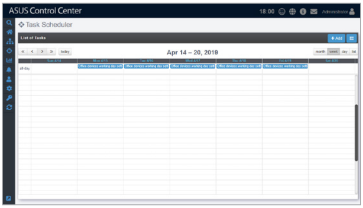
Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

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

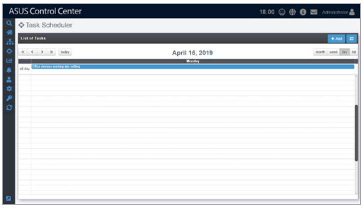
«	View previous year
»	View next year
‹	View previous month / week / day
›	View next month / week / day
today	Move to the current day. The current day will be highlighted on the calendar.
month	Display month view



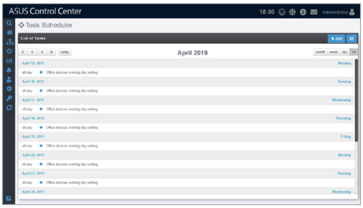
week Display week view



day   Display day view

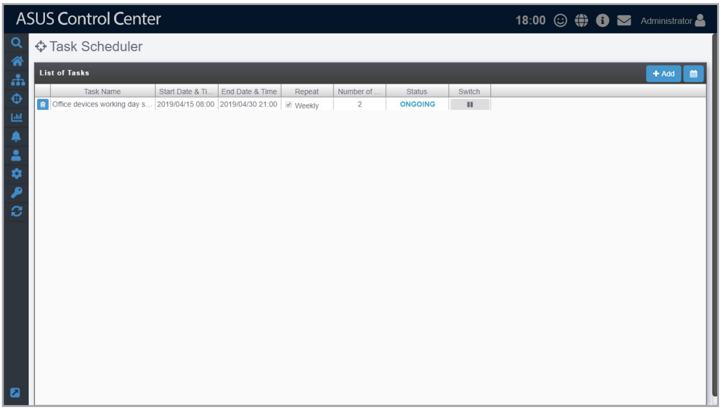


list   Display list of all tasks in the selected month and year.



April 15, 2019 Monday
all-day ● Office devices working day setting
April 16, 2019 Tuesday
all-day ● Office devices working day setting
April 17, 2019 Wednesday
all-day ● Office devices working day setting
April 18, 2019 Thursday
all-day ● Office devices working day setting
April 19, 2019 Friday
all-day ● Office devices working day setting
April 22, 2019 Monday
all-day ● Office devices working day setting
April 23, 2019 Tuesday
all-day ● Office devices working day setting
April 24, 2019 Wednesday

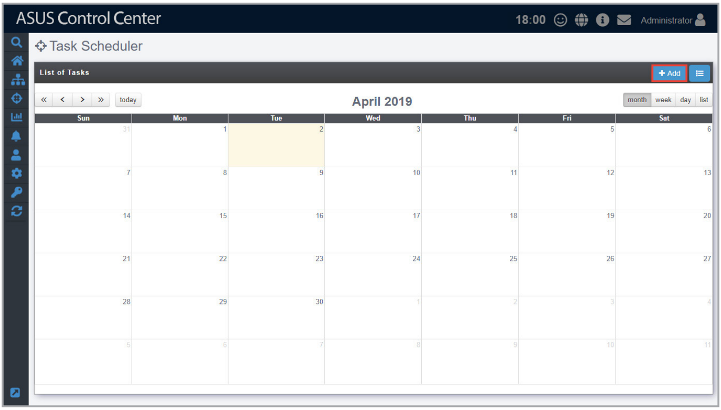
: History list of all tasks, including Task Name, Start Date & Time, End Date & Time, Repeat, Number of Clients, Status, and Switch.



	Task Name	Start Date & Ti...	End Date & Time	Repeat	Number of ...	Status	Switch
	Office devices working day s...	2019/04/15 08:00	2019/04/30 21:00	✓ Weekly	2	ONGOING	▮▮

Adding a scheduled task

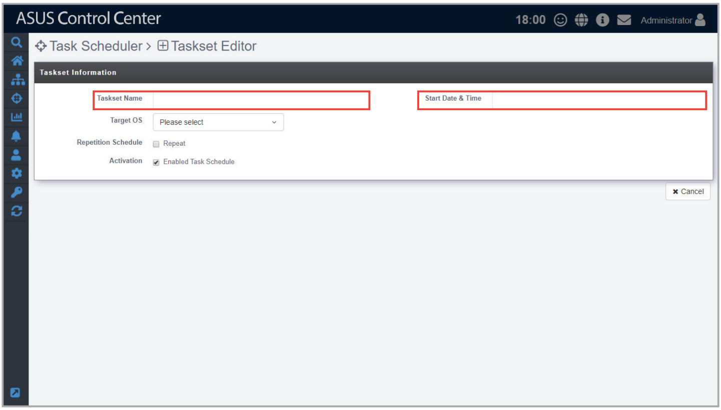
1. Click on **Add**.



April 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4
5	6	7	8	9	10	11

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



Taskset Name

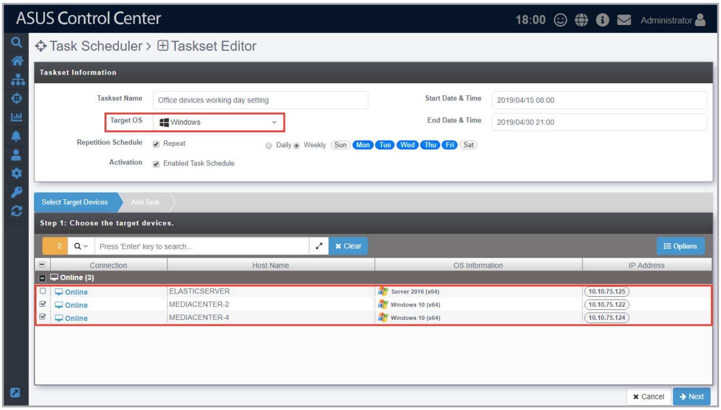
Start Date & Time

Target OS: Please select

Repetition Schedule: □ Repeat

Activation: ☑ Enabled Task Schedule

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



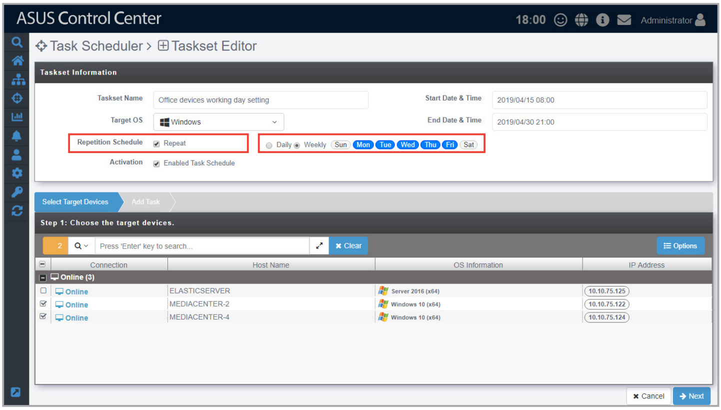
Taskset Information

Taskset Name	Office devices working day setting	Start Date & Time	2019/04/15 08:00
Target OS	Windows	End Date & Time	2019/04/30 21:00
Repetition Schedule	☑ Repeat	○ Daily ● Weekly Sun Mon Tue Wed Thu Fri Sat	
Activation	☑ Enabled Task Schedule		

Step 1: Choose the target devices.

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

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.



Taskset Information

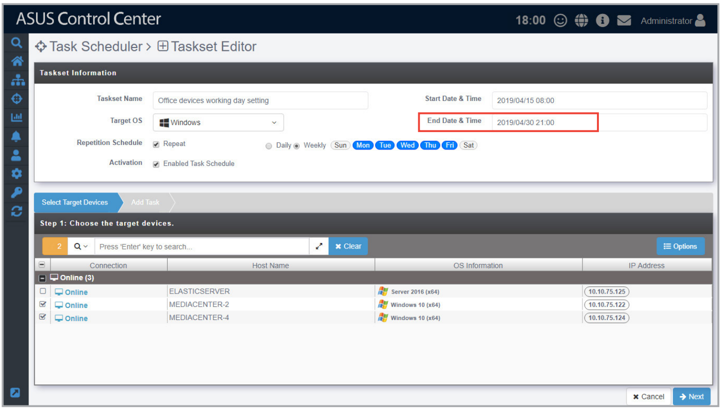
Taskset Name	Office devices working day setting	Start Date & Time	2019/04/15 08:00
Target OS	Windows	End Date & Time	2019/04/30 21:00
Repetition Schedule	☑ Repeat	○ Daily ● Weekly Sun Mon Tue Wed Thu Fri Sat	
Activation	☑ Enabled Task Schedule		

Step 1: Choose the target devices.

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

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

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



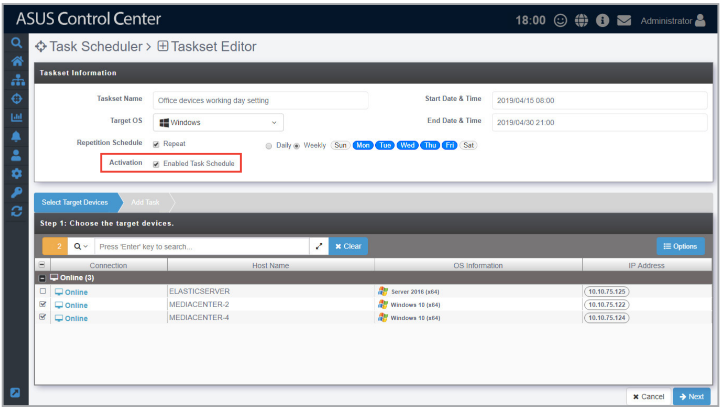
Taskset Information

Taskset Name	Office devices working day setting	Start Date & Time	2019/04/15 08:00
Target OS	Windows	End Date & Time	2019/04/30 21:00
Repetition Schedule	☑ Repeat	○ Daily ● Weekly Sun **Mon** **Tue** **Wed** **Thu** **Fri** Sat	
Activation	☑ Enabled Task Schedule		

Step 1: Choose the target devices.

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

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	Start Date & Time	2019/04/15 08:00
Target OS	Windows	End Date & Time	2019/04/30 21:00
Repetition Schedule	☑ Repeat	○ Daily ● Weekly Sun **Mon** **Tue** **Wed** **Thu** **Fri** Sat	
Activation	☑ Enabled Task Schedule		

Select Target Devices
Add Task

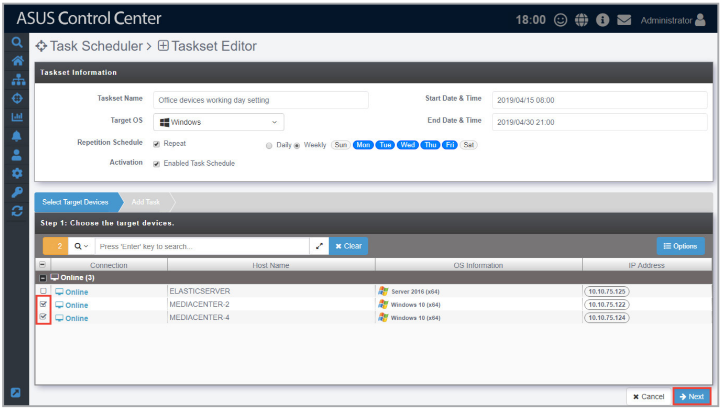
Step 1: Choose the target devices.

2
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	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122
☑ Online	MEDIACENTER-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**.



Taskset Information

Taskset Name: Office devices working day setting

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

Target OS: Windows

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

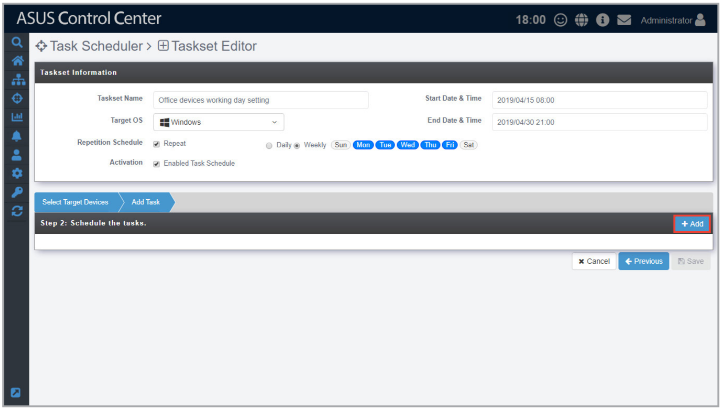
Repetition Schedule: ☑ Repeat ○ Daily ● Weekly Sun Mon Tue Wed Thu Fri Sat

Activation: ☑ Enabled Task Schedule

Step 1: Choose the target devices.

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

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



Taskset Information

Taskset Name: Office devices working day setting

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

Target OS: Windows

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

Repetition Schedule: ☑ Repeat ○ Daily ● Weekly Sun Mon Tue Wed Thu Fri Sat

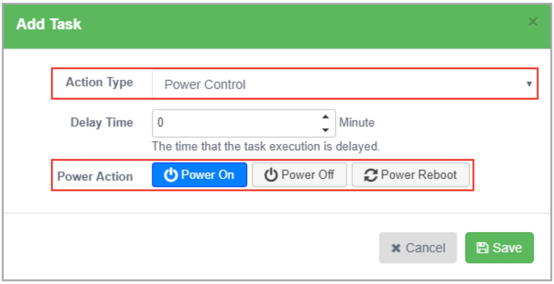
Activation: ☑ Enabled Task Schedule

Step 2: Schedule the tasks.

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

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

Power Control:



Add Task

Action Type: Power Control

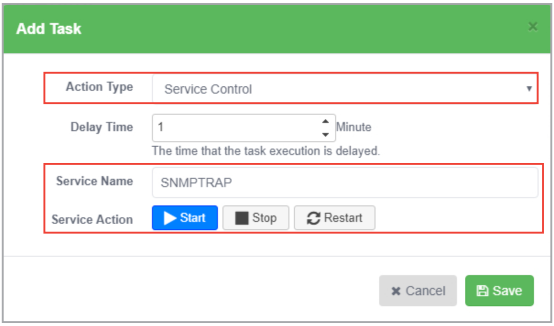
Delay Time: 0 Minute

The time that the task execution is delayed.

Power Action: Power On

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

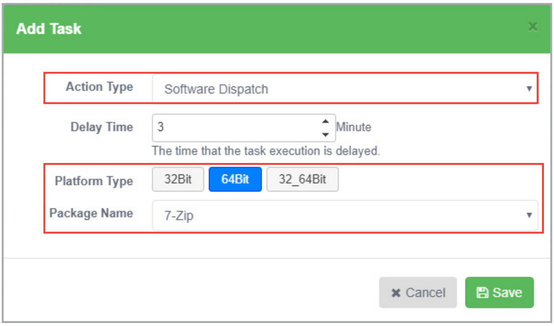
The time that the task execution is delayed.

Service Name: SNMPTRAP

Service Action: Start

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 **Software** 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

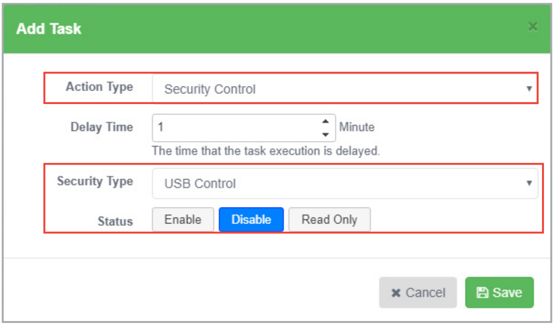
The time that the task execution is delayed.

Platform Type: 32Bit [✓ 64Bit] 32_64Bit

Package Name: 7-Zip

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

Security Control:



Add Task

Action Type: Security Control

Delay Time: 1 Minute

The time that the task execution is delayed.

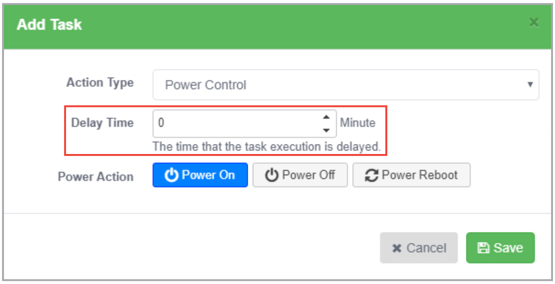
Security Type: USB Control

Status: Enable [✓ Disable] Read Only

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.
		Disable	Disables Watchdog timer.
	Registry Tool	Enable	Enable access to Regedit Tool.
		Disable	Disable access to Regedit Tool.

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

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



Add Task

Action Type: Power Control

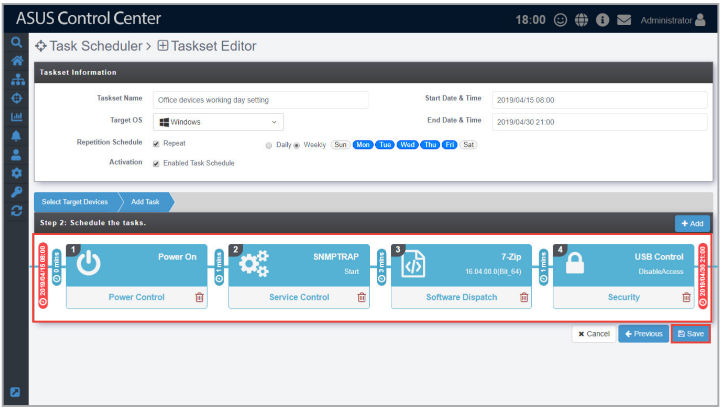
Delay Time: 0 Minute

The time that the task execution is delayed.

Power Action: Power On

11. 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.

12. When you are finished, click on the **Save** at the bottom of the screen.



ASUS Control Center

Task Scheduler > Taskset Editor

Taskset Information

Taskset Name: Office devices working day setting

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

Target OS: Windows

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

Repetition Schedule: ☑ Repeat ○ Daily ● Weekly Sun **Mon** **Tue** **Wed** **Thu** **Fri** Sat

Activation: ☑ Enabled Task Schedule

Step 2: Schedule the tasks.

1 Power On — Power Control (0 mins)

2 SNMPTRAP Start — Service Control (1 mins)

3 7-Zip 16.04.00.0(Bit_64) — Software Dispatch (3 mins)

4 USB Control DisableAccess — Security (1 mins)

Editing a scheduled task

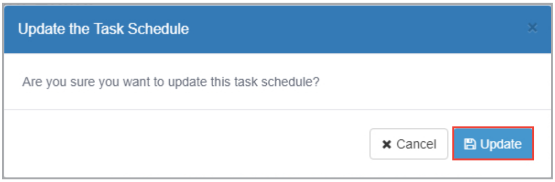
1. Click on the task you wish to edit on the calendar in Calendar view.

   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.

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.



Update the Task Schedule

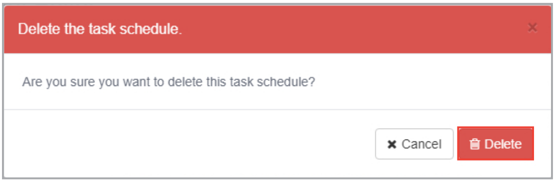
Are you sure you want to update this task schedule?

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.

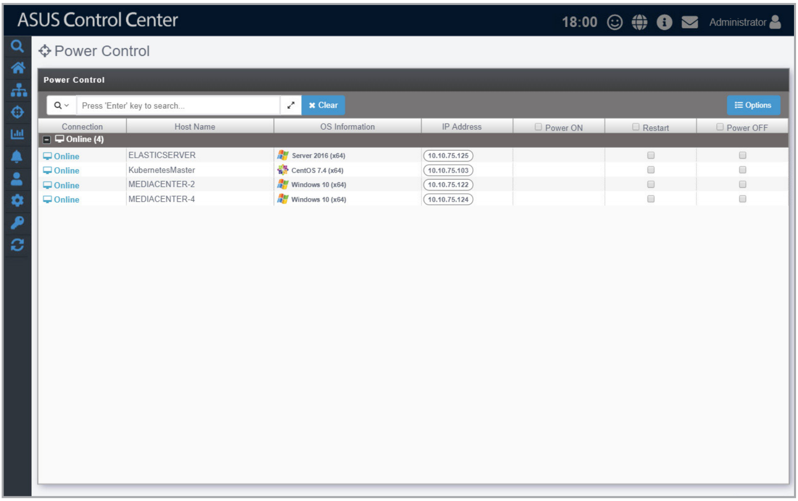


Delete the task schedule.

Are you sure you want to delete this task schedule?

4.6 Power Control

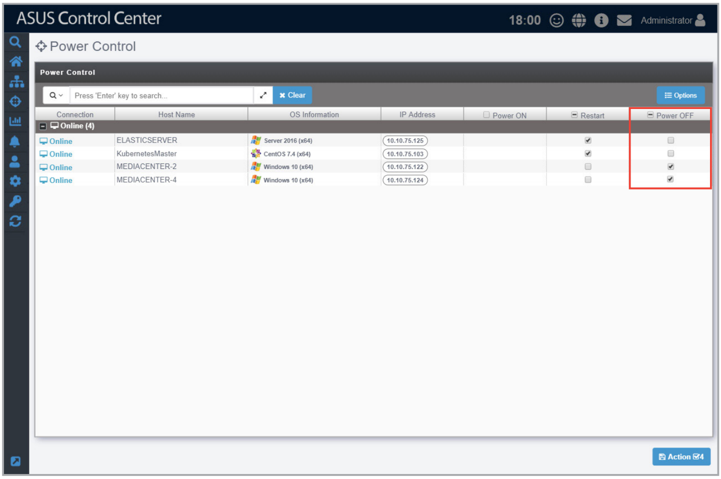
Power Control allows you to control the power settings of managed devices all from a centralized location. The centralized control over the power settings for managed devices makes it so that you do not have to manually power off, power on, or restart each managed device individually.



Connection	Host Name	OS Information	IP Address	□ Power ON	□ Restart	□ Power OFF
Online (4)						
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125		□	□
Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103		□	□
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		□	□
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		□	□

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

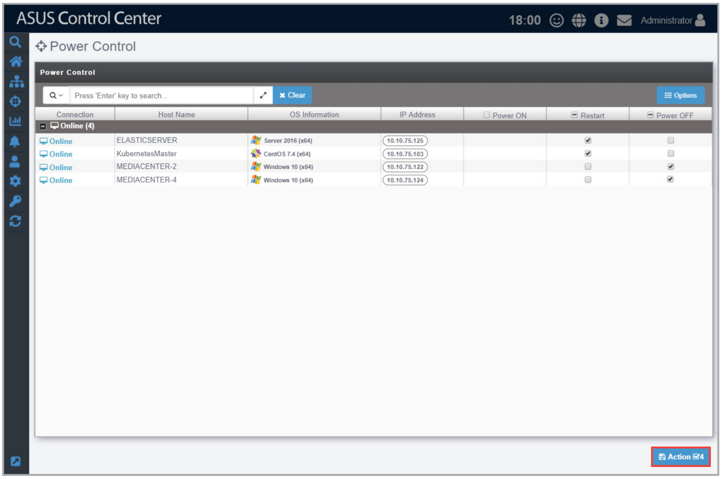
1. Check the **Power ON** / **Power OFF** / **Restart** check boxes of devices you would like to power on / power off / restart, or you may check the column title to check all devices eligible for the chosen action.



Connection	Host Name	OS Information	IP Address	□ Power ON	⊟ Restart	⊟ Power OFF
Online (4)						
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125		☑	□
Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103		☑	□
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		□	☑
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		□	☑

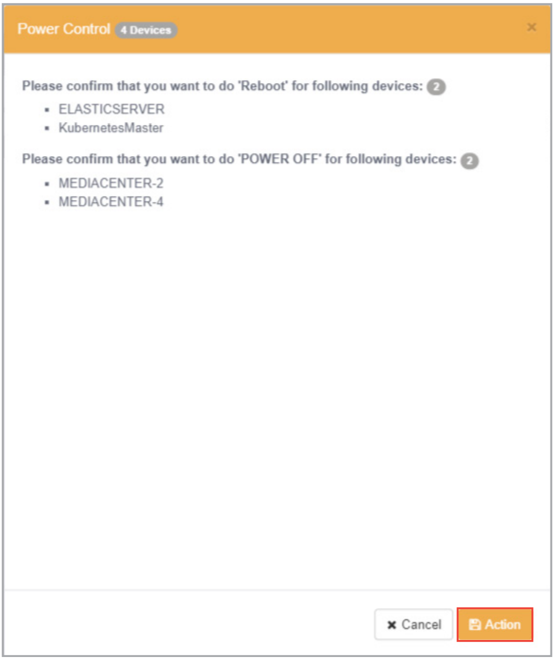
The availability of the **Power ON**, **Power OFF**, and **Restart** check boxes will vary according to the current power status of the managed device.

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



Connection	Host Name	OS Information	IP Address	□ Power ON	⊟ Restart	⊟ Power OFF
⊟ Online (4)						
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125		☑	□
Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103		☑	□
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122		□	☑
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124		□	☑

A pop-up window should appear, displaying your selected actions and devices, this will help you check to see if the right devices and actions are selected before executing the power on, power off, or restart action. Click **Action** when you have confirmed the actions and devices.



Please confirm that you want to do 'Reboot' for following devices: 2

- ELASTICSERVER
- KubernetesMaster

Please confirm that you want to do 'POWER OFF' for following devices: 2

- MEDIACENTER-2
- MEDIACENTER-4

Chapter 5

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

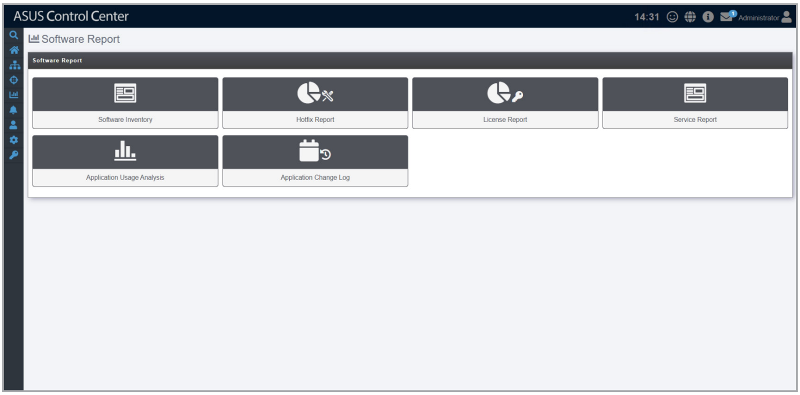
Report

5.1 Software Report

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**.



- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

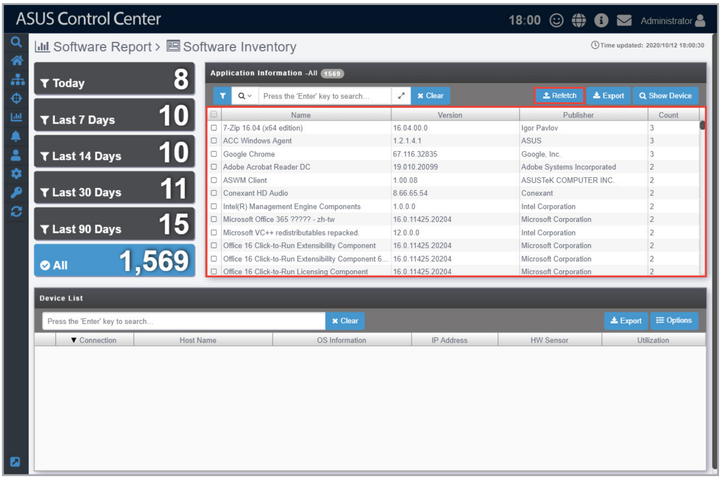
5.1.1 Software Inventory

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.

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.

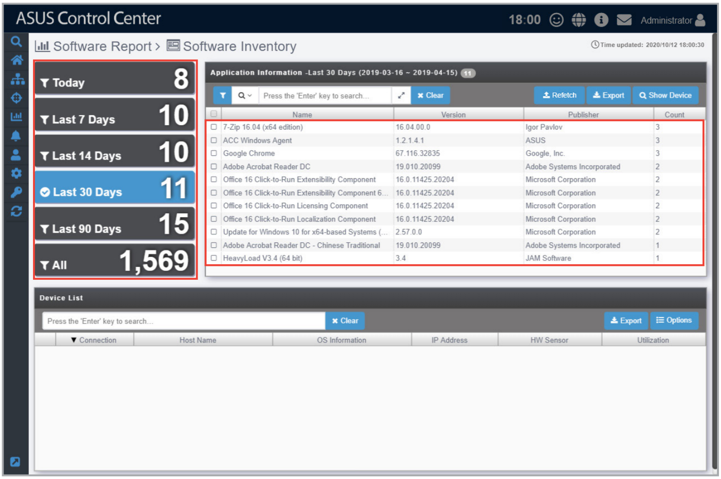

ASUS Control Center
18:00
Administrator
Software Report > Software Inventory
Time updated: 2020/10/12 18:00:30
Today 8
Last 7 Days 10
Last 14 Days 10
Last 30 Days 11
Last 90 Days 15
All 1,569
Application Information -All 1569
Press the 'Enter' key to search...
Clear
Refetch
Export
Show Device
Device List
Press the 'Enter' key to search...
Clear
Export
Options

□	Name	Version	Publisher	Count
□	7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	3
□	ACC Windows Agent	1.2.1.4.1	ASUS	3
□	Google Chrome	67.116.32835	Google, Inc.	3
□	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Incorporated	2
□	ASWM Client	1.00.08	ASUSTeK COMPUTER INC.	2
□	Conexant HD Audio	8.66.65.54	Conexant	2
□	Intel(R) Management Engine Components	1.0.0.0	Intel Corporation	2
□	Microsoft Office 365 ????? - zh-tw	16.0.11425.20204	Microsoft Corporation	2
□	Microsoft VC++ redistributables repacked.	12.0.0.0	Intel Corporation	2
□	Office 16 Click-to-Run Extensibility Component	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Extensibility Component 6...	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Licensing Component	16.0.11425.20204	Microsoft Corporation	2

	▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization

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.


ASUS Control Center
18:00
Administrator
Software Report > Software Inventory
Time updated: 2020/10/12 18:00:30
Today 8
Last 7 Days 10
Last 14 Days 10
Last 30 Days 11
Last 90 Days 15
All 1,569
Application Information -Last 30 Days (2019-03-16 ~ 2019-04-15) 11
Press the 'Enter' key to search...
Clear
Refetch
Export
Show Device
Device List
Press the 'Enter' key to search...
Clear
Export
Options

□	Name	Version	Publisher	Count
□	7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	3
□	ACC Windows Agent	1.2.1.4.1	ASUS	3
□	Google Chrome	67.116.32835	Google, Inc.	3
□	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Incorporated	2
□	Office 16 Click-to-Run Extensibility Component	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Extensibility Component 6...	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Licensing Component	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Localization Component	16.0.11425.20204	Microsoft Corporation	2
□	Update for Windows 10 for x64-based Systems (...	2.57.0.0	Microsoft Corporation	2
□	Adobe Acrobat Reader DC - Chinese Traditional	19.010.20099	Adobe Systems Incorporated	1
□	HeavyLoad V3.4 (64 bit)	3.4	JAM Software	1

	▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization

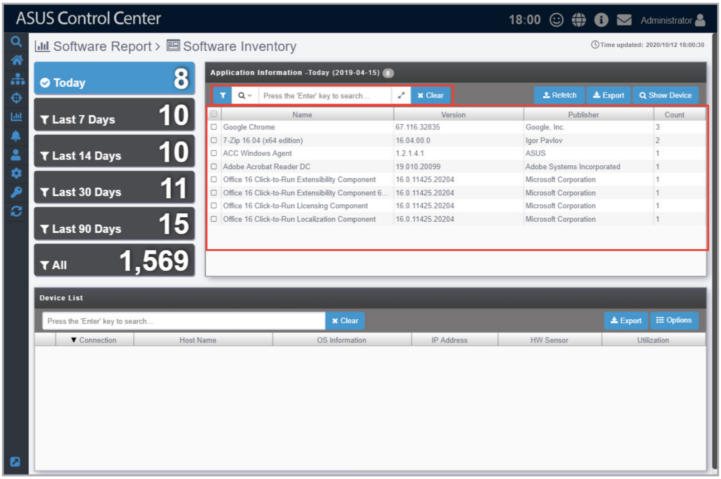
Search for applications using keywords

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

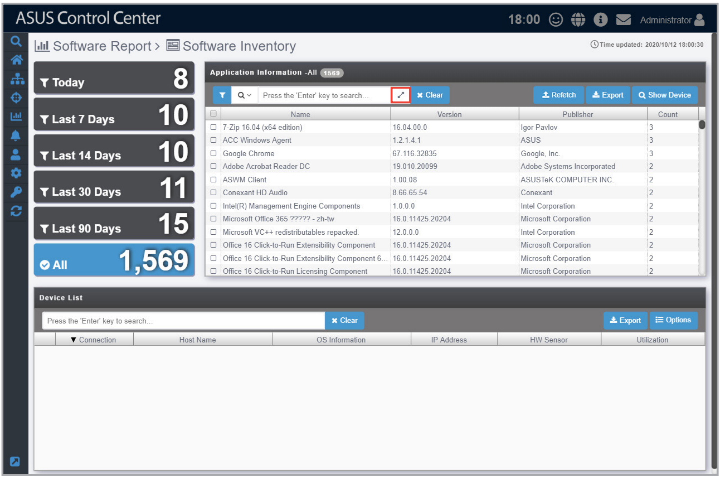
     Enter the keyword(s) you wish to search with into the search bar and press <Enter>. Click on 🔍 ˅ to toggle between searching with the **AND** operator or **OR** operator. Searching using **AND** will search for items which contain all keywords entered, whilst searching using **OR** will search for items which contain at least one of the keywords entered.



☐	Name	Version	Publisher	Count
☐	Google Chrome	67.116.32835	Google, Inc.	3
☐	7-Zip 16.04 (x64 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

- Importing multiple keywords from a .csv file

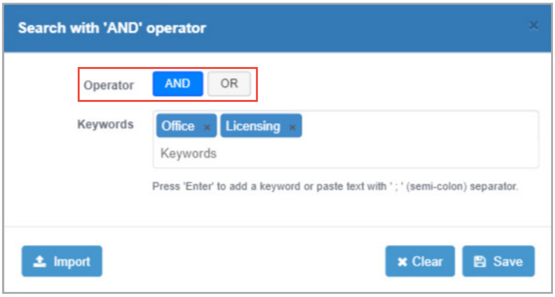
  a. Click on ⤢ to bring up the search condition pop-up window.



	Name	Version	Publisher	Count
□	7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	3
□	ACC Windows Agent	1.2.1.4.1	ASUS	3
□	Google Chrome	67.116.32835	Google, Inc.	3
□	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Incorporated	2
□	ASWM Client	1.00.08	ASUSTeK COMPUTER INC.	2
□	Conexant HD Audio	8.66.65.54	Conexant	2
□	Intel(R) Management Engine Components	1.0.0.0	Intel Corporation	2
□	Microsoft Office 365 ????? - zh-tw	16.0.11425.20204	Microsoft Corporation	2
□	Microsoft VC++ redistributables repacked.	12.0.0.0	Intel Corporation	2
□	Office 16 Click-to-Run Extensibility Component	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Extensibility Component 6...	16.0.11425.20204	Microsoft Corporation	2
□	Office 16 Click-to-Run Licensing Component	16.0.11425.20204	Microsoft Corporation	2

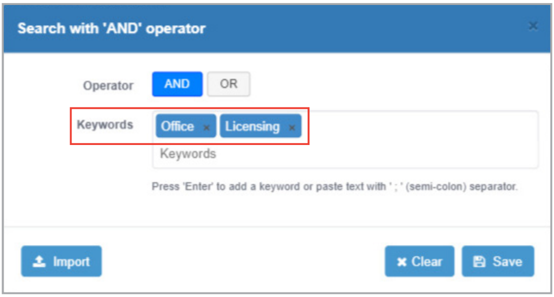
Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization

  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.



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

c. Enter the keyword(s) you wish to search with into the **Keywords** field and press <Enter>.

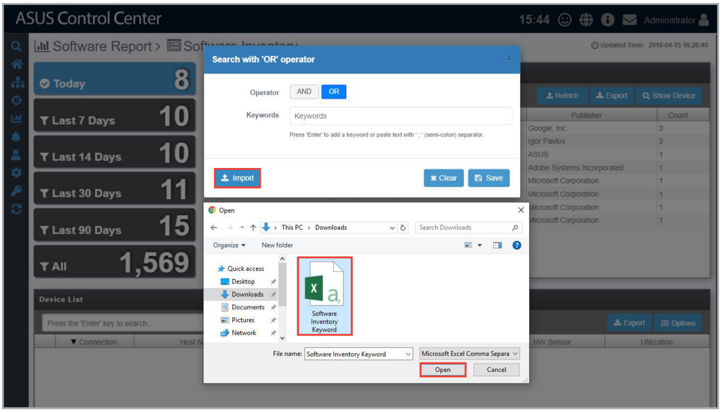

Search with 'AND' operator

Operator: AND / OR

Keywords: Office × Licensing ×

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

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

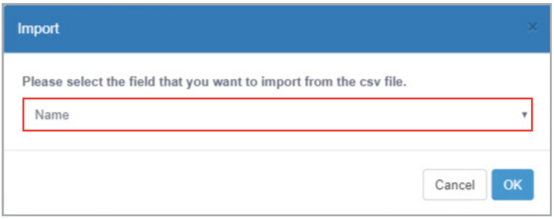
Operator: AND / OR

Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

File name: Software Inventory Keyword

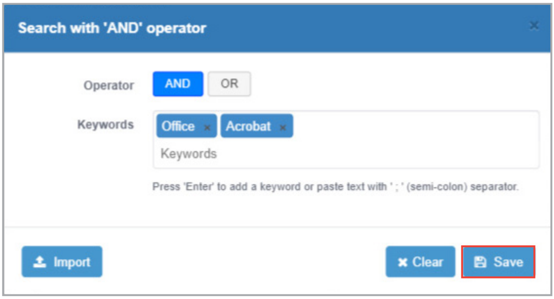
Microsoft Excel Comma Separa


Import

Please select the field that you want to import from the csv file.

Name

d. Click on **Save** once you have finished setting the search conditions.



Search with 'AND' operator

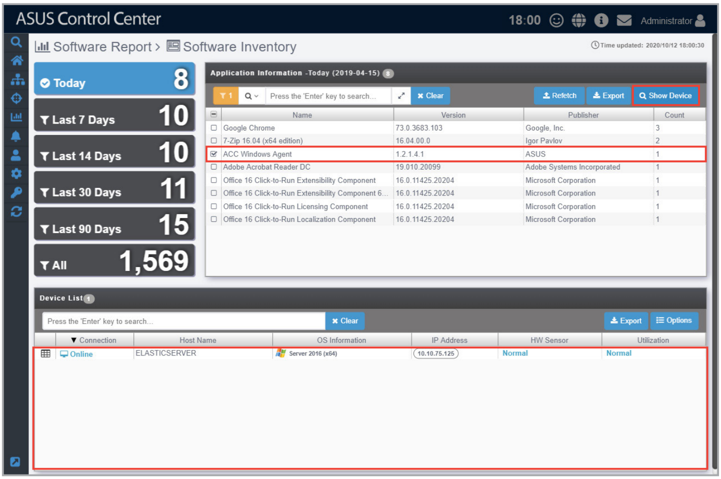
Operator: AND | OR

Keywords: Office × Acrobat ×

Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

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



Time updated: 2020/10/12 18:00:30

Application Information -Today (2019-04-15) 8

Press the 'Enter' key to search...

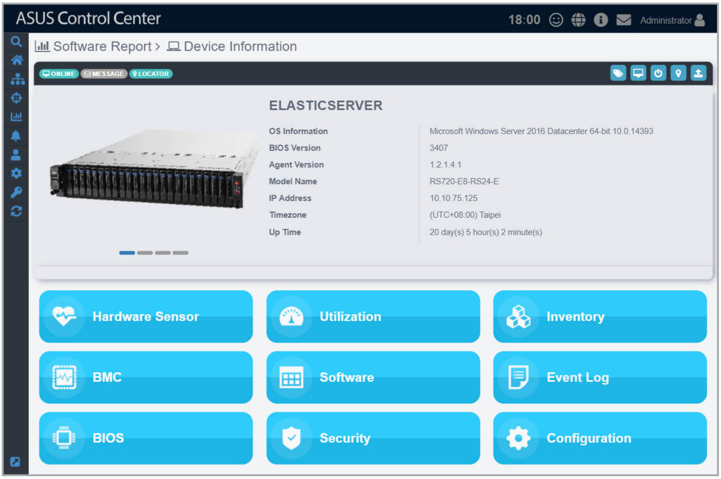
	Name	Version	Publisher	Count
☐	Google Chrome	73.0.3683.103	Google, Inc.	3
☐	7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	2
☑	ACC Windows Agent	1.2.1.4.1	ASUS	1
☐	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Incorporated	1
☐	Office 16 Click-to-Run Extensibility Component	16.0.11425.20204	Microsoft 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 1

Press the 'Enter' key to search...

	▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	Normal

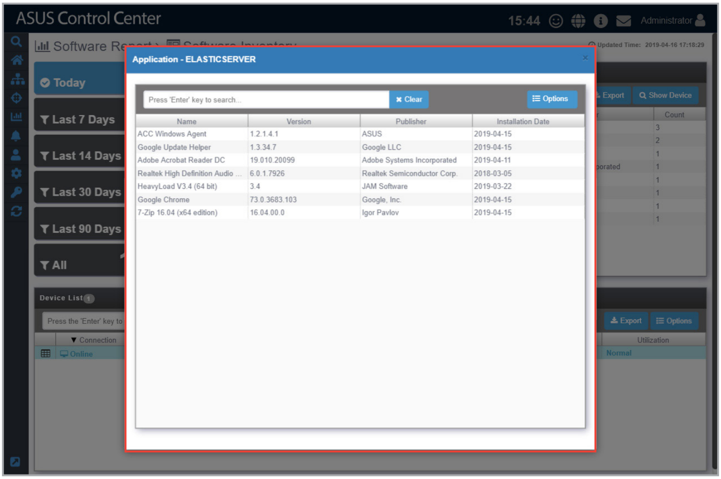
3. (optional) Clicking on ☰ next to each device in the **Device List** will allow you to view the Device Information.



ELASTICSERVER

OS Information	Microsoft Windows Server 2016 Datacenter 64-bit 10.0.14393
BIOS Version	3407
Agent Version	1.2.1.4.1
Model Name	RS720-E8-RS24-E
IP Address	10.10.75.125
Timezone	(UTC+08:00) Taipei
Up Time	20 day(s) 5 hour(s) 2 minute(s)

4. (optional) Clicking on the device will display all applications on the selected device.



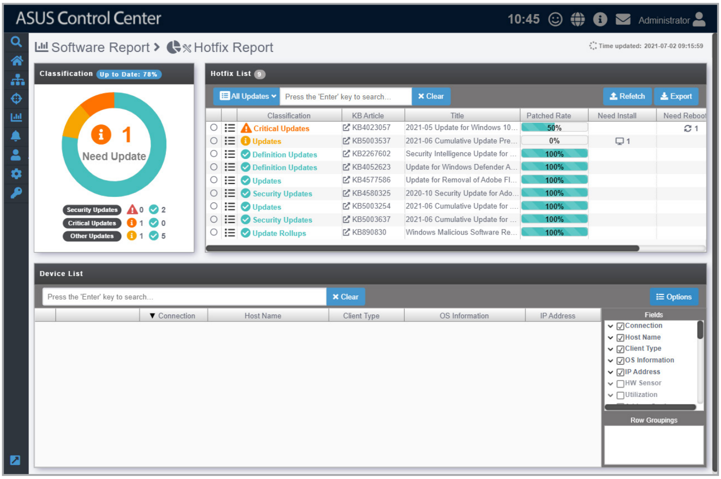
Application - ELASTICSERVER

Name	Version	Publisher	Installation Date
ACC Windows Agent	1.2.1.4.1	ASUS	2019-04-15
Google Update Helper	1.3.34.7	Google LLC	2019-04-15
Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Incorporated	2019-04-11
Realtek High Definition Audio ...	6.0.1.7926	Realtek Semiconductor Corp.	2018-03-05
HeavyLoad V3.4 (64 bit)	3.4	JAM Software	2019-03-22
Google Chrome	73.0.3683.103	Google, Inc.	2019-04-15
7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	2019-04-15

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.

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



ASUS Control Center 10:45 Administrator

Software Report > Hotfix Report

Time updated: 2021-07-02 09:15:59

Classification Up to Date: 78%

1 Need Update

Security Updates	0	2
Critical Updates	1	0
Other Updates	1	5

Hotfix List 9

All Updates | Press the 'Enter' key to search... | ✕ Clear | Refetch | Export

		Classification	KB Article	Title	Patched Rate	Need Install	Need Reboot
○	☰	Critical Updates	KB4023057	2021-05 Update for Windows 10...	50%		1
○	☰	Updates	KB5003537	2021-06 Cumulative Update Pre...	0%	1	
○	☰	Definition Updates	KB2267602	Security Intelligence Update for ...	100%		
○	☰	Definition Updates	KB4052623	Update for Windows Defender A...	100%		
○	☰	Updates	KB4577586	Update for Removal of Adobe Fl...	100%		
○	☰	Security Updates	KB4580325	2020-10 Security Update for Ado...	100%		
○	☰	Updates	KB5003254	2021-06 Cumulative Update for	100%		
○	☰	Security Updates	KB5003637	2021-06 Cumulative Update for ...	100%		
○	☰	Update Rollups	KB890830	Windows Malicious Software Re...	100%		

Device List

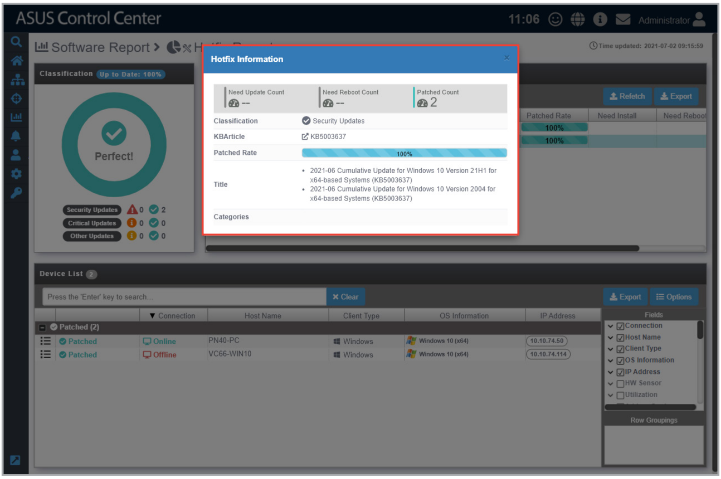
Press the 'Enter' key to search... | ✕ Clear | Options

		▼ Connection	Host Name	Client Type	OS Information	IP Address

Fields
- ☑Connection
- ☑Host Name
- ☑Client Type
- ☑OS Information
- ☑IP Address
- □HW Sensor
- □Utilization

Row Groupings

Clicking on ☰ next to a hotfix update in the Hotfix List will allow you to view more details on the hotfix.



ASUS Control Center 11:06 Administrator

Software Report > Hotfix Report

Time updated: 2021-07-02 09:15:59

Classification Up to Date: 100%

Perfect!

Security Updates	0	2
Critical Updates	0	0
Other Updates	0	0

Hotfix Information

Need Update Count	Need Reboot Count	Patched Count
--	--	2

Classification	Security Updates
KBArticle	KB5003637
Patched Rate	100%
Title	• 2021-06 Cumulative Update for Windows 10 Version 21H1 for x64-based Systems (KB5003637) • 2021-06 Cumulative Update for Windows 10 Version 2004 for x64-based Systems (KB5003637)
Categories	

Device List 2

Press the 'Enter' key to search... | ✕ Clear | Export | Options

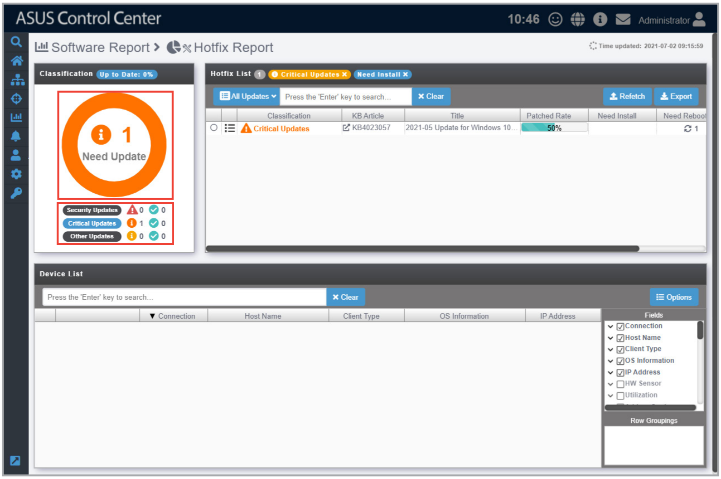
		▼ Connection	Host Name	Client Type	OS Information	IP Address
Patched (2)						
☰	Patched	Online	PN40-PC	Windows	Windows 10 (x64)	10.10.74.50
☰	Patched	Offline	VC66-WIN10	Windows	Windows 10 (x64)	10.10.74.114

Fields
- ☑Connection
- ☑Host Name
- ☑Client Type
- ☑OS Information
- ☑IP Address
- □HW Sensor
- □Utilization

Row Groupings

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.



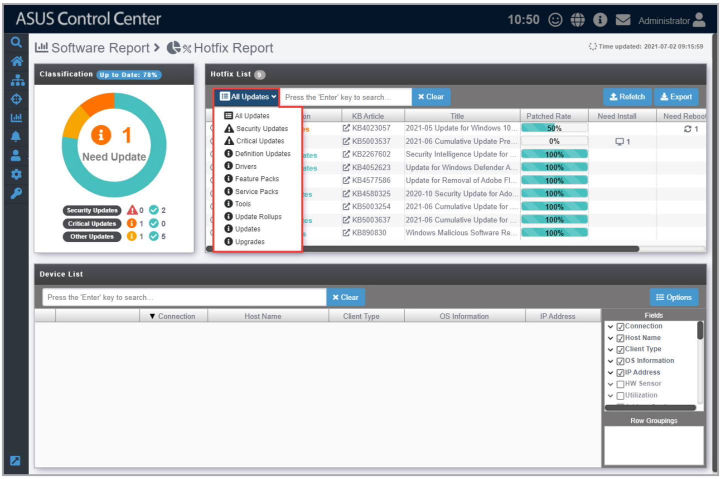
		Classification	KB Article	Title	Patched Rate	Need Install	Need Reboot
○	☰	Critical Updates	KB4023057	2021-05 Update for Windows 10...	50%		1

		▼ Connection	Host Name	Client Type	OS Information	IP Address

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.

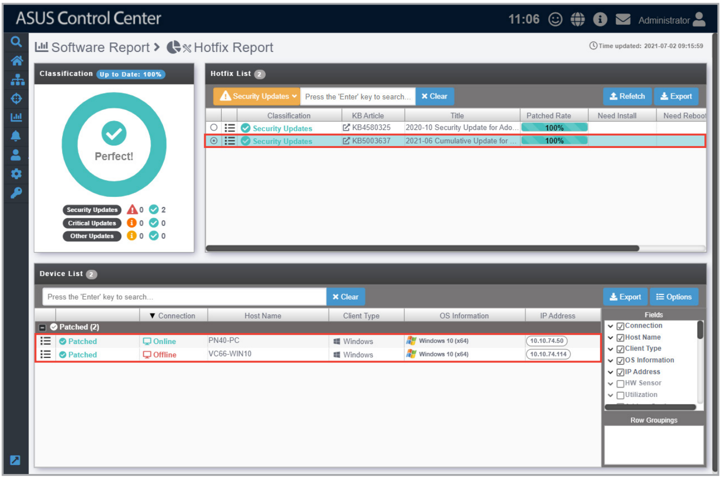


KB Article	Title	Patched Rate	Need Install	Need Reboot
KB4023057	2021-05 Update for Windows 10...	50%		1
KB5003537	2021-06 Cumulative Update Pre...	0%	1	
KB2267602	Security Intelligence Update for ...	100%		
KB4052623	Update for Windows Defender A...	100%		
KB4577586	Update for Removal of Adobe Fl...	100%		
KB4580325	2020-10 Security Update for Ado...	100%		
KB5003254	2021-06 Cumulative Update for	100%		
KB5003637	2021-06 Cumulative Update for ...	100%		
KB890830	Windows Malicious Software Re...	100%		

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.

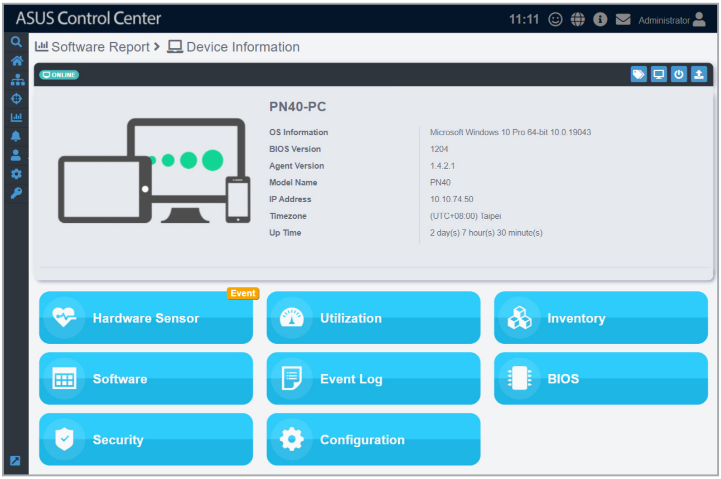


		Classification	KB Article	Title	Patched Rate	Need Install	Need Reboot
○	☰	Security Updates	KB4580325	2020-10 Security Update for Ado...	100%		
●	☰	Security Updates	KB5003637	2021-06 Cumulative Update for ...	100%		

		▼ Connection	Host Name	Client Type	OS Information	IP Address
Patched (2)						
☰	Patched	Online	PN40-PC	Windows	Windows 10 (x64)	10.10.74.50
☰	Patched	Offline	VC66-WIN10	Windows	Windows 10 (x64)	10.10.74.114

Fields:
- ☑ Connection
- ☑ Host Name
- ☑ Client Type
- ☑ OS Information
- ☑ IP Address
- □ HW Sensor
- □ Utilization

You may also click on ☰ next to each device in the **Device List** to view the Device Information.



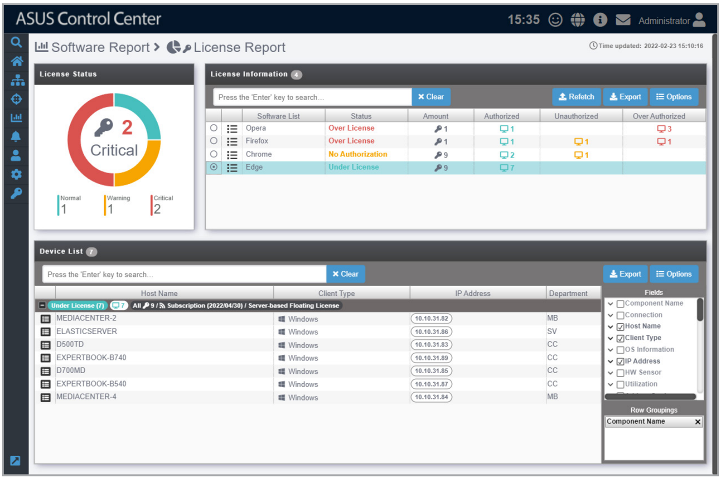
PN40-PC

OS Information	Microsoft Windows 10 Pro 64-bit 10.0.19043
BIOS Version	1204
Agent Version	1.4.2.1
Model Name	PN40
IP Address	10.10.74.50
Timezone	(UTC+08:00) Taipei
Up Time	2 day(s) 7 hour(s) 30 minute(s)

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.

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



		Software List	Status	Amount	Authorized	Unauthorized	Over Authorized
○	☰	Opera	Over License	1	1		3
○	☰	Firefox	Over License	1	1	1	1
○	☰	Chrome	No Authorization	9	2	1	
●	☰	Edge	Under License	9	7		

Under License (7) 7 All 9 / Subscription (2022/04/30) / Server-based Floating License

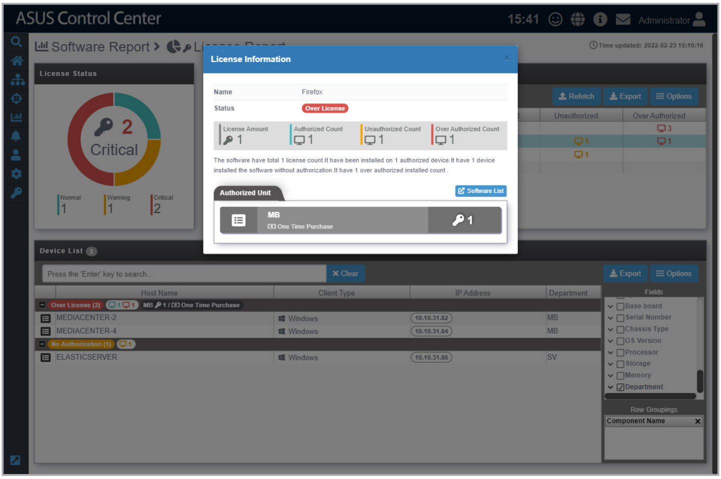
	Host Name	Client Type	IP Address	Department
☰	MEDIACENTER-2	Windows	10.10.31.82	MB
☰	ELASTICSERVER	Windows	10.10.31.86	SV
☰	D500TD	Windows	10.10.31.83	CC
☰	EXPERTBOOK-B740	Windows	10.10.31.89	CC
☰	D700MD	Windows	10.10.31.85	CC
☰	EXPERTBOOK-B540	Windows	10.10.31.87	CC
☰	MEDIACENTER-4	Windows	10.10.31.84	MB

Fields
- □ Component Name
- □ Connection
- ☑ Host Name
- ☑ Client Type
- □ OS Information
- ☑ IP Address
- □ HW Sensor
- □ Utilization

Row Groupings
Component Name ✕

Viewing information on the license

Click on ☰ next to a selected license to view more information about the license.



License Information

Name	Firefox
Status	Over License

License Amount	Authorized Count	Unauthorized Count	Over Authorized Count
1	1	1	1

The software have total 1 license count.It have been installed on 1 authorized device.It have 1 device installed the software without authorization.It have 1 over authorized installed count .

Authorized Unit

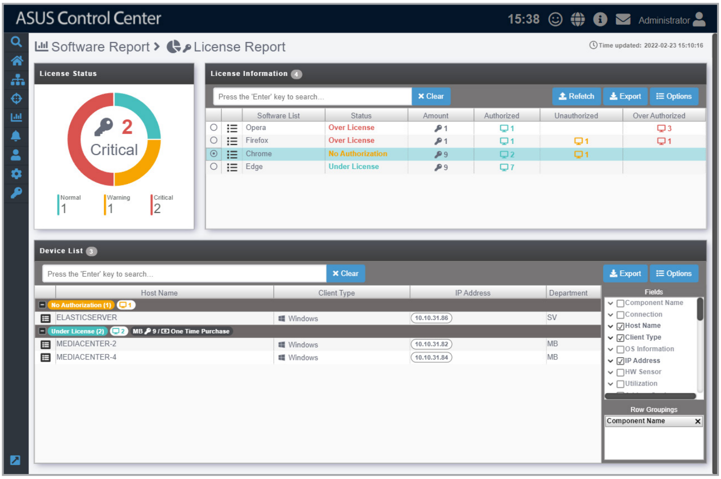
Software List

MB
One Time Purchase
1

Host Name	Client Type	IP Address	Department
Over License (2) 1 1 MB 1 / One Time Purchase			
MEDIACENTER-2	Windows	10.10.31.82	MB
MEDIACENTER-4	Windows	10.10.31.84	MB
No Authorization (1) 1			
ELASTICSERVER	Windows	10.10.31.86	SV

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.



		Software List	Status	Amount	Authorized	Unauthorized	Over Authorized
○		Opera	Over License	1	1		3
○		Firefox	Over License	1	1	1	1
●		Chrome	No Authorization	9	2	1	
○		Edge	Under License	9	7		

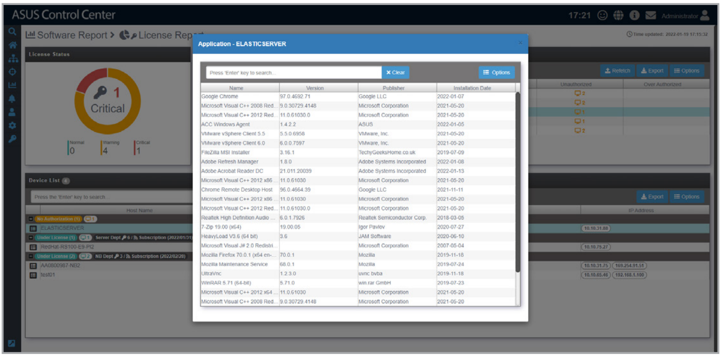
	Host Name	Client Type	IP Address	Department
No Authorization (1) 1				
	ELASTICSERVER	Windows	10.10.31.86	SV
Under License (2) 2 MB 9 / One Time Purchase				
	MEDIACENTER-2	Windows	10.10.31.82	MB
	MEDIACENTER-4	Windows	10.10.31.84	MB

Fields:
- ☐ Component Name
- ☐ Connection
- ☑ Host Name
- ☑ Client Type
- ☐ OS Information
- ☑ IP Address
- ☐ HW Sensor
- ☐ Utilization

Row Groupings: Component Name ✕

- **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.



ASUS Control Center
Software Report > License Report
License Status
Device List
Press 'Enter' key to search...
✕ Clear
Options

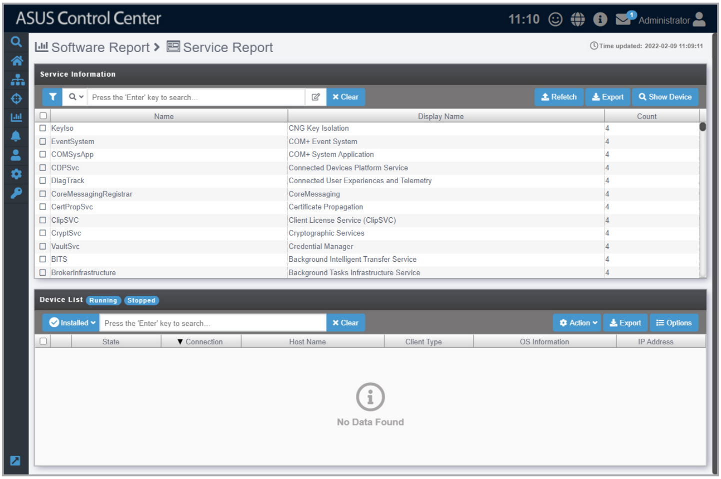
Application - ELASTICSERVER

Name	Version	Publisher	Installation Date
Google Chrome	97.0.4692.71	Google LLC	2022-01-07
Microsoft Visual C++ 2008 Red...	9.0.30729.4148	Microsoft Corporation	2021-05-20
Microsoft Visual C++ 2012 Red...	11.0.61030.0	Microsoft Corporation	2021-05-20
ACC Windows Agent	1.4.2.2	ASUS	2022-01-05
VMware vSphere Client 5.5	5.5.0.6958	VMware, Inc.	2021-05-20
VMware vSphere Client 6.0	6.0.0.7597	VMware, Inc.	2021-05-20
FileZilla MSI Installer	3.16.1	TechyGeeksHome.co.uk	2019-07-09
Adobe Refresh Manager	1.8.0	Adobe Systems Incorporated	2022-01-08
Adobe Acrobat Reader DC	21.011.20039	Adobe Systems Incorporated	2022-01-13
Microsoft Visual C++ 2012 x86 ...	11.0.61030	Microsoft Corporation	2021-05-20
Chrome Remote Desktop Host	96.0.4664.39	Google LLC	2021-11-11
Microsoft Visual C++ 2012 x86 ...	11.0.61030	Microsoft Corporation	2021-05-20
Microsoft Visual C++ 2012 Red...	11.0.61030.0	Microsoft Corporation	2021-05-20
Realtek High Definition Audio ...	6.0.1.7926	Realtek Semiconductor Corp.	2018-03-05
7-Zip 19.00 (x64)	19.00.05	Igor Pavlov	2020-07-27
HeavyLoad V3.6 (64 bit)	3.6	JAM Software	2020-06-10
Microsoft Visual J# 2.0 Redistri...		Microsoft Corporation	2007-05-04
Mozilla Firefox 70.0.1 (x64 en-...	70.0.1	Mozilla	2019-11-18
Mozilla Maintenance Service	68.0.1	Mozilla	2019-07-24
UltraVnc	1.2.3.0	uvnc bvba	2019-11-18
WinRAR 5.71 (64-bit)	5.71.0	win.rar GmbH	2019-07-23
Microsoft Visual C++ 2012 x64 ...	11.0.61030	Microsoft Corporation	2021-05-20
Microsoft Visual C++ 2008 Red...	9.0.30729.4148	Microsoft Corporation	2021-05-20

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.

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



ASUS Control Center
11:10
1
Administrator
Software Report > Service Report
Time updated: 2022-02-09 11:09:11
Service Information
Press the 'Enter' key to search...
Clear
Refetch
Export
Show Device

□	Name	Display Name	Count
□	KeyIso	CNG Key Isolation	4
□	EventSystem	COM+ Event System	4
□	COMSysApp	COM+ System Application	4
□	CDPSvc	Connected Devices Platform Service	4
□	DiagTrack	Connected User Experiences and Telemetry	4
□	CoreMessagingRegistrar	CoreMessaging	4
□	CertPropSvc	Certificate Propagation	4
□	ClipSVC	Client License Service (ClipSVC)	4
□	CryptSvc	Cryptographic Services	4
□	VaultSvc	Credential Manager	4
□	BITS	Background Intelligent Transfer Service	4
□	BrokerInfrastructure	Background Tasks Infrastructure Service	4

□		State	▼ Connection	Host Name	Client Type	OS Information	IP Address

No Data Found

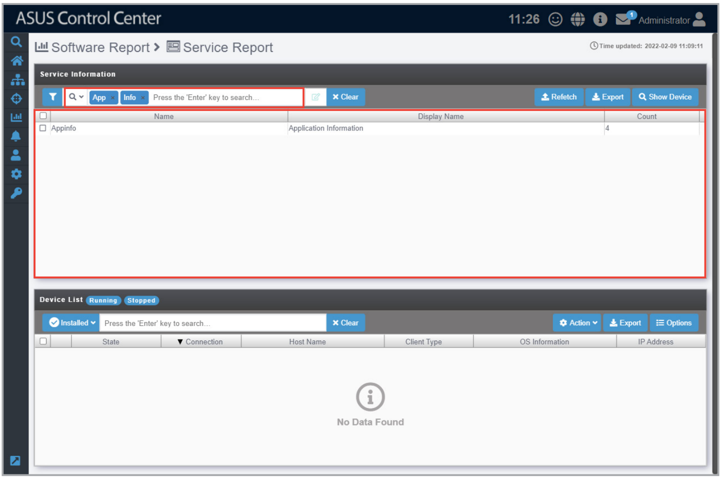
Search for services using keywords

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.



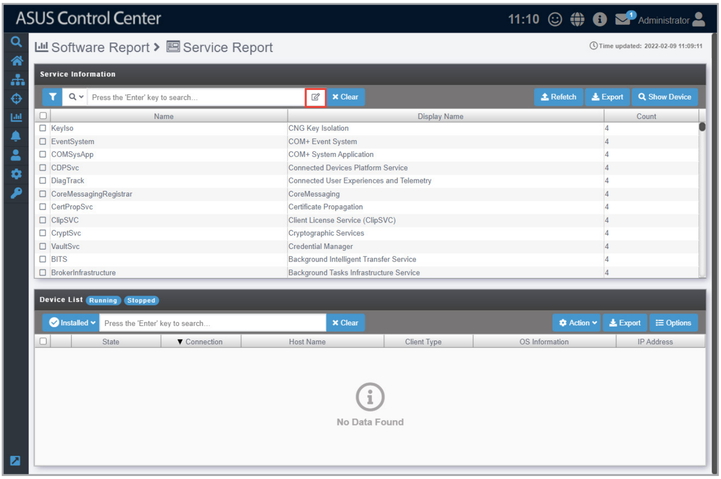
□	Name	Display Name	Count
□	Appinfo	Application Information	4

□		State	▼ Connection	Host Name	Client Type	OS Information	IP Address

No Data Found

- Importing multiple keywords from a .csv file

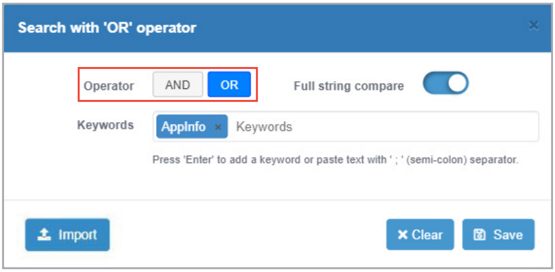
a. Click on [icon] to bring up the search condition pop-up window.



Name	Display Name	Count
KeyIso	CNG Key Isolation	4
EventSystem	COM+ Event System	4
COMSysApp	COM+ System Application	4
CDPSvc	Connected Devices Platform Service	4
DiagTrack	Connected User Experiences and Telemetry	4
CoreMessagingRegistrar	CoreMessaging	4
CertPropSvc	Certificate Propagation	4
ClipSVC	Client License Service (ClipSVC)	4
CryptSvc	Cryptographic Services	4
VaultSvc	Credential Manager	4
BITS	Background Intelligent Transfer Service	4
BrokerInfrastructure	Background Tasks Infrastructure Service	4

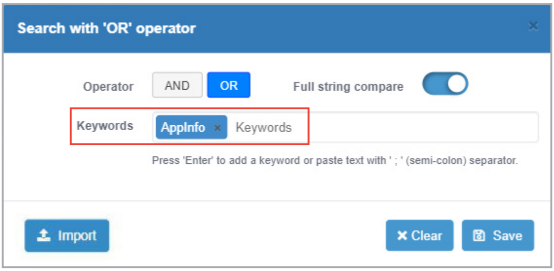
State	Connection	Host Name	Client Type	OS Information	IP Address

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.



Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

c. Enter the keyword(s) you wish to search with into the **Keywords** field and press <Enter>.

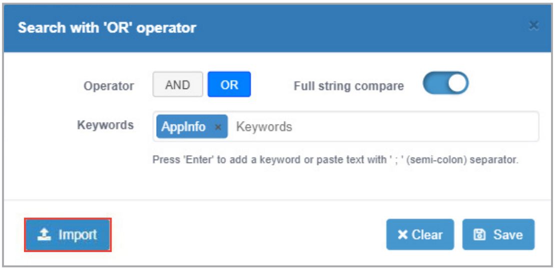

Search with 'OR' operator

Operator AND [✓ OR] Full string compare

Keywords AppInfo × Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

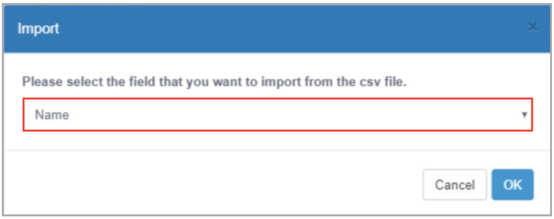
Import multiple keywords using a .csv file by click on **Import**, selecting the .csv file you wish to import, and then selecting the column in the .csv file you would like to import.


Search with 'OR' operator

Operator AND [✓ OR] Full string compare

Keywords AppInfo × Keywords

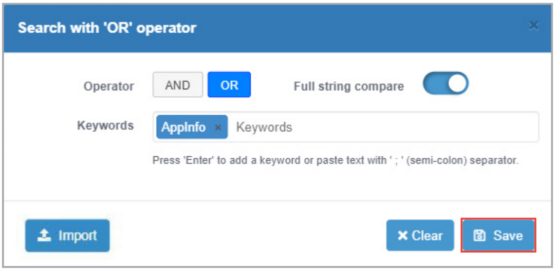
Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.


Import

Please select the field that you want to import from the csv file.

Name ▾

d. Click on **Save** once you have finished setting the search conditions.



Search with 'OR' operator

Operator: AND | OR

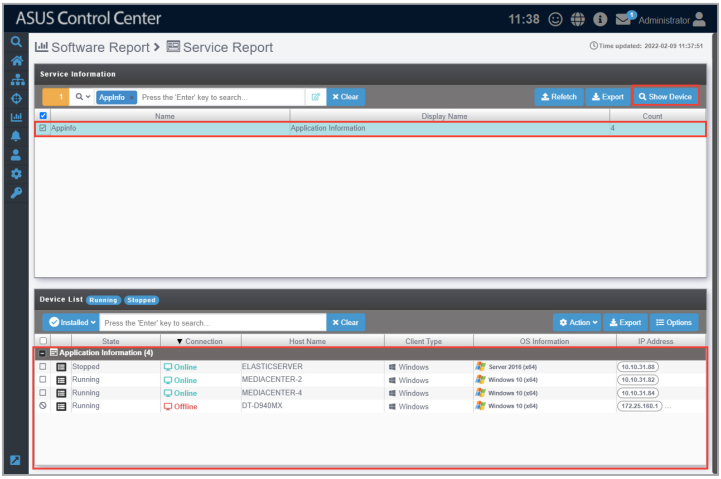
Full string compare

Keywords: AppInfo × Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

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.

You can also click on 1 to quickly deselect services already selected.



Time updated: 2022-02-09 11:37:51

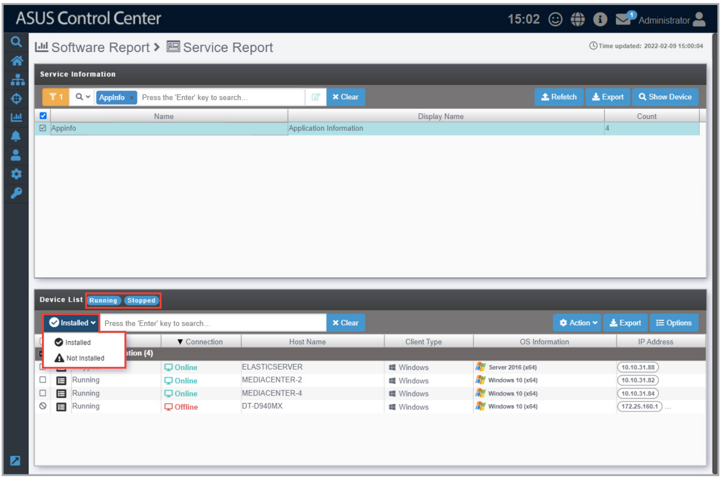
Service Information

☑	Name	Display Name	Count
☑	Appinfo	Application Information	4

Device List Running Stopped

□		State	▼ Connection	Host Name	Client Type	OS Information	IP Address
Application Information (4)							
□		Stopped	Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.88
□		Running	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.31.82
□		Running	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.31.84
⦸		Running	Offline	DT-D940MX	Windows	Windows 10 (x64)	172.25.160.1 ...

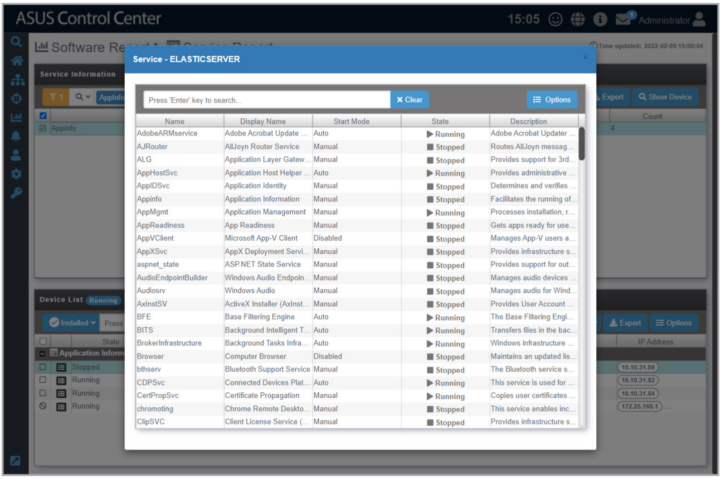
3. (optional) You may filter through the devices by clicking on the tags next to the Device List title, or filter by **Installed** or **Not Installed** by clicking on the drop down menu next to the search bar.


ASUS Control Center
15:02
Administrator
Software Report › Service Report
Time updated: 2022-02-09 15:00:04
Service Information
1
AppInfo
Press the 'Enter' key to search...
✖ Clear
Refetch
Export
Show Device

☑	Name	Display Name	Count
☑	Appinfo	Application Information	4

□			▼ Connection	Host Name	Client Type	OS Information	IP Address
⊟		...tion (4)					
□	☰		Online	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.88
□	☰	Running	Online	MEDIACENTER-2	Windows	Windows 10 (x64)	10.10.31.82
□	☰	Running	Online	MEDIACENTER-4	Windows	Windows 10 (x64)	10.10.31.84
⃠	☰	Running	Offline	DT-D940MX	Windows	Windows 10 (x64)	172.25.160.1 ...

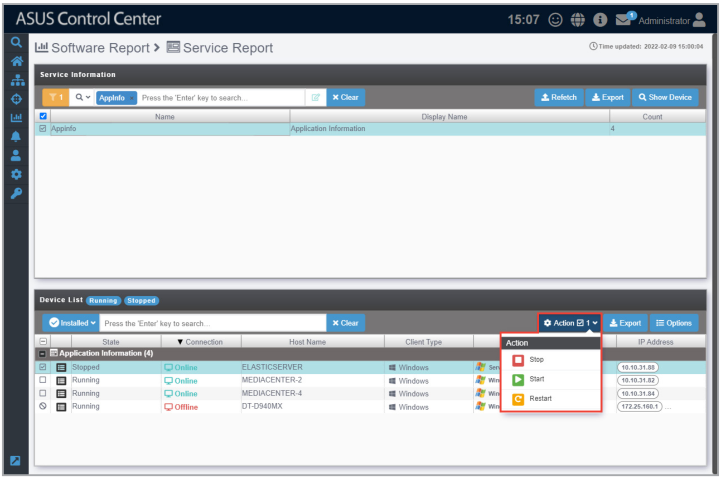
4. (optional) Clicking on ☰ next to each device in the **Device List** will allow you to view all services on the selected device.



Name	Display Name	Start Mode	State	Description
AdobeARMservice	Adobe Acrobat Update ...	Auto	▶ Running	Adobe Acrobat Updater ...
AJRouter	AllJoyn Router Service	Manual	■ Stopped	Routes AllJoyn messag...
ALG	Application Layer Gatew...	Manual	■ Stopped	Provides support for 3rd...
AppHostSvc	Application Host Helper ...	Auto	▶ Running	Provides administrative ...
AppIDSvc	Application Identity	Manual	■ Stopped	Determines and verifies ...
Appinfo	Application Information	Manual	■ Stopped	Facilitates the running of...
AppMgmt	Application Management	Manual	▶ Running	Processes installation, r...
AppReadiness	App Readiness	Manual	■ Stopped	Gets apps ready for use...
AppVClient	Microsoft App-V Client	Disabled	■ Stopped	Manages App-V users a...
AppXSvc	AppX Deployment Servi...	Manual	■ Stopped	Provides infrastructure s...
aspnet_state	ASP.NET State Service	Manual	■ Stopped	Provides support for out...
AudioEndpointBuilder	Windows Audio Endpoin...	Manual	■ Stopped	Manages audio devices ...
Audiosrv	Windows Audio	Manual	■ Stopped	Manages audio for Wind...
AxInstSV	ActiveX Installer (AxInst...	Manual	■ Stopped	Provides User Account ...
BFE	Base Filtering Engine	Auto	▶ Running	The Base Filtering Engi...
BITS	Background Intelligent T...	Auto	▶ Running	Transfers files in the bac...
BrokerInfrastructure	Background Tasks Infra...	Auto	▶ Running	Windows infrastructure ...
Browser	Computer Browser	Disabled	■ Stopped	Maintains an updated lis...
bthserv	Bluetooth Support Service	Manual	■ Stopped	The Bluetooth service s...
CDPSvc	Connected Devices Plat...	Auto	▶ Running	This service is used for ...
CertPropSvc	Certificate Propagation	Manual	▶ Running	Copies user certificates ...
chromoting	Chrome Remote Deskto...	Manual	■ Stopped	This service enables inc...
ClipSVC	Client License Service (...	Manual	■ Stopped	Provides infrastructure s...

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.



☑	Name	Display Name	Count
☑	Appinfo	Application Information	4

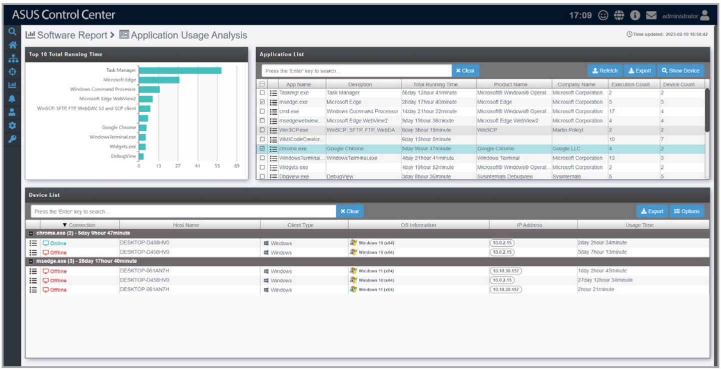
⊟		State	▼ Connection	Host Name	Client Type		IP Address
⊟	Application Information (4)						
☑		Stopped	Online	ELASTICSERVER	Windows	Serv	10.10.31.88
☐		Running	Online	MEDIACENTER-2	Windows	Win	10.10.31.82
☐		Running	Online	MEDIACENTER-4	Windows	Win	10.10.31.84
⦸		Running	Offline	DT-D940MX	Windows	Win	172.25.160.1 ...

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 **Refetch** button to refetch 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.

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


ASUS Control Center
17:09
administrator
Software Report > Application Usage Analysis
Time updated: 2023-02-10 16:58:42
Top 10 Total Running Time
Task Manager
Microsoft Edge
Windows Command Processor
Microsoft Edge WebView2
WinSCP: SFTP, FTP, WebDAV, S3 and SCP client
Google Chrome
WindowsTerminal.exe
Widgets.exe
DebugView
0
13
27
41
55
69
Application List
Press the 'Enter' key to search...
Clear
Refetch
Export
Show Device
Device List
Press the 'Enter' key to search...
Clear
Export
Options

⊟		App Name	Desription	Total Running Time	Product Name	Company Name	Execution Count	Device Count
□	☰	Taskmgr.exe	Task Manager	58day 13hour 41minute	Microsoft® Windows® Operat...	Microsoft Corporation	2	2
☑	☰	msedge.exe	Microsoft Edge	28day 17hour 40minute	Microsoft Edge	Microsoft Corporation	3	3
□	☰	cmd.exe	Windows Command Processor	14day 21hour 22minute	Microsoft® Windows® Operat...	Microsoft Corporation	17	4
□	☰	msedgewebview...	Microsoft Edge WebView2	9day 19hour 36minute	Microsoft Edge WebView2	Microsoft Corporation	4	4
□	☰	WinSCP.exe	WinSCP: SFTP, FTP, WebDA...	8day 3hour 19minute	WinSCP	Martin Prikryl	2	2
□	☰	WMICodeCreator...		6day 13hour 5minute			10	7
☑	☰	chrome.exe	Google Chrome	5day 9hour 47minute	Google Chrome	Google LLC	4	2
□	☰	WindowsTerminal...	WindowsTerminal.exe	4day 21hour 41minute	Windows Terminal	Microsoft Corporation	13	3
□	☰	Widgets.exe		4day 19hour 52minute	Microsoft® Windows® Operat...	Microsoft Corporation	2	2
□	☰	Dbgview.exe	DebugView	3day 8hour 36minute	Sysinternals Debugview	Sysinternals	5	5

	▼ Connection	Host Name	Client Type	OS Information	IP Address	Usage Time
⊟ chrome.exe (2) - 5day 9hour 47minute						
☰	Online	DESKTOP-D458HV0	Windows	Windows 10 (x64)	10.0.2.15	2day 2hour 34minute
☰	Offline	DESKTOP-D458HV0	Windows	Windows 10 (x64)	10.0.2.15	3day 7hour 13minute
⊟ msedge.exe (3) - 28day 17hour 40minute						
☰	Offline	DESKTOP-061AN7H	Windows	Windows 11 (x64)	10.10.30.157	1day 2hour 45minute
☰	Offline	DESKTOP-D458HV0	Windows	Windows 10 (x64)	10.0.2.15	27day 12hour 34minute
☰	Offline	DESKTOP-061AN7H	Windows	Windows 11 (x64)	10.10.30.157	2hour 21minute

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 Show Device 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.

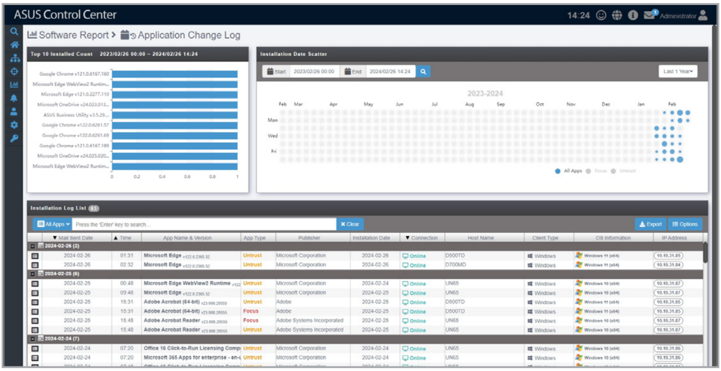
Refetching application usage information

Click on Refetch 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.

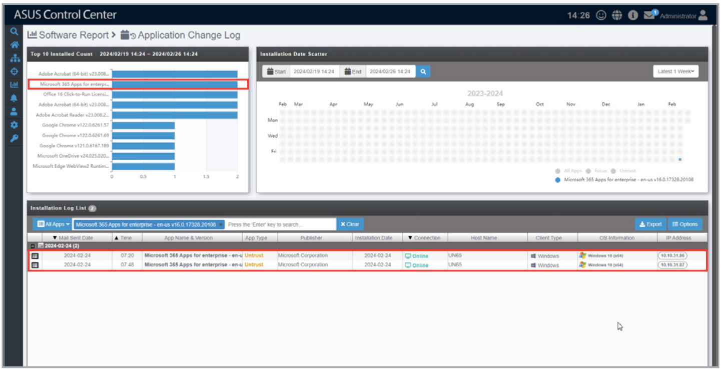
> To export the information of a block, click the **Export** button in that block, then enter a filename and click **OK**.


ASUS Control Center
14:24
Administrator
Software Report > Application Change Log
Top 10 Installed Count 2023/02/26 00:00 ~ 2024/02/26 14:24
Google Chrome v121.0.6167.160
Microsoft Edge WebView2 Runtim...
Microsoft Edge v121.0.2277.110
Microsoft OneDrive v24.023.013...
ASUS Business Utility v3.5.29....
Google Chrome v122.0.6261.57
Google Chrome v122.0.6261.69
Google Chrome v121.0.6167.189
Microsoft OneDrive v24.025.020...
Microsoft Edge WebView2 Runtim...
0
0.2
0.4
0.6
0.8
1
Installation Date Scatter
Start
2023/02/26 00:00
End
2024/02/26 14:24
Last 1 Year
2023-2024
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mon
Wed
Fri
All Apps
Focus
Untrust
Installation Log List 83
All Apps
Press the 'Enter' key to search...
Clear
Export
Options

	▼ Mail Sent Date	▲ Time	App Name & Version	App Type	Publisher	Installation Date	▼ Connection	Host Name	Client Type	OS Information	IP Address
2024-02-26 (2)											
	2024-02-26	01:31	**Microsoft Edge** v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-26	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
	2024-02-26	02:32	**Microsoft Edge** v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-26	Online	D700MD	Windows	Windows 11 (x64)	10.10.31.84
2024-02-25 (6)											
	2024-02-25	00:48	**Microsoft Edge WebView2 Runtime** v122	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
	2024-02-25	09:48	**Microsoft Edge** v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
	2024-02-25	15:31	**Adobe Acrobat (64-bit)** v23.008.20555	Untrust	Adobe	2024-02-25	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
	2024-02-25	15:31	**Adobe Acrobat (64-bit)** v23.008.20555	Focus	Adobe	2024-02-25	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
	2024-02-25	15:48	**Adobe Acrobat Reader** v23.008.20555	Focus	Adobe Systems Incorporated	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
	2024-02-25	15:48	**Adobe Acrobat Reader** v23.008.20555	Untrust	Adobe Systems Incorporated	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
2024-02-24 (7)											
	2024-02-24	07:20	**Office 16 Click-to-Run Licensing Comp**	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.86
	2024-02-24	07:20	**Microsoft 365 Apps for enterprise - en-u**	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.86

Filtering by application

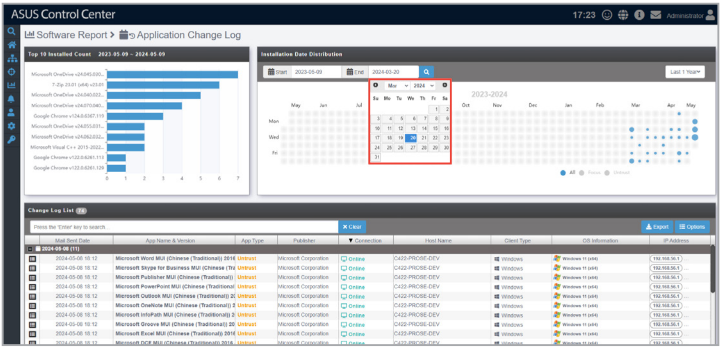
Click an application in the **Top 10 Installed Count** block to only show devices with the specified application installed.


ASUS Control Center
14:26
Administrator
Software Report > Application Change Log
Top 10 Installed Count 2024/02/19 14:24 ~ 2024/02/26 14:24
Adobe Acrobat (64-bit) v23.008...
Microsoft 365 Apps for enterpr...
Office 16 Click-to-Run Licensi...
Adobe Acrobat (64-bit) v23.008...
Adobe Acrobat Reader v23.008.2...
Google Chrome v122.0.6261.57
Google Chrome v122.0.6261.69
Google Chrome v121.0.6167.189
Microsoft OneDrive v24.025.020...
Microsoft Edge WebView2 Runtim...
0
0.5
1
1.5
2
Installation Date Scatter
Start
2024/02/19 14:24
End
2024/02/26 14:24
Latest 1 Week
2023-2024
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mon
Wed
Fri
All Apps
Focus
Untrust
Microsoft 365 Apps for enterprise - en-us v16.0.17328.20108
Installation Log List 2
All Apps
Microsoft 365 Apps for enterprise - en-us v16.0.17328.20108
Press the 'Enter' key to search...
Clear
Export
Options

	▼ Mail Sent Date	▲ Time	App Name & Version	App Type	Publisher	Installation Date	▼ Connection	Host Name	Client Type	OS Information	IP Address
2024-02-24 (2)											
	2024-02-24	07:20	**Microsoft 365 Apps for enterprise - en-u**	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.86
	2024-02-24	07:48	**Microsoft 365 Apps for enterprise - en-u**	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87

Filtering by time period

Select a time period using the **Start** and **End** fields to only show records within the specified time period.



ASUS Control Center — 17:23 — Administrator

Software Report > Application Change Log

Top 10 Installed Count 2023-05-09 ~ 2024-05-09

Microsoft OneDrive v24.045.030...
7-Zip 23.01 (x64) v23.01
Microsoft OneDrive v24.040.022...
Microsoft OneDrive v24.070.040...
Google Chrome v124.0.6367.119
Microsoft OneDrive v24.055.031...
Microsoft OneDrive v24.062.032...
Microsoft Visual C++ 2015-2022...
Google Chrome v122.0.6261.113
Google Chrome v122.0.6261.129
0
1
2
3
4
5
6
7

Installation Date Distribution

Start 2023-05-09 End 2024-03-20 — Last 1 Year

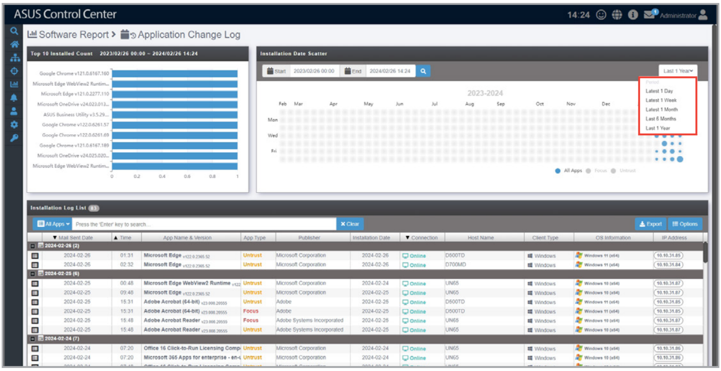
Mar 2024
Su Mo Tu We Th Fr Sa
2023-2024
May
Jun
Jul
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Mon
Wed
Fri
All
Focus
Untrust

Change Log List 74

Press the 'Enter' key to search... ✕ Clear — Export — Options

Mail Sent Date	App Name & Version	App Type	Publisher	▼ Connection	Host Name	Client Type	OS Information	IP Address
2024-05-08 (11)								
2024-05-08 18:12	Microsoft Word MUI (Chinese (Traditional)) 2016	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft Skype for Business MUI (Chinese (Tra	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft Publisher MUI (Chinese (Traditional))	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft PowerPoint MUI (Chinese (Traditional	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft Outlook MUI (Chinese (Traditional)) 20	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft OneNote MUI (Chinese (Traditional)) 2	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft InfoPath MUI (Chinese (Traditional)) 2	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft Groove MUI (Chinese (Traditional)) 20	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft Excel MUI (Chinese (Traditional)) 2016	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1 ...
2024-05-08 18:12	Microsoft DCF MUI (Chinese (Traditional)) 2016	Untrust	Microsoft Corporation	Online	C422-PROSE-DEV	Windows	Windows 11 (x64)	192.168.56.1

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



ASUS Control Center — 14:24 — Administrator

Software Report > Application Change Log

Top 10 Installed Count 2023/02/26 00:00 ~ 2024/02/26 14:24

Google Chrome v121.0.6167.160
Microsoft Edge WebView2 Runtim...
Microsoft Edge v121.0.2277.110
Microsoft OneDrive v24.023.013...
ASUS Business Utility v3.5.29...
Google Chrome v122.0.6261.57
Google Chrome v122.0.6261.69
Google Chrome v121.0.6167.189
Microsoft OneDrive v24.025.020...
Microsoft Edge WebView2 Runtim...
0
0.2
0.4
0.6
0.8
1

Installation Date Scatter

Start 2023/02/26 00:00 End 2024/02/26 14:24 — Last 1 Year

Period
- Latest 1 Day
- Latest 1 Week
- Latest 1 Month
- Last 6 Months
- Last 1 Year

2023-2024
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Mon
Wed
Fri
All Apps
Focus
Untrust

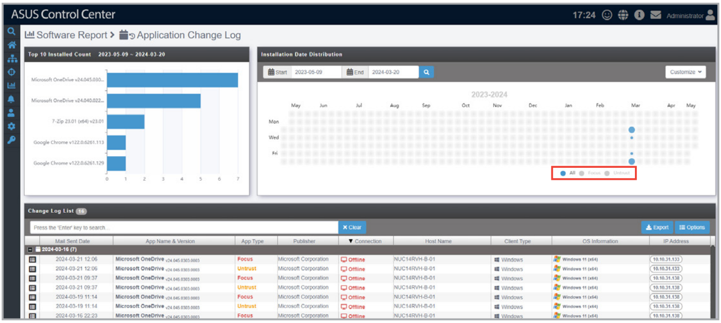
Installation Log List 83

All Apps — Press the 'Enter' key to search... ✕ Clear — Export — Options

▼ Mail Sent Date	▲ Time	App Name & Version	App Type	Publisher	Installation Date	▼ Connection	Host Name	Client Type	OS Information	IP Address
2024-02-26 (2)										
2024-02-26	01:31	Microsoft Edge v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-26	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
2024-02-26	02:32	Microsoft Edge v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-26	Online	D700MD	Windows	Windows 11 (x64)	10.10.31.84
2024-02-25 (6)										
2024-02-25	00:48	Microsoft Edge WebView2 Runtime v122	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
2024-02-25	09:48	Microsoft Edge v122.0.2365.52	Untrust	Microsoft Corporation	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
2024-02-25	15:31	Adobe Acrobat (64-bit) v23.008.20555	Untrust	Adobe	2024-02-25	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
2024-02-25	15:31	Adobe Acrobat (64-bit) v23.008.20555	Focus	Adobe	2024-02-25	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85
2024-02-25	15:48	Adobe Acrobat Reader v23.008.20555	Focus	Adobe Systems Incorporated	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
2024-02-25	15:48	Adobe Acrobat Reader v23.008.20555	Untrust	Adobe Systems Incorporated	2024-02-25	Online	UN65	Windows	Windows 10 (x64)	10.10.31.87
2024-02-24 (7)										
2024-02-24	07:20	Office 16 Click-to-Run Licensing Comp	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.86
2024-02-24	07:20	Microsoft 365 Apps for enterprise - en-u	Untrust	Microsoft Corporation	2024-02-24	Online	UN65	Windows	Windows 10 (x64)	10.10.31.86

Filtering by App Type

Select All Apps, Focus, or Untrust to only show records matching the specified app type.

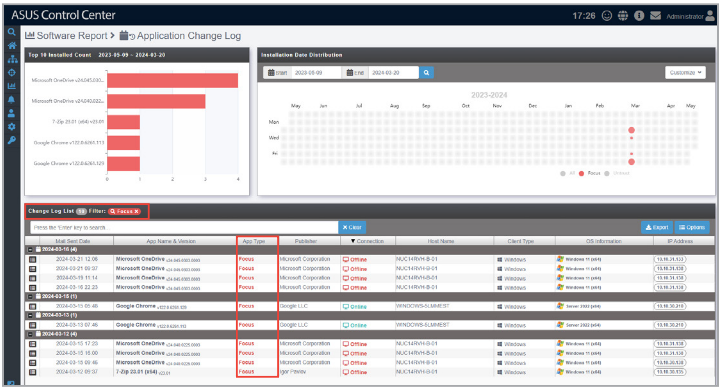

ASUS Control Center
17:24
Administrator
Software Report > Application Change Log
Top 10 Installed Count 2023-05-09 ~ 2024-03-20
Microsoft OneDrive v24.045.030...
Microsoft OneDrive v24.040.022...
7-Zip 23.01 (x64) v23.01
Google Chrome v122.0.6261.113
Google Chrome v122.0.6261.129
0
1
2
3
4
5
6
7
Installation Date Distribution
Start 2023-05-09
End 2024-03-20
Customize
2023-2024
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Mon
Wed
Fri
All
Focus
Untrust

Change Log List 16

Press the 'Enter' key to search...

✕ Clear | Export | Options

	Mail Sent Date	App Name & Version	App Type	Publisher	▼ Connection	Host Name	Client Type	OS Information	IP Address
⊟ 2024-03-16 (7)									
	2024-03-21 12:06	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.133
	2024-03-21 12:06	Microsoft OneDrive v24.045.0303.0003	Untrust	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.133
	2024-03-21 09:37	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-21 09:37	Microsoft OneDrive v24.045.0303.0003	Untrust	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-19 11:14	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-19 11:14	Microsoft OneDrive v24.045.0303.0003	Untrust	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-16 22:23	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138


ASUS Control Center
17:26
Administrator
Software Report > Application Change Log
Top 10 Installed Count 2023-05-09 ~ 2024-03-20
Microsoft OneDrive v24.045.030...
Microsoft OneDrive v24.040.022...
7-Zip 23.01 (x64) v23.01
Google Chrome v122.0.6261.113
Google Chrome v122.0.6261.129
0
1
2
3
4
Installation Date Distribution
Start 2023-05-09
End 2024-03-20
Customize
2023-2024
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May
Mon
Wed
Fri
All
Focus
Untrust

Change Log List 10 Filter: Focus ✕

Press the 'Enter' key to search...

✕ Clear | Export | Options

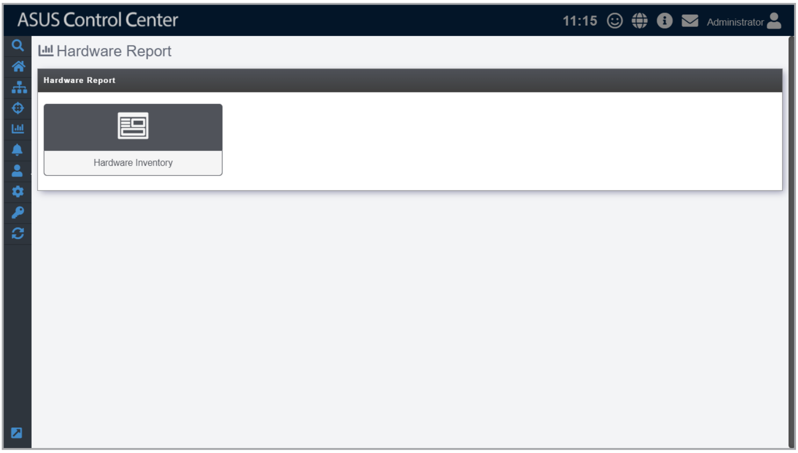
	Mail Sent Date	App Name & Version	App Type	Publisher	▼ Connection	Host Name	Client Type	OS Information	IP Address
⊟ 2024-03-16 (4)									
	2024-03-21 12:06	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.133
	2024-03-21 09:37	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-19 11:14	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-16 22:23	Microsoft OneDrive v24.045.0303.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
⊟ 2024-03-15 (1)									
	2024-03-15 05:48	Google Chrome v122.0.6261.129	Focus	Google LLC	Online	WINDOWS-5LMMEST	Windows	Server 2022 (x64)	10.10.30.210
⊟ 2024-03-13 (1)									
	2024-03-13 07:46	Google Chrome v122.0.6261.113	Focus	Google LLC	Online	WINDOWS-5LMMEST	Windows	Server 2022 (x64)	10.10.30.210
⊟ 2024-03-12 (4)									
	2024-03-15 17:23	Microsoft OneDrive v24.040.0225.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-15 16:00	Microsoft OneDrive v24.040.0225.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.31.138
	2024-03-15 09:46	Microsoft OneDrive v24.040.0225.0003	Focus	Microsoft Corporation	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.30.138
	2024-03-12 09:37	7-Zip 23.01 (x64) v23.01	Focus	Igor Pavlov	Offline	NUC14RVH-B-01	Windows	Windows 11 (x64)	10.10.30.135

5.2 Hardware Report

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**.



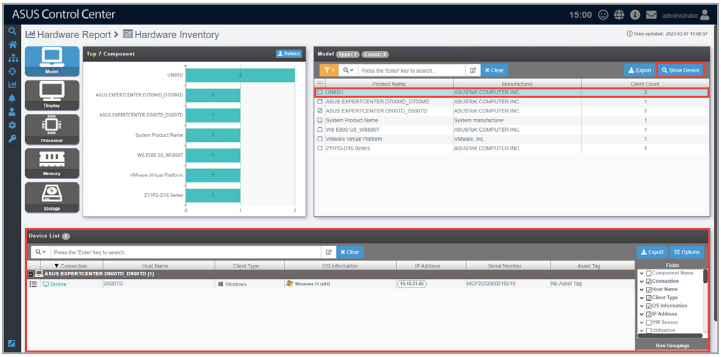
- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to the **Options** section.

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.

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

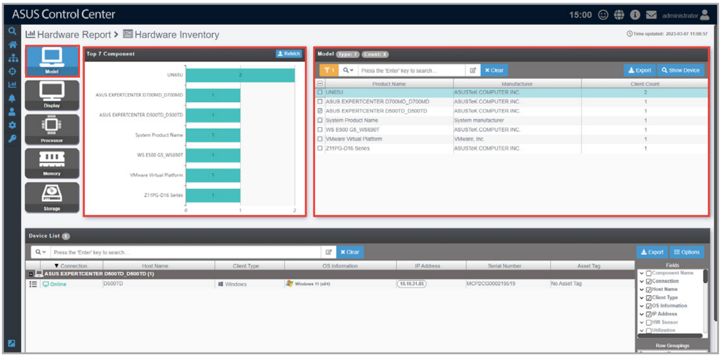


□	Product Name	Manufacturer	Client Count
□	UN65U	ASUSTeK COMPUTER INC.	2
□	ASUS EXPERTCENTER D700MD_D700MD	ASUSTeK COMPUTER INC.	1
☑	ASUS EXPERTCENTER D500TD_D500TD	ASUSTeK COMPUTER INC.	1
□	System Product Name	System manufacturer	1
□	WS E500 G5_WS690T	ASUSTeK COMPUTER INC.	1
□	VMware Virtual Platform	VMware, Inc.	1
□	Z11PG-D16 Series	ASUSTeK COMPUTER INC.	1

Connection	Host Name	Client Type	OS Information	IP Address	Serial Number	Asset Tag
ASUS EXPERTCENTER D500TD_D500TD (1)						
Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85	MCP2CG000219519	No Asset Tag

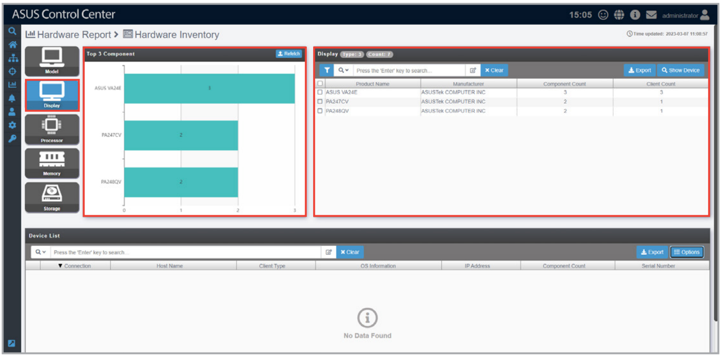
□ Component Name
☑ Connection
☑ Host Name
☑ Client Type
☑ OS Information
☑ IP Address
□ HW Sensor
□ Utilization

View Model component type and count


□	Product Name	Manufacturer	Client Count
□	UN65U	ASUSTeK COMPUTER INC.	2
□	ASUS EXPERTCENTER D700MD_D700MD	ASUSTeK COMPUTER INC.	1
☑	ASUS EXPERTCENTER D500TD_D500TD	ASUSTeK COMPUTER INC.	1
□	System Product Name	System manufacturer	1
□	WS E500 G5_WS690T	ASUSTeK COMPUTER INC.	1
□	VMware Virtual Platform	VMware, Inc.	1
□	Z11PG-D16 Series	ASUSTeK COMPUTER INC.	1

Connection	Host Name	Client Type	OS Information	IP Address	Serial Number	Asset Tag
ASUS EXPERTCENTER D500TD_D500TD (1)						
Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85	MCP2CG000219519	No Asset Tag

View Display component type and count

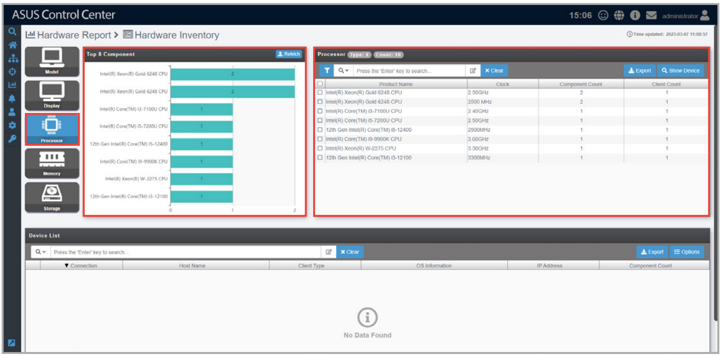


□	Product Name	Manufacturer	Component Count	Client Count
□	ASUS VA24E	ASUSTek COMPUTER INC	3	3
□	PA247CV	ASUSTek COMPUTER INC	2	1
□	PA248QV	ASUSTek COMPUTER INC	2	1

Connection	Host Name	Client Type	OS Information	IP Address	Component Count	Serial Number

No Data Found

View Processor component type and count

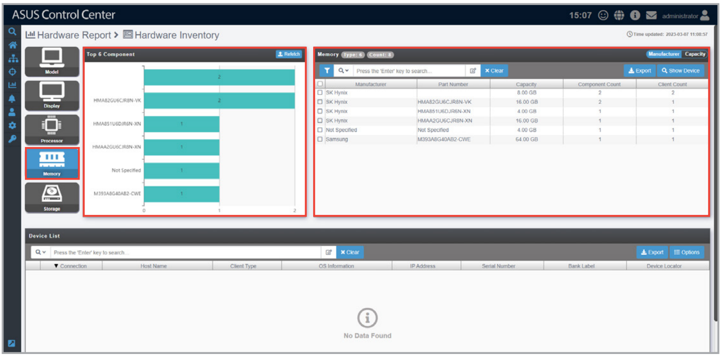

ASUS Control Center
15:06
administrator
Hardware Report > Hardware Inventory
Time updated: 2023-03-07 11:08:57
Model
Display
Processor
Memory
Storage
Top 8 Component
Refetch
Intel(R) Xeon(R) Gold 6248 CPU
2
Intel(R) Xeon(R) Gold 6248 CPU
2
Intel(R) Core(TM) i3-7100U CPU
1
Intel(R) Core(TM) i5-7200U CPU
1
12th Gen Intel(R) Core(TM) i5-12400
1
Intel(R) Core(TM) i9-9900K CPU
1
Intel(R) Xeon(R) W-2275 CPU
1
12th Gen Intel(R) Core(TM) i3-12100
1
0
1
2
Processor
Type: 8
Count: 10
Press the 'Enter' key to search...
Clear
Export
Show Device
Device List
Export
Options

□	Product Name	Clock	Component Count	Client Count
□	Intel(R) Xeon(R) Gold 6248 CPU	2.50GHz	2	1
□	Intel(R) Xeon(R) Gold 6248 CPU	2500 MHz	2	1
□	Intel(R) Core(TM) i3-7100U CPU	2.40GHz	1	1
□	Intel(R) Core(TM) i5-7200U CPU	2.50GHz	1	1
□	12th Gen Intel(R) Core(TM) i5-12400	2500MHz	1	1
□	Intel(R) Core(TM) i9-9900K CPU	3.60GHz	1	1
□	Intel(R) Xeon(R) W-2275 CPU	3.30GHz	1	1
□	12th Gen Intel(R) Core(TM) i3-12100	3300MHz	1	1

Connection	Host Name	Client Type	OS Information	IP Address	Component Count

No Data Found

View Memory component type and count

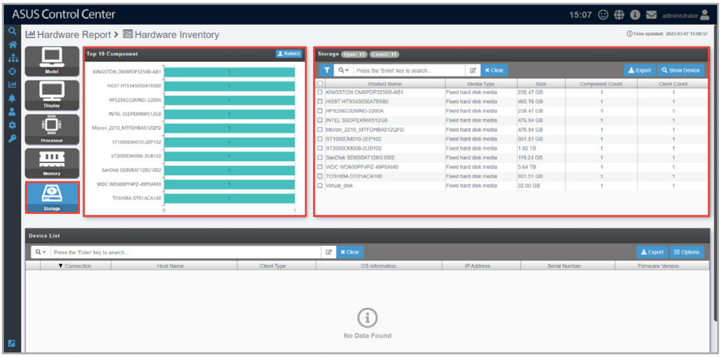


□	Manufacturer	Part Number	Capacity	Component Count	Client Count
□	SK Hynix		8.00 GB	2	2
□	SK Hynix	HMA82GU6CJR8N-VK	16.00 GB	2	1
□	SK Hynix	HMA851U6DJR6N-XN	4.00 GB	1	1
□	SK Hynix	HMAA2GU6CJR8N-XN	16.00 GB	1	1
□	Not Specified	Not Specified	4.00 GB	1	1
□	Samsung	M393A8G40AB2-CWE	64.00 GB	1	1

Connection	Host Name	Client Type	OS Information	IP Address	Serial Number	Bank Label	Device Locator

No Data Found

View Storage component type and count



Storage Type: 11 Count: 11

	Product Name	Media Type	Size	Component Count	Client Count
□	KINGSTON OM8PDP3256B-AB1	Fixed hard disk media	238.47 GB	1	1
□	HGST HTS545050A7E680	Fixed hard disk media	465.76 GB	1	1
□	HFS256G32MND-2200A	Fixed hard disk media	238.47 GB	1	1
□	INTEL SSDPEKNW512G8	Fixed hard disk media	476.94 GB	1	1
□	Micron_2210_MTFDHBA512QFD	Fixed hard disk media	476.94 GB	1	1
□	ST1000DM010-2EP102	Fixed hard disk media	931.51 GB	1	1
□	ST2000DM008-2UB102	Fixed hard disk media	1.82 TB	1	1
□	SanDisk SD8SBAT128G1002	Fixed hard disk media	119.24 GB	1	1
□	WDC WD600PF4PZ-49P0AM0	Fixed hard disk media	5.64 TB	1	1
□	TOSHIBA DT01ACA100	Fixed hard disk media	931.51 GB	1	1
□	Virtual_disk	Fixed hard disk media	32.00 GB	1	1

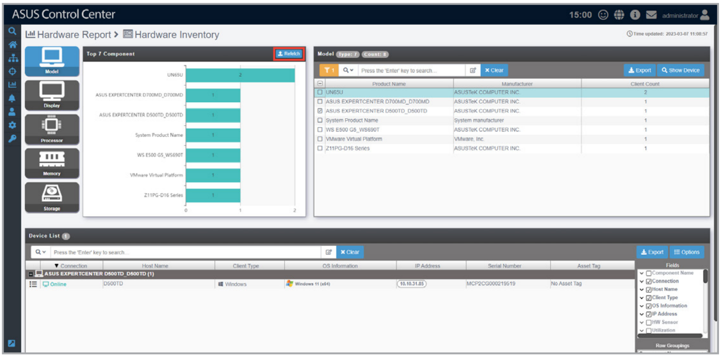
Device List

Connection	Host Name	Client Type	OS Information	IP Address	Serial Number	Firmware Version

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.



Model Type: 7 Count: 8

⊟	Product Name	Manufacturer	Client Count
□	UN65U	ASUSTeK COMPUTER INC.	2
□	ASUS EXPERTCENTER D700MD_D700MD	ASUSTeK COMPUTER INC.	1
☑	ASUS EXPERTCENTER D500TD_D500TD	ASUSTeK COMPUTER INC.	1
□	System Product Name	System manufacturer	1
□	WS E500 G5_WS690T	ASUSTeK COMPUTER INC.	1
□	VMware Virtual Platform	VMware, Inc.	1
□	Z11PG-D16 Series	ASUSTeK COMPUTER INC.	1

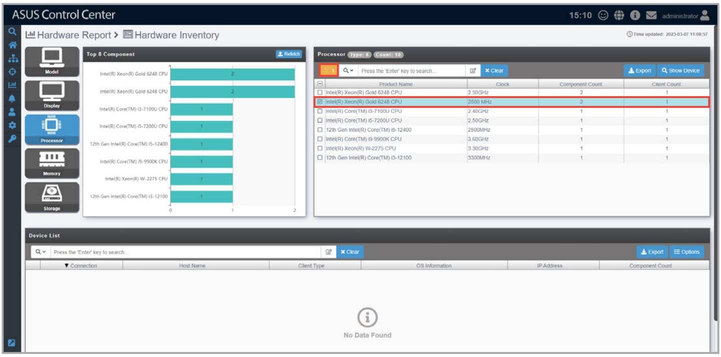
Device List 1

	Connection	Host Name	Client Type	OS Information	IP Address	Serial Number	Asset Tag
⊟	ASUS EXPERTCENTER D500TD_D500TD (1)						
	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85	MCP2CG000219519	No Asset Tag

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 ▼.

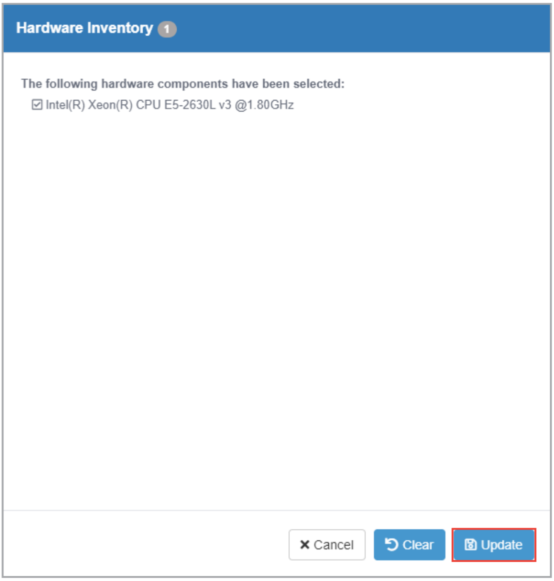


ASUS Control Center
15:10
administrator
Hardware Report > Hardware Inventory
Time updated: 2023-03-07 11:08:57
Model
Display
Processor
Memory
Storage
Top 8 Component
Refetch
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Core(TM) i3-7100U CPU
Intel(R) Core(TM) i5-7200U CPU
12th Gen Intel(R) Core(TM) i5-12400
Intel(R) Core(TM) i9-9900K CPU
Intel(R) Xeon(R) W-2275 CPU
12th Gen Intel(R) Core(TM) i3-12100
2
2
1
1
1
1
1
1
0
1
2
Processor Type: 8 Count: 10
1
Press the 'Enter' key to search...
Clear
Export
Show Device
Device List
Press the 'Enter' key to search...
Clear
Export
Options
No Data Found

	Product Name	Clock	Component Count	Client Count
☐	Intel(R) Xeon(R) Gold 6248 CPU	2.50GHz	2	1
☑	Intel(R) Xeon(R) Gold 6248 CPU	2500 MHz	2	1
☐	Intel(R) Core(TM) i3-7100U CPU	2.40GHz	1	1
☐	Intel(R) Core(TM) i5-7200U CPU	2.50GHz	1	1
☐	12th Gen Intel(R) Core(TM) i5-12400	2500MHz	1	1
☐	Intel(R) Core(TM) i9-9900K CPU	3.60GHz	1	1
☐	Intel(R) Xeon(R) W-2275 CPU	3.30GHz	1	1
☐	12th Gen Intel(R) Core(TM) i3-12100	3300MHz	1	1

	▼ Connection	Host Name	Client Type	OS Information	IP Address	Component Count

2. Confirm that the components displayed match the ones you checked, then click **Update**.



The following hardware components have been selected:

☑ Intel(R) Xeon(R) CPU E5-2630L v3 @1.80GHz

3. The component list should only display the selected components.

Search for components using keywords

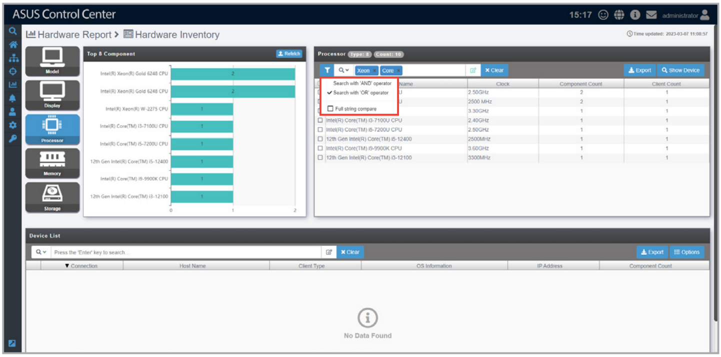
Entering keywords into the search bar will display all components which contain the keywords entered, allowing you to pinpoint certain hardware components and help you keep track of the amount of devices these hardware components are installed on.

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.

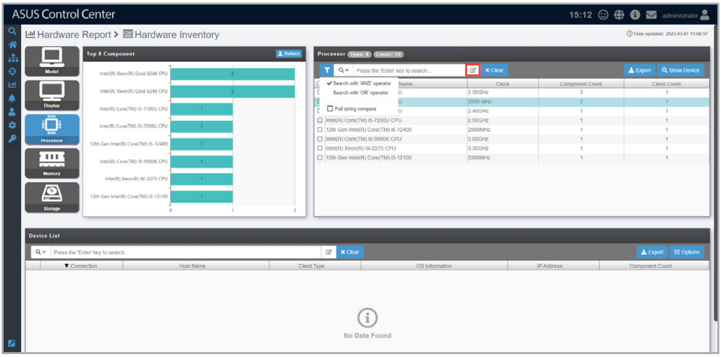

ASUS Control Center
15:17
administrator
Hardware Report > Hardware Inventory
Time updated: 2023-03-07 11:08:57
Model
Display
Processor
Memory
Storage
Top 8 Component
Refetch
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Xeon(R) W-2275 CPU
Intel(R) Core(TM) i3-7100U CPU
Intel(R) Core(TM) i5-7200U CPU
12th Gen Intel(R) Core(TM) i5-12400
Intel(R) Core(TM) i9-9900K CPU
12th Gen Intel(R) Core(TM) i3-12100
2
2
1
1
1
1
1
1
0
1
2
Processor
Type: 8
Count: 10
Xeon
Core
Clear
Export
Show Device
Search with 'AND' operator
✓ Search with 'OR' operator
□ Full string compare
Device List
Press the 'Enter' key to search...
Clear
Export
Options
No Data Found

Name	Clock	Component Count	Client Count
□ U	2.50GHz	2	1
□ U	2500 MHz	2	1
□	3.30GHz	1	1
□ Intel(R) Core(TM) i3-7100U CPU	2.40GHz	1	1
□ Intel(R) Core(TM) i5-7200U CPU	2.50GHz	1	1
□ 12th Gen Intel(R) Core(TM) i5-12400	2500MHz	1	1
□ Intel(R) Core(TM) i9-9900K CPU	3.60GHz	1	1
□ 12th Gen Intel(R) Core(TM) i3-12100	3300MHz	1	1

▼ Connection	Host Name	Client Type	OS Information	IP Address	Component Count

- Importing multiple keywords from a .csv file

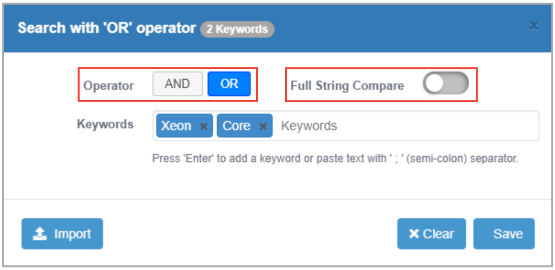
  a. Click on ☑ to bring up the search condition pop-up window.


ASUS Control Center
15:12
administrator
Hardware Report > Hardware Inventory
Time updated: 2023-03-07 11:08:57
Model
Display
Processor
Memory
Storage
Top 8 Component
Refetch
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Core(TM) i3-7100U CPU
Intel(R) Core(TM) i5-7200U CPU
12th Gen Intel(R) Core(TM) i5-12400
Intel(R) Core(TM) i9-9900K CPU
Intel(R) Xeon(R) W-2275 CPU
12th Gen Intel(R) Core(TM) i3-12100
2
2
1
1
1
1
1
1
0
1
2
Processor
Type: 8
Count: 10
Press the 'Enter' key to search...
Clear
Export
Show Device
✓ Search with 'AND' operator
Search with 'OR' operator
□ Full string compare
Device List
Press the 'Enter' key to search...
Clear
Export
Options
▼ Connection
Host Name
Client Type
OS Information
IP Address
Component Count
No Data Found

Name	Clock	Component Count	Client Count
U	2.50GHz	2	1
U	2500 MHz	2	1
U	2.40GHz	1	1
Intel(R) Core(TM) i5-7200U CPU	2.50GHz	1	1
12th Gen Intel(R) Core(TM) i5-12400	2500MHz	1	1
Intel(R) Core(TM) i9-9900K CPU	3.60GHz	1	1
Intel(R) Xeon(R) W-2275 CPU	3.30GHz	1	1
12th Gen Intel(R) Core(TM) i3-12100	3300MHz	1	1

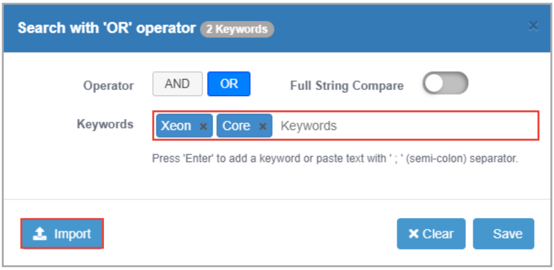
  b. Select the operator you wish to use. **AND** will search for items which contain all the keywords entered, whilst **OR** will search for items which contain at least one of the keywords entered.

  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.



Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

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.

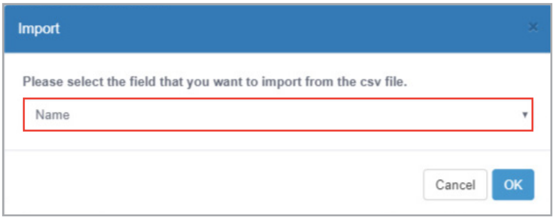


Search with 'OR' operator 2 Keywords

Operator: AND [✓ OR]   Full String Compare ○

Keywords: Xeon × Core × Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

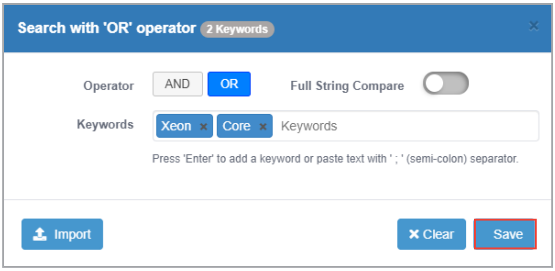


Import

Please select the field that you want to import from the csv file.

Name ▾

d. Click on **Save** once you have finished setting the search conditions.



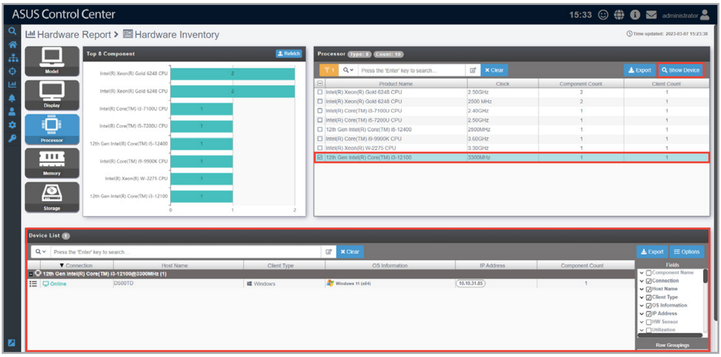
Search with 'OR' operator 2 Keywords

Operator: AND [✓ OR]   Full String Compare ○

Keywords: Xeon × Core × Keywords

Press 'Enter' to add a keyword or paste text with ' ; ' (semi-colon) separator.

2. 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


ASUS Control Center
15:33
administrator
Hardware Report > Hardware Inventory
Time updated: 2023-03-07 15:23:38
Model
Display
Processor
Memory
Storage
Top 8 Component
Refetch
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Xeon(R) Gold 6248 CPU
Intel(R) Core(TM) i3-7100U CPU
Intel(R) Core(TM) i5-7200U CPU
12th Gen Intel(R) Core(TM) i5-12400
Intel(R) Core(TM) i9-9900K CPU
Intel(R) Xeon(R) W-2275 CPU
12th Gen Intel(R) Core(TM) i3-12100
0
1
2

Processor Type: 8 Count: 10

Press the 'Enter' key to search... ✕ Clear Export Show Device

⊟	Product Name	Clock	Component Count	Client Count
□	Intel(R) Xeon(R) Gold 6248 CPU	2.50GHz	2	1
□	Intel(R) Xeon(R) Gold 6248 CPU	2500 MHz	2	1
□	Intel(R) Core(TM) i3-7100U CPU	2.40GHz	1	1
□	Intel(R) Core(TM) i5-7200U CPU	2.50GHz	1	1
□	12th Gen Intel(R) Core(TM) i5-12400	2500MHz	1	1
□	Intel(R) Core(TM) i9-9900K CPU	3.60GHz	1	1
□	Intel(R) Xeon(R) W-2275 CPU	3.30GHz	1	1
☑	12th Gen Intel(R) Core(TM) i3-12100	3300MHz	1	1

Device List 1

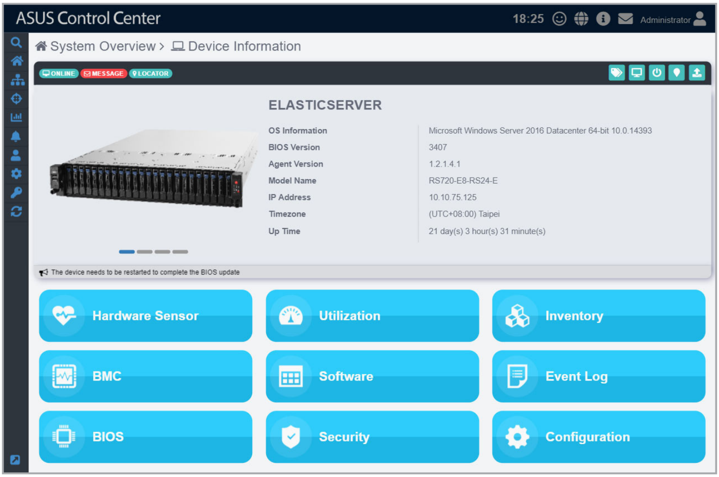
Press the 'Enter' key to search... ✕ Clear Export Options

	Connection	Host Name	Client Type	OS Information	IP Address	Component Count
⊟ 12th Gen Intel(R) Core(TM) i3-12100@3300MHz (1)						
☰	Online	D500TD	Windows	Windows 11 (x64)	10.10.31.85	1

Fields
□ Component Name
☑ Connection
☑ Host Name
☑ Client Type
☑ OS Information
☑ IP Address
□ HW Sensor
□ Utilization

Row Groupings

3. (optional) Clicking on ☰ next to each device in the **Device List** will allow you to view the Device Information.



ELASTICSERVER

OS Information	Microsoft Windows Server 2016 Datacenter 64-bit 10.0.14393
BIOS Version	3407
Agent Version	1.2.1.4.1
Model Name	RS720-E8-RS24-E
IP Address	10.10.75.125
Timezone	(UTC+08:00) Taipei
Up Time	21 day(s) 3 hour(s) 31 minute(s)

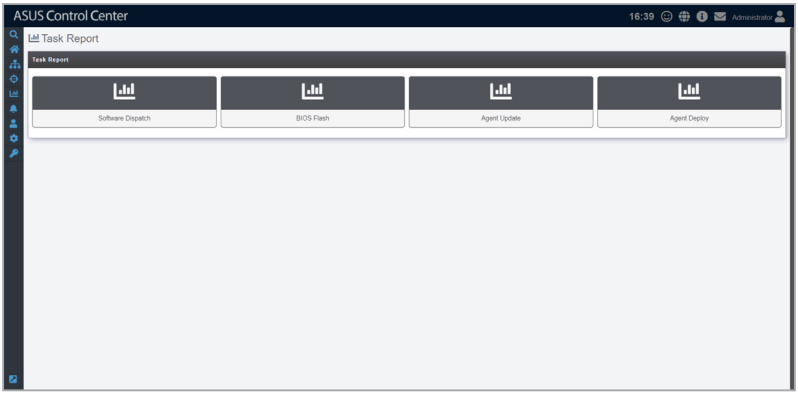
The device needs to be restarted to complete the BIOS update

5.3 Task Report

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.

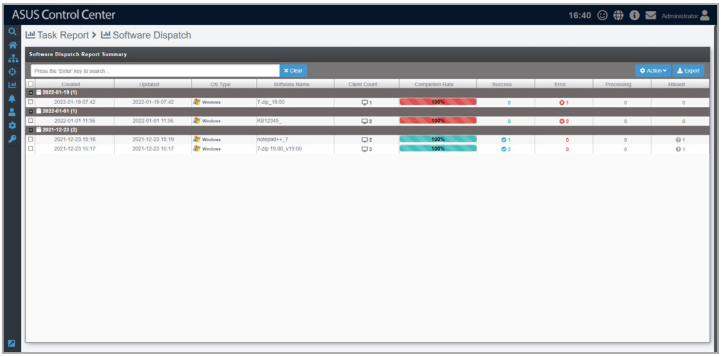


If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.

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.

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

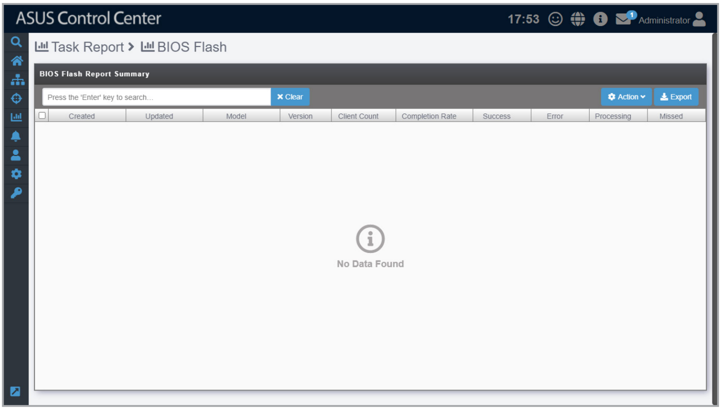

ASUS Control Center
16:40
Administrator
Task Report > Software Dispatch
Software Dispatch Report Summary
Press the 'Enter' key to search...
✕ Clear
Action
Export

□	Created	Updated	OS Type	Software Name	Client Count	Completion Rate	Success	Error	Processing	Missed
⊟	2022-01-19 (1)									
□	2022-01-19 07:42	2022-01-19 07:42	Windows	7-zip_19.00	1	100%	0	1	0	0
⊟	2022-01-01 (1)									
□	2022-01-01 11:56	2022-01-01 11:56	Windows	KB12345_	2	100%	0	2	0	0
⊟	2021-12-23 (2)									
□	2021-12-23 15:18	2021-12-23 15:19	Windows	notepad++_7	2	100%	1	0	0	1
□	2021-12-23 15:17	2021-12-23 15:17	Windows	7-zip 19.00_v19.00	3	100%	2	0	0	1

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.

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



BIOS Flash Report Summary

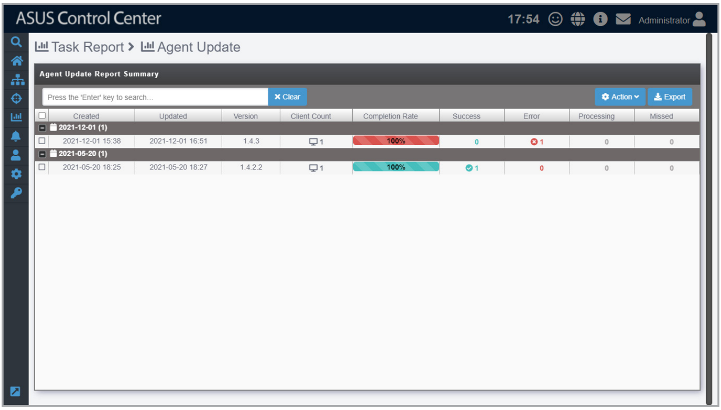
□	Created	Updated	Model	Version	Client Count	Completion Rate	Success	Error	Processing	Missed

No Data Found

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.

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



Agent Update Report Summary

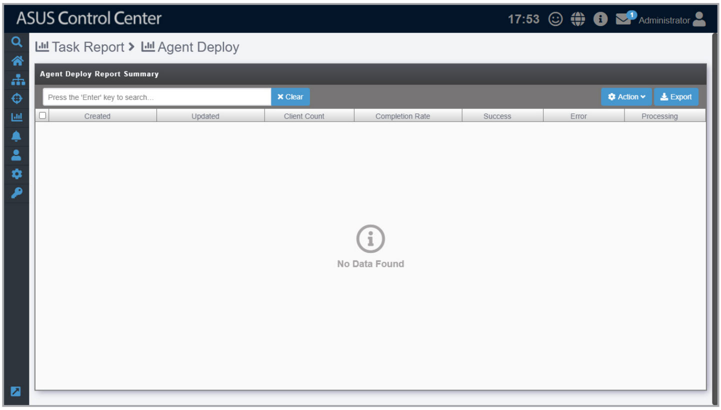
Press the 'Enter' key to search...

□	Created	Updated	Version	Client Count	Completion Rate	Success	Error	Processing	Missed
2021-12-01 (1)									
□	2021-12-01 15:38	2021-12-01 16:51	1.4.3	1	100%	0	1	0	0
2021-05-20 (1)									
□	2021-05-20 18:25	2021-05-20 18:27	1.4.2.2	1	100%	1	0	0	0

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 be each batch of agent deployments. You can refer to the **Agent Deploy Report** section for more details.

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



Chapter 6

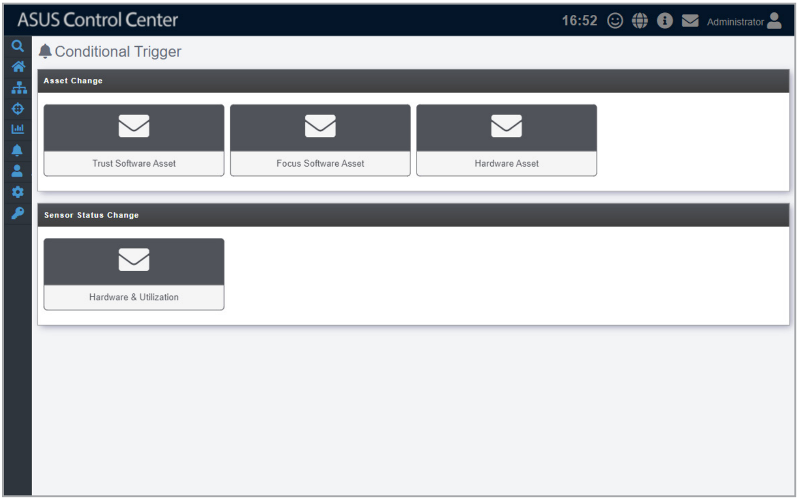
Notification

This chapter describes notification rules and asset report options.

6.1 Conditional Trigger

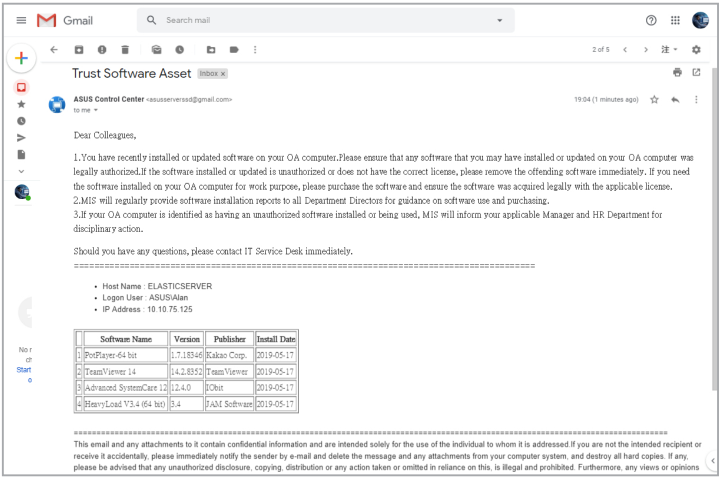
Conditional Trigger allows you to set notifications for software changes, or hardware changes on managed devices. Notifications are sent when software not on the Trust or Focus list have been installed on managed devices, or if hardware such as CPUs or DIMMs that are removed or do not comply to company 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**.



6.1.1 Trust Software Asset

Trust Software Asset allows you to set notifications when there are *applications not in the **Trust Software Asset*** being installed on managed devices. These notifications will be sent immediately to the owner of managed device as well as his/her director. Below is an example of a notification sent when an application not in the Trust Software Asset is installed on the managed device.



Trust Software Asset

ASUS Control Center <asusserverssd@gmail.com>
to me
19:04 (1 minutes ago)

Dear Colleagues,

1.You have recently installed or updated software on your OA computer.Please ensure that any software that you may have installed or updated on your OA computer was legally authorized.If the software installed or updated is unauthorized or does not have the correct license, please remove the offending software immediately. If you need the software installed on your OA computer for work purpose, please purchase the software and ensure the software was acquired legally with the applicable license.
2.MIS will regularly provide software installation reports to all Department Directors for guidance on software use and purchasing.
3.If your OA computer is identified as having an unauthorized software installed or being used, MIS will inform your applicable Manager and HR Department for disciplinary action.

Should you have any questions, please contact IT Service Desk immediately.

==

- Host Name : ELASTICSERVER
- Logon User : ASUS\Alan
- IP Address : 10.10.75.125

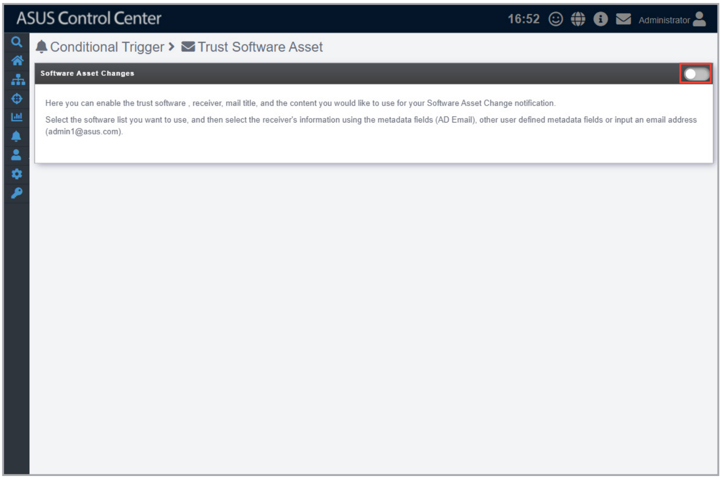
	Software Name	Version	Publisher	Install Date
1	PotPlayer-64 bit	1.7.18346	Kakao Corp.	2019-05-17
2	TeamViewer 14	14.2.8352	TeamViewer	2019-05-17
3	Advanced SystemCare 12	12.4.0	IObit	2019-05-17
4	HeavyLoad V3.4 (64 bit)	3.4	JAM Software	2019-05-17

===

This email and any attachments to it contain confidential information and are intended solely for the use of the individual to whom it is addressed.If you are not the intended recipient or receive it accidentally, please immediately notify the sender by e-mail and delete the message and any attachments from your computer system, and destroy all hard copies. If any, please be advised that any unauthorized disclosure, copying, distribution or any action taken or omitted in reliance on this, is illegal and prohibited. Furthermore, any views or opinions

To enable Trust Software Asset :

1. Click on the button to configure and enable Software Asset Changes notifications.



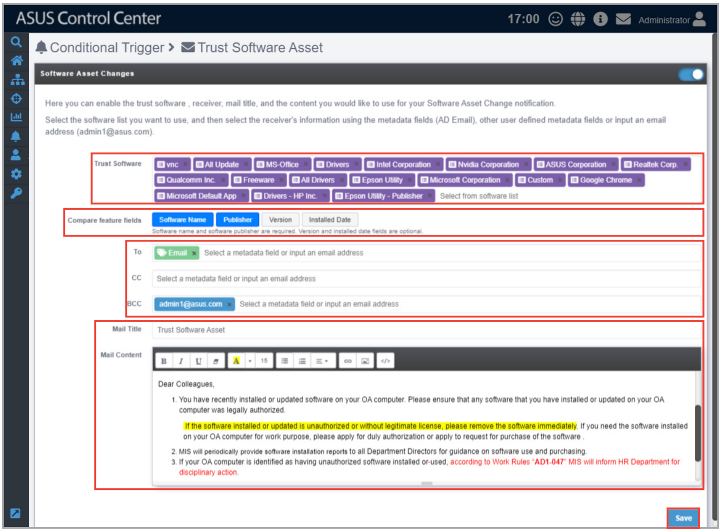
Here you can enable the trust software , receiver, mail title, and the content you would like to use for your Software Asset Change notification.

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).

2. Select softwares 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.

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.



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: vnc, All Update, MS-Office, Drivers, Intel Corporation, Nvidia Corporation, ASUS Corporation, Realtek Corp., Qualcomm Inc., Freeware, All 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: Email; Select a metadata field or input an email address

CC: Select a metadata field or input an email address

BCC: admin1@asus.com; Select a metadata field or input an email address

Mail Title: Trust Software Asset

Mail Content:

Dear Colleagues,

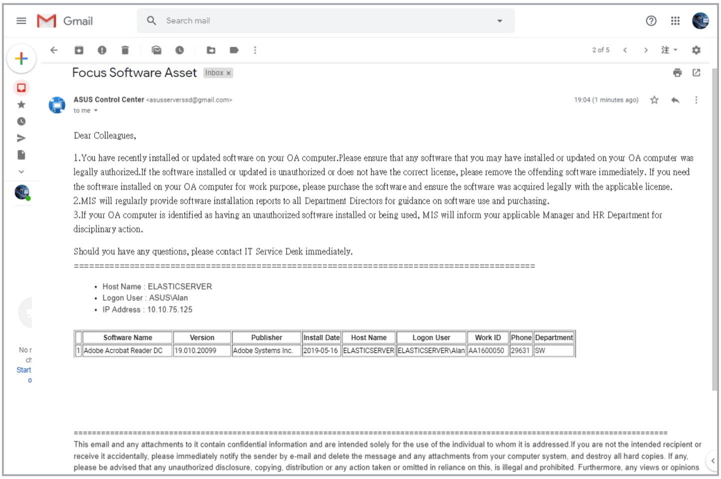
1. You have recently installed or updated software on your OA computer. Please ensure that any software that you have installed or updated on your OA computer was legally authorized.

   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 duly 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.

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.

6.1.2 Focus Software Asset

Focus Software Asset allows you to set notifications when there are *applications in the **Focus Software Asset*** being installed on *non-authorized managed devices*. These notifications will be sent immediately to the owner of non-authorized managed device as well as his/her director. Below is an example of a notification sent when an application in the Focus Software Asset is installed on a non-authorized managed device.



Focus Software Asset

ASUS Control Center <asusserverssd@gmail.com>
to me
19:04 (1 minutes ago)

Dear Colleagues,

1.You have recently installed or updated software on your OA computer.Please ensure that any software that you may have installed or updated on your OA computer was legally authorized.If the software installed or updated is unauthorized or does not have the correct license, please remove the offending software immediately. If you need the software installed on your OA computer for work purpose, please purchase the software and ensure the software was acquired legally with the applicable license.
2.MIS will regularly provide software installation reports to all Department Directors for guidance on software use and purchasing.
3.If your OA computer is identified as having an unauthorized software installed or being used, MIS will inform your applicable Manager and HR Department for disciplinary action.

Should you have any questions, please contact IT Service Desk immediately.
===

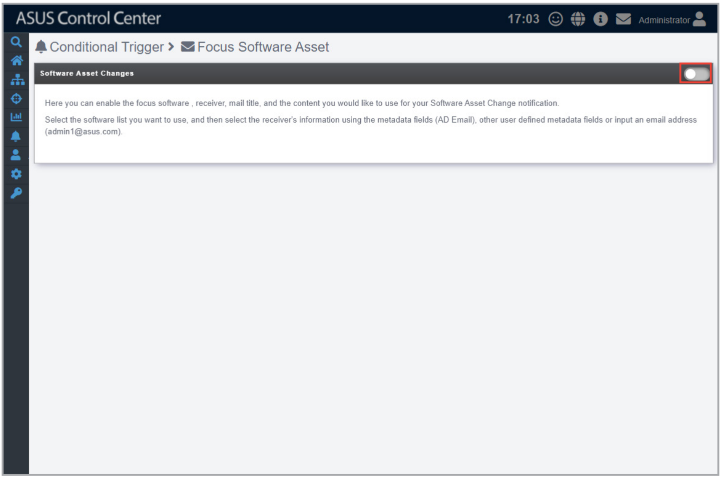
- Host Name : ELASTICSERVER
- Logon User : ASUS\Alan
- IP Address : 10.10.75.125

	Software Name	Version	Publisher	Install Date	Host Name	Logon User	Work ID	Phone	Department
1	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Inc.	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW

==
This email and any attachments to it contain confidential information and are intended solely for the use of the individual to whom it is addressed.If you are not the intended recipient or receive it accidentally, please immediately notify the sender by e-mail and delete the message and any attachments from your computer system, and destroy all hard copies. If any, please be advised that any unauthorized disclosure, copying, distribution or any action taken or omitted in reliance on this, is illegal and prohibited. Furthermore, any views or opinions

<u>To enable Focus Software Asset :</u>

1. Click on the button to configure and enable Software Asset Changes notifications.



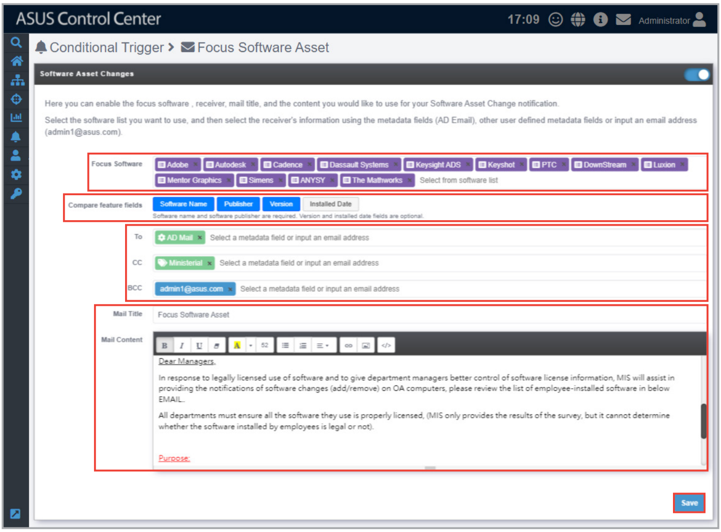
Here you can enable the focus software , receiver, mail title, and the content you would like to use for your Software Asset Change notification.

Select 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).

2. Select softwares 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.

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.



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 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).

Focus Software: Adobe, Autodesk, Cadence, Dassault Systems, Keysight ADS, Keyshot, PTC, DownStream, Luxion, Mentor Graphics, Simens, ANYSY, The Mathworks — 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: Ministerial — 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 OA computers, please review the list of employee-installed software in below EMAIL.

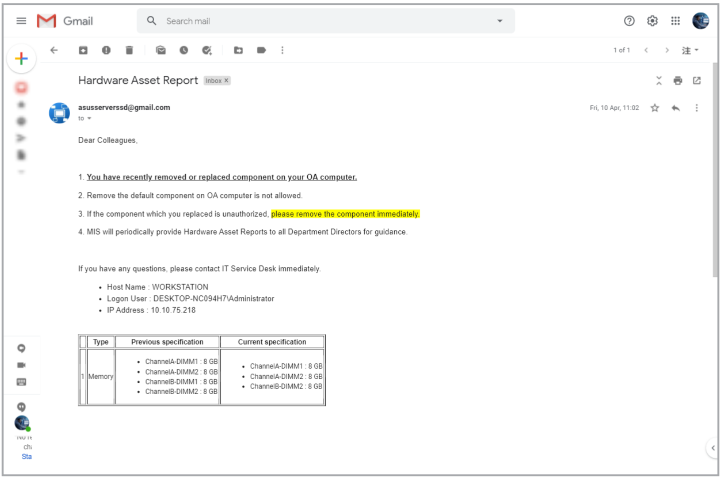
All departments must ensure all the software they use is properly licensed, (MIS only provides the results of the survey, but it cannot determine whether the software installed by employees is legal or not).

Purpose:

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.

6.1.3 Hardware Asset

Hardware Asset allows you to set notifications when there are *hardware components which do not comply to company specifications* being installed on managed devices, or if *spec components are being removed* from managed devices. These notifications will be sent immediately to the owner of managed device as well as his/her director and will list the hardware changes. Below is an example of a notification sent when a DIMM is removed from a managed device.



Hardware Asset Report Inbox ×

asusserverssd@gmail.com
to

Fri, 10 Apr, 11:02

Dear Colleagues,

1. You have recently removed or replaced component on your OA computer.

2. Remove the default component on OA computer is not allowed.

3. If the component which you replaced is unauthorized, please remove the component immediately.

4. MIS will periodically provide Hardware Asset Reports to all Department Directors for guidance.

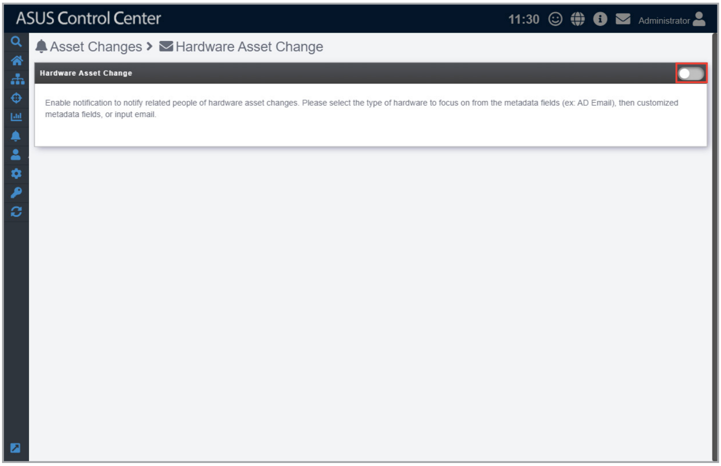
If you have any questions, please contact IT Service Desk immediately.

- Host Name : WORKSTATION
- Logon User : DESKTOP-NC094H7\Administrator
- IP Address : 10.10.75.218

	Type	Previous specification	Current specification
1	Memory	• ChannelA-DIMM1 : 8 GB • ChannelA-DIMM2 : 8 GB • ChannelB-DIMM1 : 8 GB • ChannelB-DIMM2 : 8 GB	• ChannelA-DIMM1 : 8 GB • ChannelA-DIMM2 : 8 GB • ChannelB-DIMM2 : 8 GB

<u>To enable Hardware Asset :</u>

1. Click on the button to configure and enable Hardware Asset change notifications.

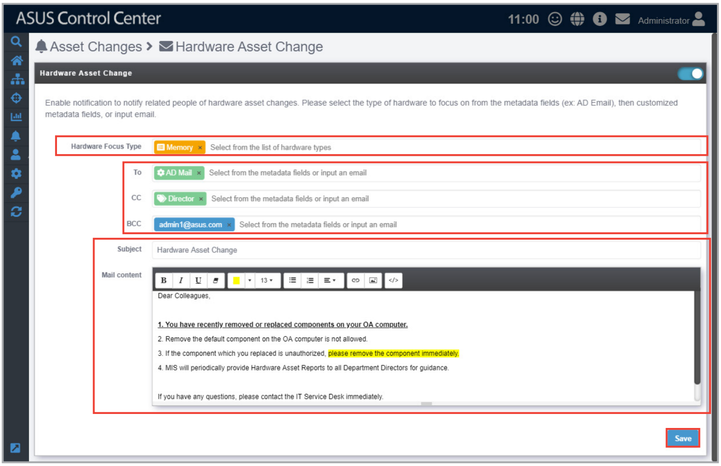


Enable notification to notify related people of hardware asset changes. Please select the type of hardware to focus on from the metadata fields (ex: AD Email), then customized metadata fields, or input email.

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.



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: admin1@asus.com × Select from the metadata fields or input an email

Subject: Hardware Asset Change

Mail content:

Dear Colleagues,

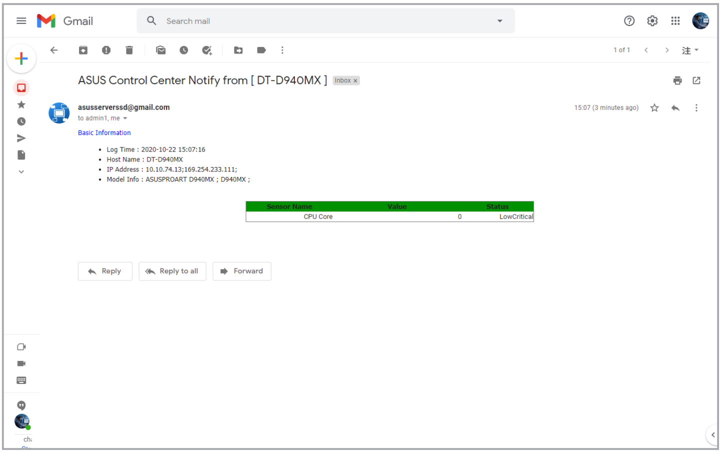
1. You have recently removed or replaced components on your OA computer.
2. Remove the default component on the OA computer is not allowed.
3. If the component which you replaced is unauthorized, please remove the component immediately.
4. MIS will periodically provide Hardware Asset Reports to all Department Directors for guidance.

If you have any questions, please contact the IT Service Desk immediately.

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.

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**.



ASUS Control Center Notify from [DT-D940MX]

asusserverssd@gmail.com
to admin1, me

Basic Information

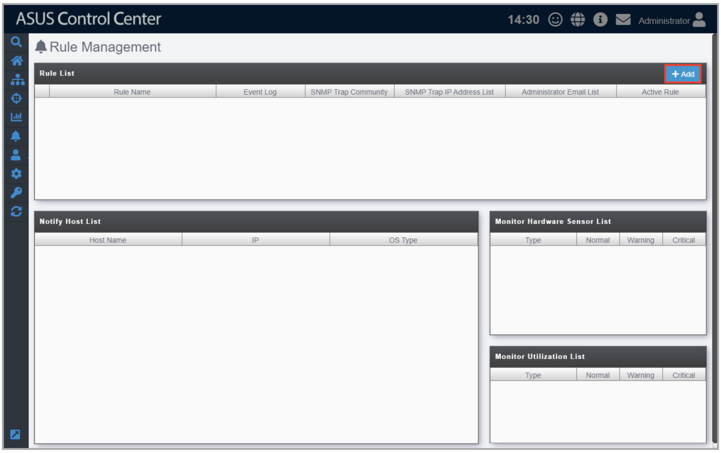
- Log Time : 2020-10-22 15:07:16
- Host Name : DT-D940MX
- IP Address : 10.10.74.13;169.254.233.111;
- Model Info : ASUSPROART D940MX ; D940MX ;

Sensor Name	Value	Status
CPU Core	0	LowCritical

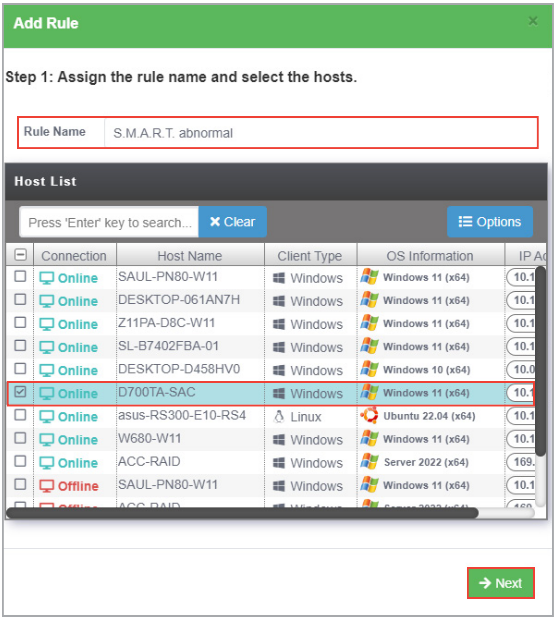
If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to the **Search and Filter devices** section.

Adding a new rule

1. Click **Add**.



2. Enter a rule name, then select the devices to apply the rule to. Click **Next**.



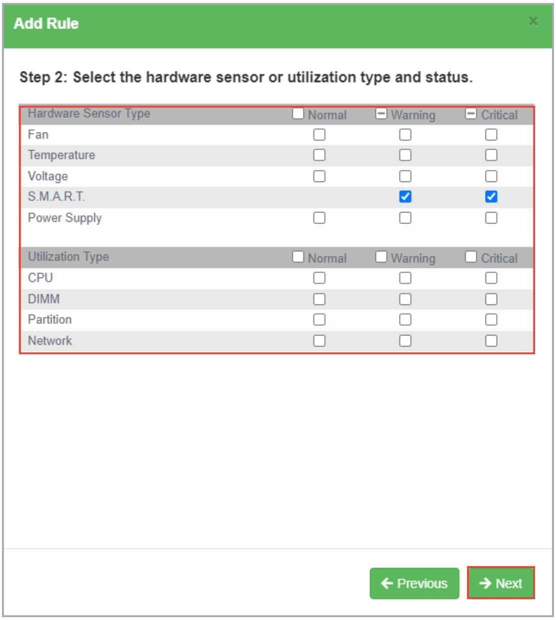
Step 1: Assign the rule name and select the hosts.

Rule Name: S.M.A.R.T. abnormal

☐	Connection	Host Name	Client Type	OS Information	IP Ac
☐	Online	SAUL-PN80-W11	Windows	Windows 11 (x64)	10.1
☐	Online	DESKTOP-061AN7H	Windows	Windows 11 (x64)	10.1
☐	Online	Z11PA-D8C-W11	Windows	Windows 11 (x64)	10.1
☐	Online	SL-B7402FBA-01	Windows	Windows 11 (x64)	10.1
☐	Online	DESKTOP-D458HV0	Windows	Windows 10 (x64)	10.0
☑	Online	D700TA-SAC	Windows	Windows 11 (x64)	10.1
☐	Online	asus-RS300-E10-RS4	Linux	Ubuntu 22.04 (x64)	10.1
☐	Online	W680-W11	Windows	Windows 11 (x64)	10.1
☐	Online	ACC-RAID	Windows	Server 2022 (x64)	169.
☐	Offline	SAUL-PN80-W11	Windows	Windows 11 (x64)	10.1

3. Select conditions (type and status of hardware sensors or utilization) to send notifications, then click **Next**.

- 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.



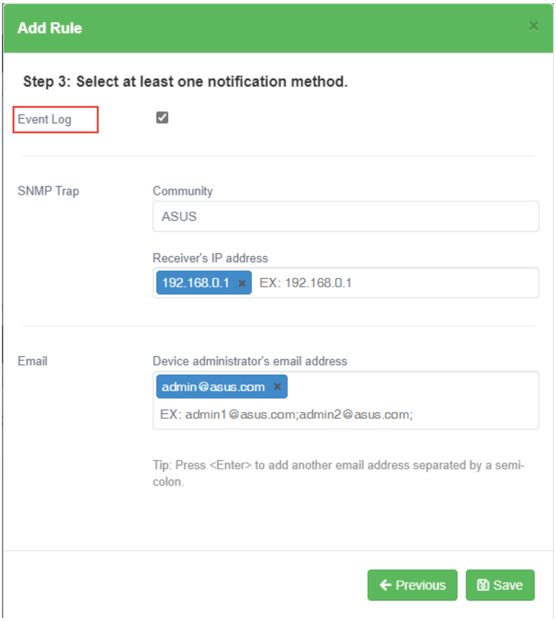
Step 2: Select the hardware sensor or utilization type and status.

Hardware Sensor Type	☐ Normal	⊟ Warning	⊟ Critical
Fan	☐	☐	☐
Temperature	☐	☐	☐
Voltage	☐	☐	☐
S.M.A.R.T.		☑	☑
Power Supply	☐	☐	☐
Utilization Type	**☐ Normal**	**☐ Warning**	**☐ Critical**
CPU	☐	☐	☐
DIMM	☐	☐	☐
Partition	☐	☐	☐
Network	☐	☐	☐

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

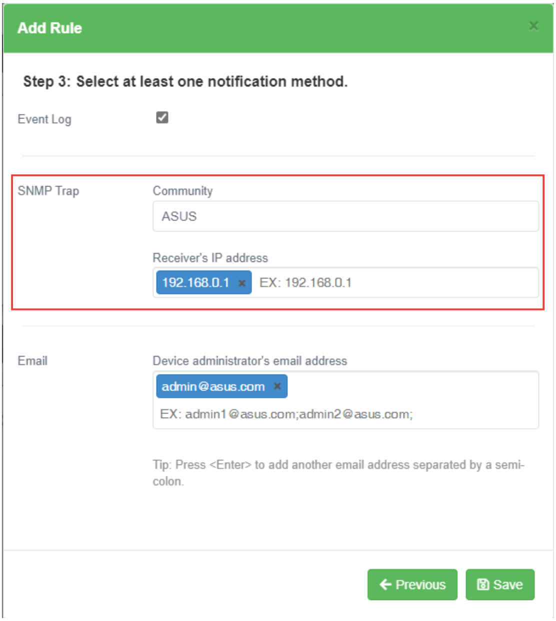
admin@asus.com ×

EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

- 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 ×

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;

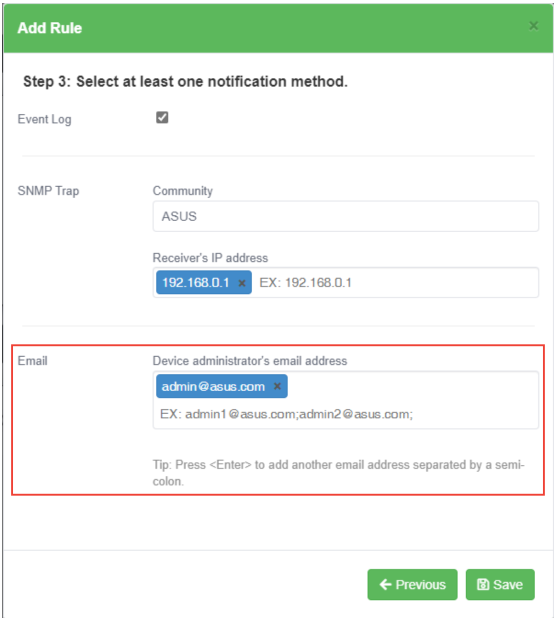
Tip: Press <Enter> to add another email address separated by a semi-colon.

- Email

  The notification is sent to the entered email addresses of the IT department as well as all people associated with the device.

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

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

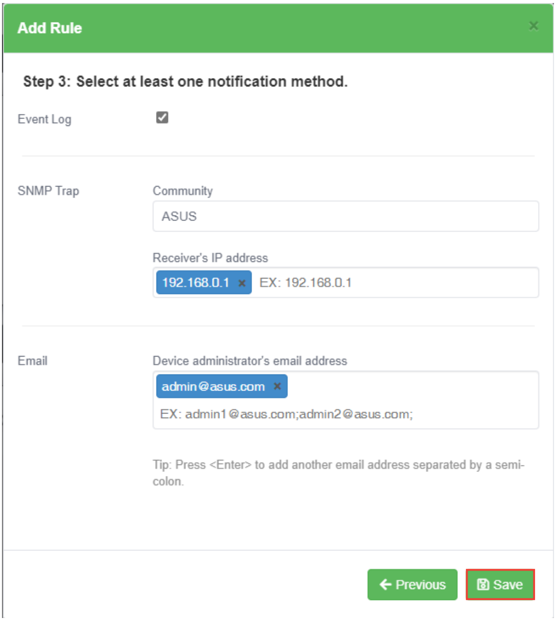
Email

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.

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

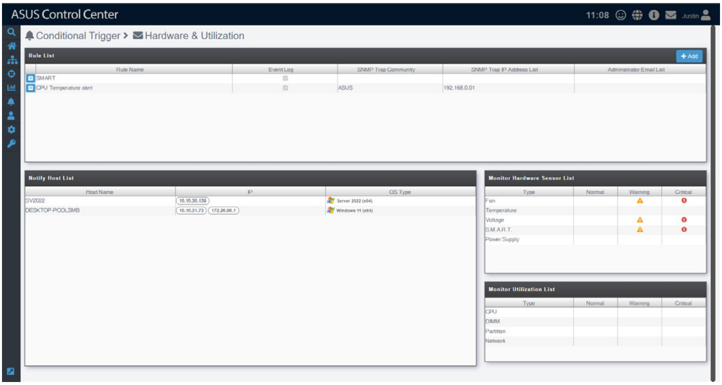
Email

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.

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**.



Rule List

Rule Name	Event Log	SNMP Trap Community	SNMP Trap IP Address List	Administrator Email List
SMART	☑			
CPU Temperature alert	☑	ASUS	192.168.0.01	

Notify Host List

Host Name	IP	OS Type
SV2022	10.10.30.139	Server 2022 (x64)
DESKTOP-PCOLSMB	10.10.31.73 172.26.96.1	Windows 11 (x64)

Monitor Hardware Sensor List

Type	Normal	Warning	Critical
Fan		⚠	❗
Temperature			
Voltage		⚠	❗
S.M.A.R.T.		⚠	❗
Power Supply			

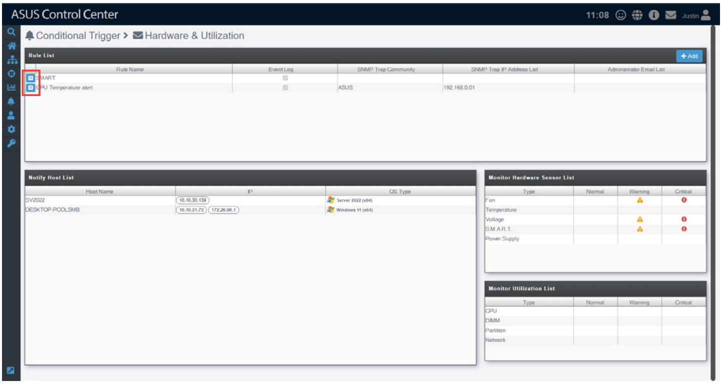
Monitor Utilization List

Type	Normal	Warning	Critical
CPU			
DIMM			
Partition			
Network			

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.

Editing an existing rule

1. Click on ☰ next to the rule you wish to edit.



ASUS Control Center

11:08 Justin

Conditional Trigger > Hardware & Utilization

Rule List + Add

	Rule Name	Event Log	SNMP Trap Community	SNMP Trap IP Address List	Administrator Email List
☰	SMART	☑			
☰	CPU Temperature alert	☑	ASUS	192.168.0.01	

Notify Host List

Host Name	IP	OS Type
SV2022	10.10.30.139	Server 2022 (x64)
DESKTOP-PCOLSMB	10.10.31.73 172.26.96.1	Windows 11 (x64)

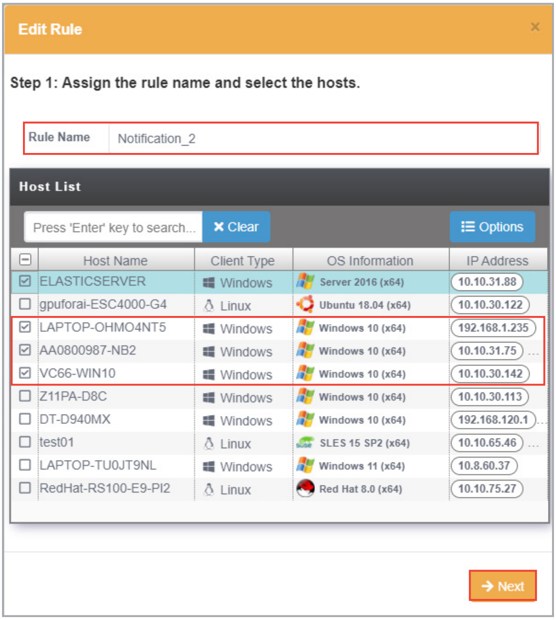
Monitor Hardware Sensor List

Type	Normal	Warning	Critical
Fan		⚠	●
Temperature			
Voltage		⚠	●
S.M.A.R.T.		⚠	●
Power Supply			

Monitor Utilization List

Type	Normal	Warning	Critical
CPU			
DIMM			
Partition			
Network			

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

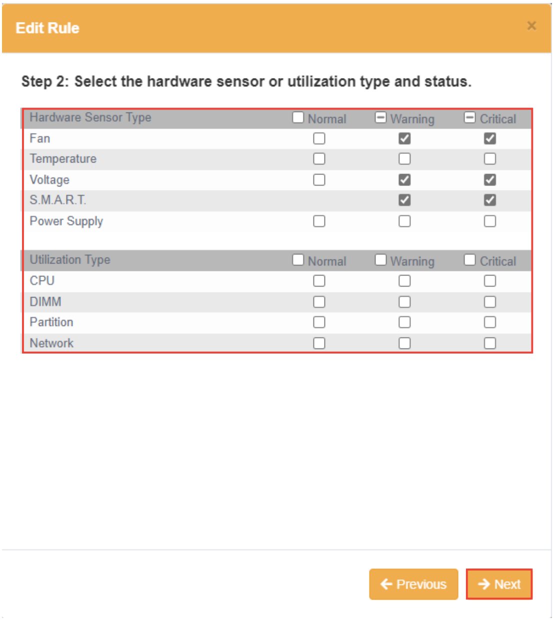
Press 'Enter' key to search... ✖ Clear ☰ Options

⊟	Host Name	Client Type	OS Information	IP Address
☑	ELASTICSERVER	Windows	Server 2016 (x64)	10.10.31.88
☐	gpuforai-ESC4000-G4	Linux	Ubuntu 18.04 (x64)	10.10.30.122
☑	LAPTOP-OHMO4NT5	Windows	Windows 10 (x64)	192.168.1.235
☑	AA0800987-NB2	Windows	Windows 10 (x64)	10.10.31.75 ...
☑	VC66-WIN10	Windows	Windows 10 (x64)	10.10.30.142
☐	Z11PA-D8C	Windows	Windows 10 (x64)	10.10.30.113
☐	DT-D940MX	Windows	Windows 10 (x64)	192.168.120.1 ...
☐	test01	Linux	SLES 15 SP2 (x64)	10.10.65.46 ...
☐	LAPTOP-TU0JT9NL	Windows	Windows 11 (x64)	10.8.60.37
☐	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**.

- 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.



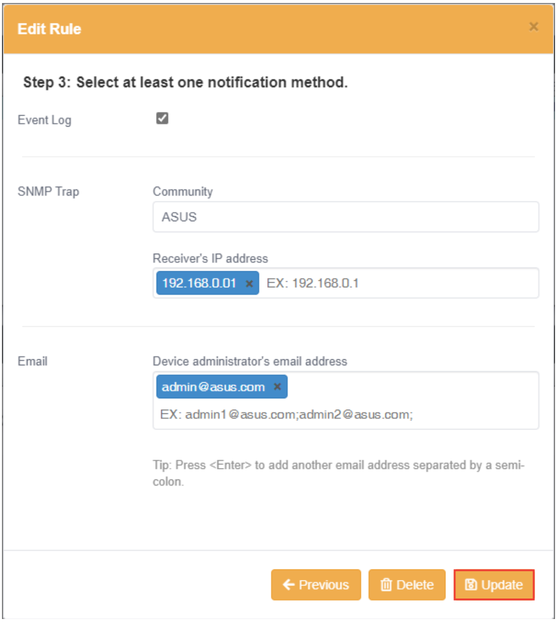
Step 2: Select the hardware sensor or utilization type and status.

Hardware Sensor Type	□ Normal	⊟ Warning	⊟ Critical
Fan	□	☑	☑
Temperature	□	□	□
Voltage	□	☑	☑
S.M.A.R.T.		☑	☑
Power Supply	□	□	□

Utilization Type	□ Normal	□ Warning	□ Critical
CPU	□	□	□
DIMM	□	□	□
Partition	□	□	□
Network	□	□	□

4. Select the notification method (multiple notification methods may be selected).

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 ×

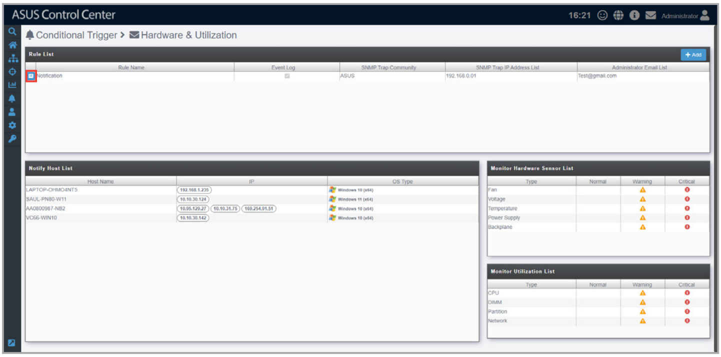
EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semi-colon.

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.



Rule List

	Rule Name	Event Log	SNMP Trap Community	SNMP Trap IP Address List	Administrator Email List
☰	Notification	☑	ASUS	192.168.0.01	Test@gmail.com

Notify Host List

Host Name	IP	OS Type
LAPTOP-OHMO4NT5	192.168.1.235	Windows 10 (x64)
SAUL-PN80-W11	10.10.30.124	Windows 11 (x64)
AA0800987-NB2	10.95.129.27 10.10.31.75 169.254.91.51	Windows 10 (x64)
VC66-WIN10	10.10.30.142	Windows 10 (x64)

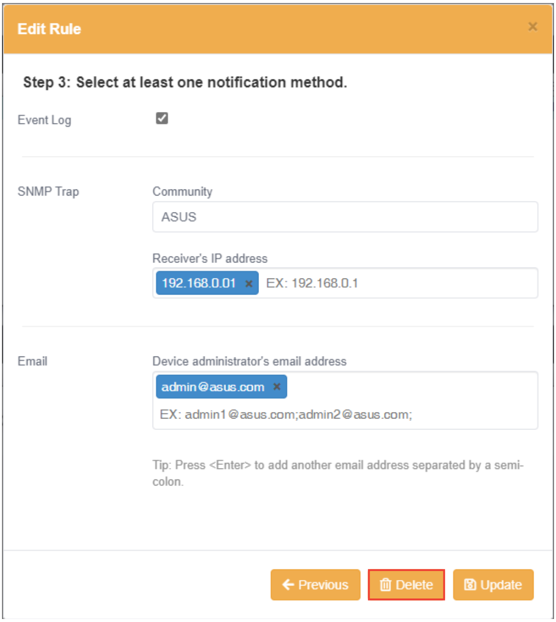
Monitor Hardware Sensor List

Type	Normal	Warning	Critical
Fan		⚠	●
Voltage		⚠	●
Temperature		⚠	●
Power Supply		⚠	●
Backplane		⚠	●

Monitor Utilization List

Type	Normal	Warning	Critical
CPU		⚠	●
DIMM		⚠	●
Partition		⚠	●
Network		⚠	●

2. Click **Next**, then **Next** again until you reach the following window, then click **Delete**.



Step 3: Select at least one notification method.

Event Log ☑

SNMP Trap

Community: ASUS

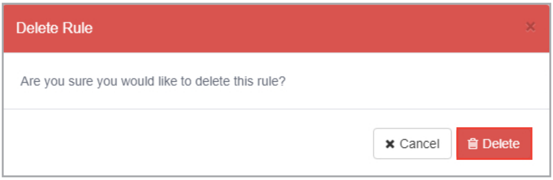
Receiver's IP address: 192.168.0.01 × EX: 192.168.0.1

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.

3. Click **Delete** on the pop up window to delete the rule.



Delete Rule

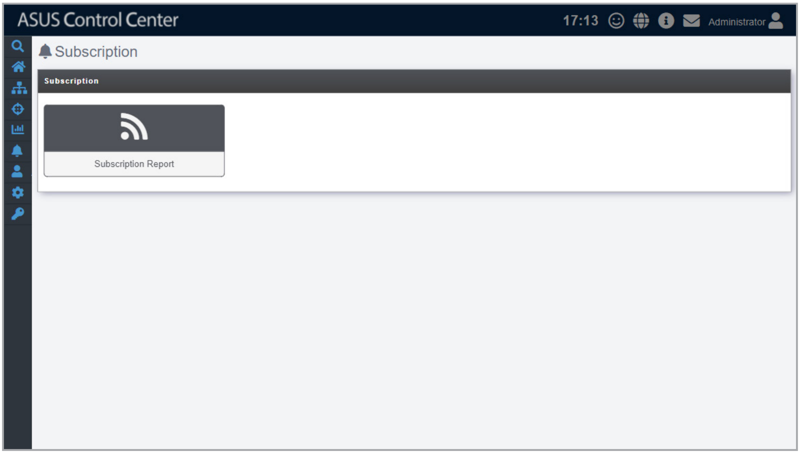
Are you sure you would like to delete this rule?

6.2 Subscription

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**.

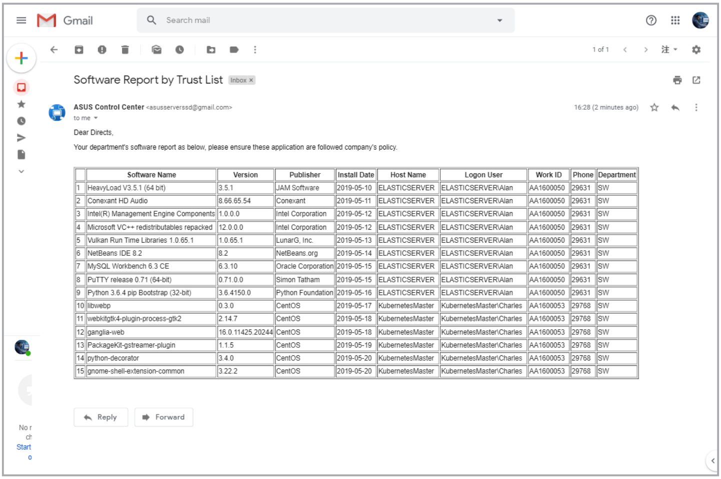


6.2.1 Subscription Report

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.

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 <asusserverssd@gmail.com>

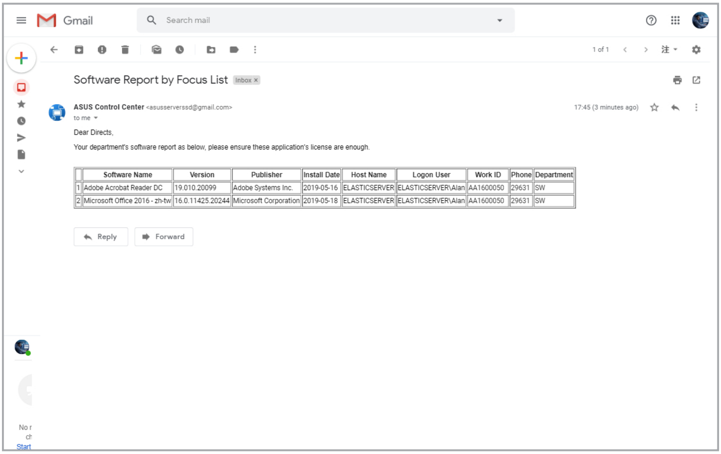
16:28 (2 minutes ago)

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	Logon User	Work ID	Phone	Department
1	HeavyLoad V3.5.1 (64 bit)	3.5.1	JAM Software	2019-05-10	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
2	Conexant HD Audio	8.66.65.54	Conexant	2019-05-11	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
3	Intel(R) Management Engine Components	1.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
4	Microsoft VC++ redistributables repacked	12.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
5	Vulkan Run Time Libraries 1.0.65.1	1.0.65.1	LunarG, Inc.	2019-05-13	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
6	NetBeans IDE 8.2	8.2	NetBeans.org	2019-05-14	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
7	MySQL Workbench 6.3 CE	6.3.10	Oracle Corporation	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
8	PuTTY release 0.71 (64-bit)	0.71.0.0	Simon Tatham	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
9	Python 3.6.4 pip Bootstrap (32-bit)	3.6.4150.0	Python Foundation	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
10	libwebp	0.3.0	CentOS	2019-05-17	KubernetesMaster	KubernetesMaster\Charles	AA1600053	29768	SW
11	webkitgtk4-plugin-process-gtk2	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	PackageKit-gstreamer-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 softwares of a department's managed devices.



Software Report by Focus List

ASUS Control Center <asusserverssd@gmail.com>
to me

17:45 (3 minutes ago)

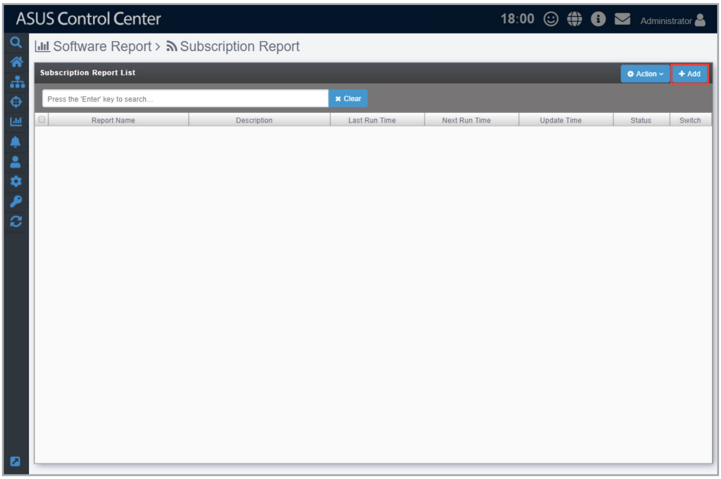
Dear Directs,

Your department's software report as below, please ensure these application's license are enough.

	Software Name	Version	Publisher	Install Date	Host Name	Logon User	Work ID	Phone	Department
1	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Inc.	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
2	Microsoft Office 2016 - zh-tw	16.0.11425.20244	Microsoft Corporation	2019-05-18	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW

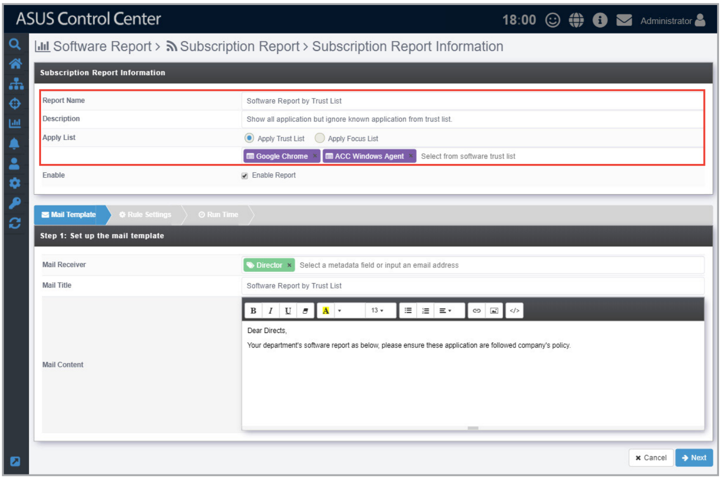
<u>To create a Subscription Report:</u>

1. 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.

- 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.



Software Report > Subscription Report > Subscription Report Information

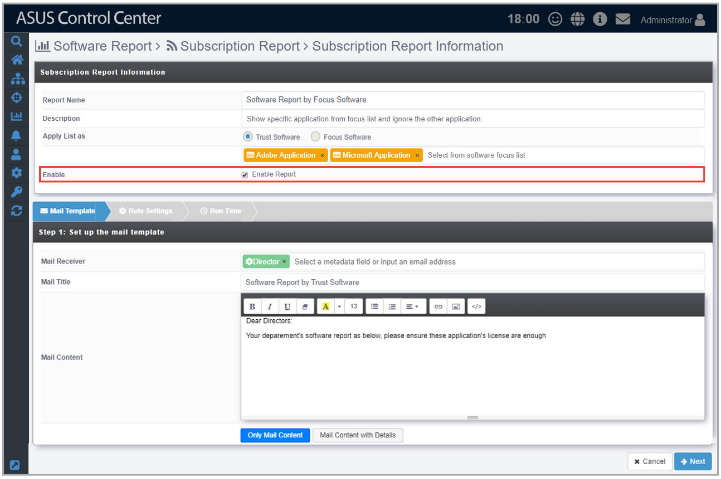
Subscription Report Information

Report Name	Software Report by Trust List
Description	Show all application but ignore known application from trust list.
Apply List	● Apply Trust List ○ Apply Focus List
	Google Chrome × ACC Windows Agent × Select from software trust list
Enable	☑ Enable Report

Step 1: Set up the mail template

Mail Receiver	Director × Select a metadata field or input an email address
Mail Title	Software Report by Trust List
Mail Content	Dear Directs, Your department's software report as below, please ensure these application are followed company's policy.

3. Check **Enable Report** to enable this report.



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	● Trust Software ○ Focus Software
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

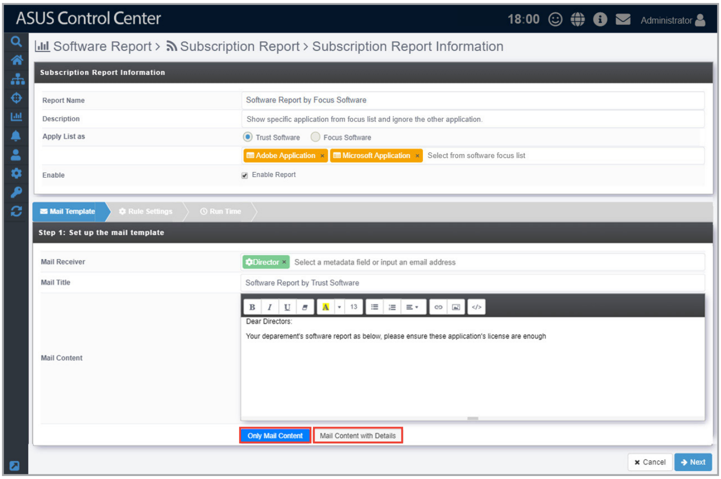
Step 1: Set up the mail template

Mail Receiver	Director × Select a metadata field or input an email address
Mail Title	Software Report by Trust Software
Mail Content	Dear Directors: Your deparement's software report as below, please ensure these application's license are enough
	Only Mail Content Mail Content with Details

4. Select a metadata tag or enter an email address into the **Mail Receiver** field, then enter your mail title and mail content.

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.



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	● Trust Software ○ Focus Software
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

Mail Template
Rule Settings
Run Time

Step 1: Set up the mail template

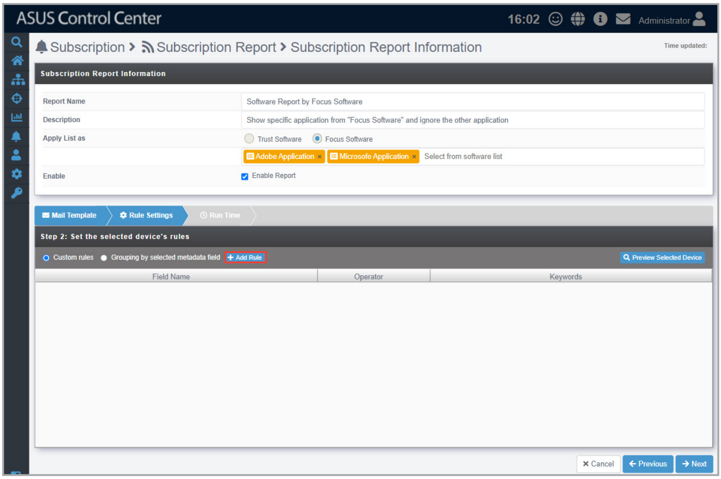
Mail Receiver	Director × Select a metadata field or input an email address
Mail Title	Software Report by Trust Software
Mail Content	Dear Directors: Your deparement's software report as below, please ensure these application's license are enough

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.

- 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**.

Follow this step only if you selected the **Custom rules** option.



Subscription > Subscription Report > Subscription Report Information

Time updated:

Subscription Report Information

Report Name: Software Report by Focus Software

Description: Show specific application from "Focus Software" and ignore the other application

Apply List as: ○ Trust Software ● Focus Software

Adobe Application × Microsofe Application × Select from software list

Enable: ☑ Enable Report

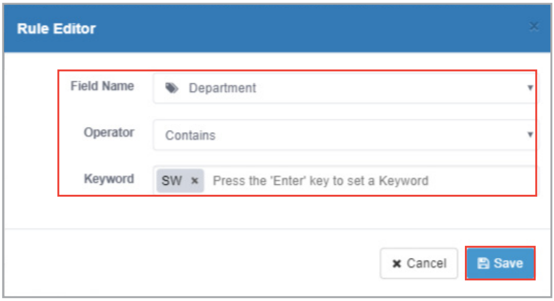
Step 2: Set the selected device's rules

● Custom rules ○ Grouping by selected metadata field + Add Rule

Field Name	Operator	Keywords

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**.

Follow this step only if you selected the **Custom rules** option.



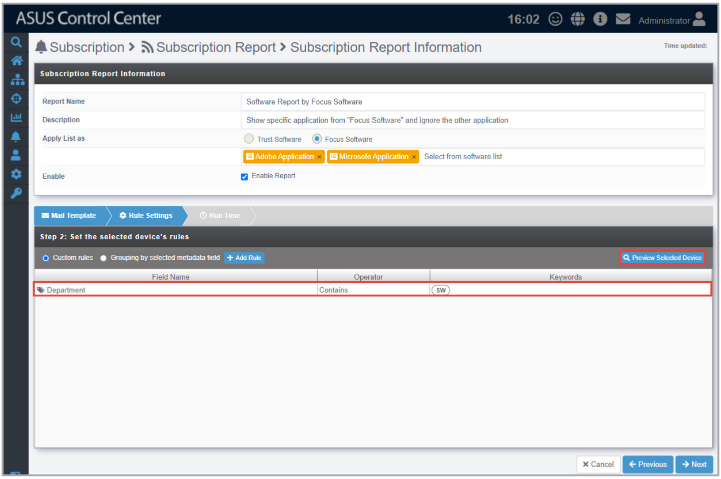
Rule Editor

Field Name: Department

Operator: Contains

Keyword: SW × Press the 'Enter' key to set a Keyword

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.



ASUS Control Center
16:02
Administrator
Subscription > Subscription Report > Subscription Report Information
Time updated:

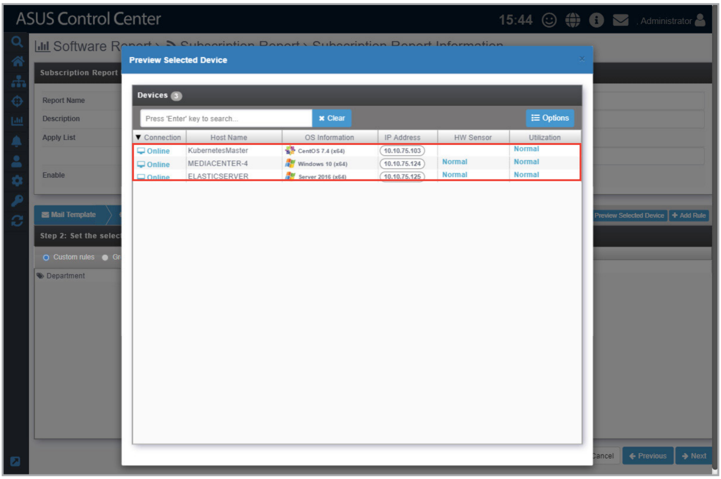
Subscription Report Information

Report Name	Software Report by Focus Software
Description	Show specific application from "Focus Software" and ignore the other application
Apply List as	○ Trust Software ● Focus Software
	Adobe Application × Microsofe Application × Select from software list
Enable	☑ Enable Report

Step 2: Set the selected device's rules

● Custom rules ● Grouping by selected metadata field

Field Name	Operator	Keywords
Department	Contains	SW

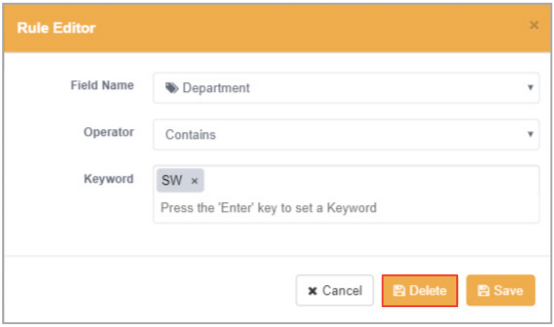


Press 'Enter' key to search...

▼ Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103		Normal
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	Normal	Normal
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	Normal

10. Repeat steps 6 to 8 to add another rule.

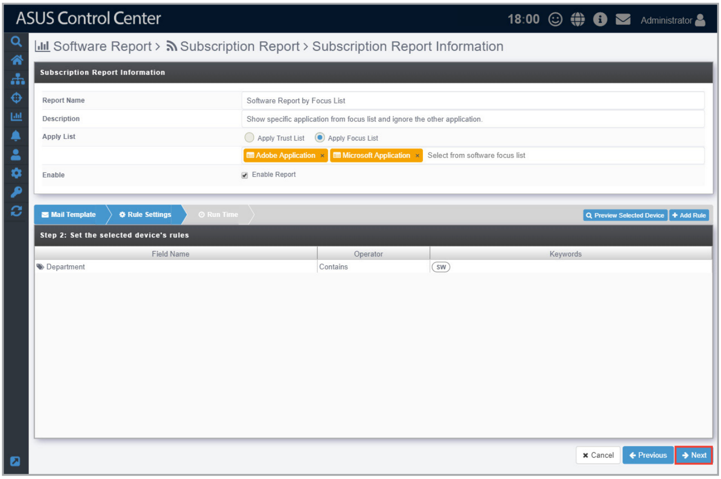
11. (optional) You may also edit or delete a rule by clicking on the rule, then repeat steps 4 to edit the rule, or click on **Delete** to delete the rule.



Rule Editor

Field Name	Department
Operator	Contains
Keyword	SW × Press the 'Enter' key to set a Keyword

12. Click on **Next** once you are finished.



ASUS Control Center

Software Report > Subscription Report > Subscription Report Information

Subscription Report Information

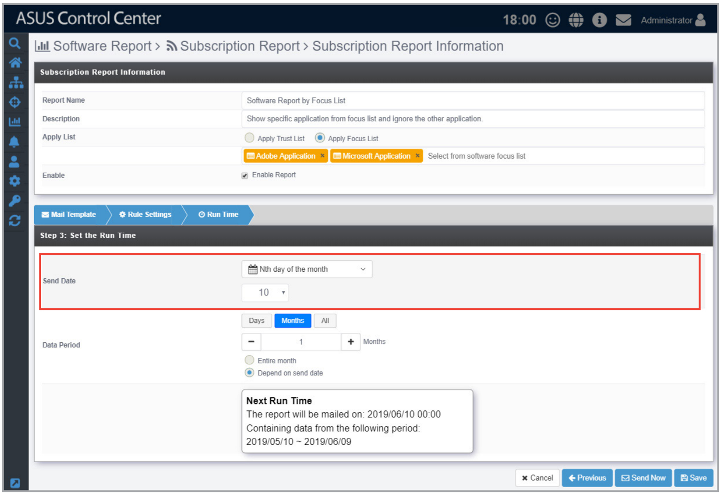
Report Name	Software Report by Focus List
Description	Show specific application from focus list and ignore the other application.
Apply List	○ Apply Trust List ● Apply Focus List
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

Step 2: Set the selected device's rules

Field Name	Operator	Keywords
Department	Contains	SW

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.


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
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

Mail Template
Rule Settings
Run Time

Step 3: Set the Run Time

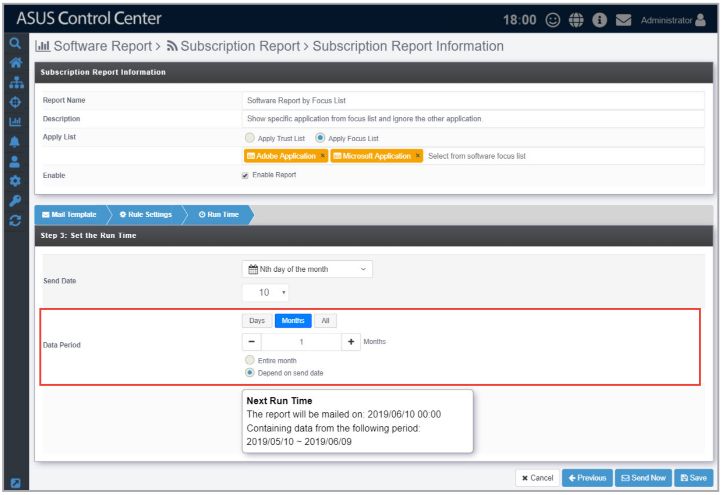
Send Date	Nth day of the month 10
Data Period	Days [✓ Months] All − 1 + Months ○ Entire month ● Depend on send date

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

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.



Software Report > Subscription Report > Subscription Report Information

Subscription Report Information

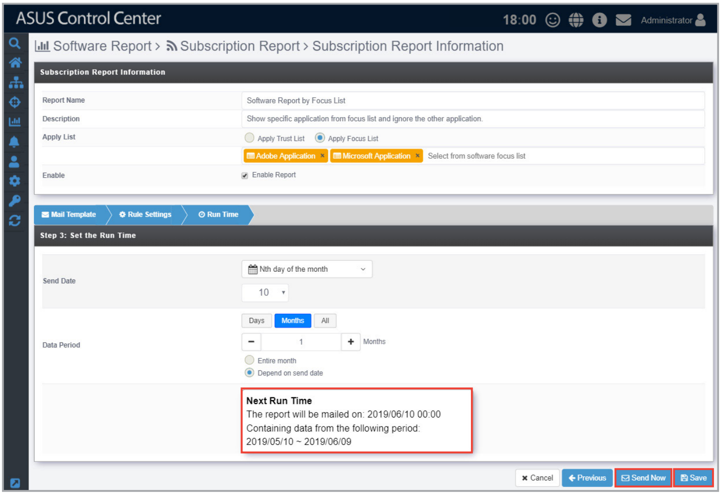
Report Name	Software Report by Focus List
Description	Show specific application from focus list and ignore the other application.
Apply List	○ Apply Trust List ● Apply Focus List
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

Step 3: Set the Run Time

Send Date	Nth day of the month 10
Data Period	Days [✓ Months] 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

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.


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
	Adobe Application × Microsoft Application × Select from software focus list
Enable	☑ Enable Report

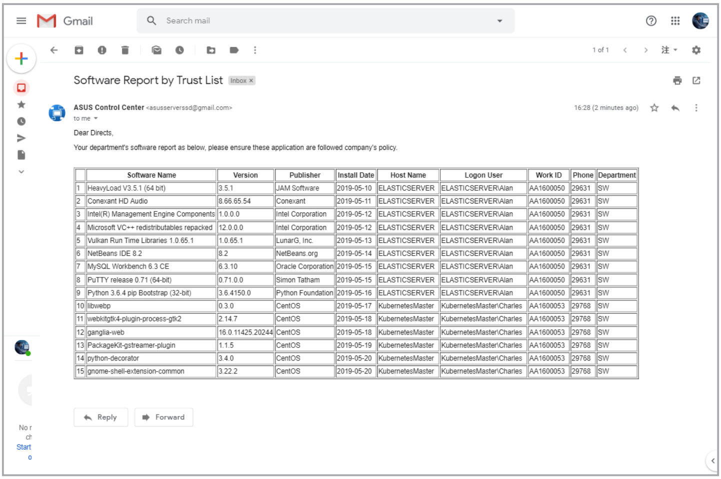
Mail Template
Rule Settings
Run Time

Step 3: Set the Run Time

Send Date	Nth day of the month 10
Data Period	Days [✓ Months] 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

- Report as a result of applying **Trust Software Asset**. (Does not show white listed applications)



Software Report by Trust List

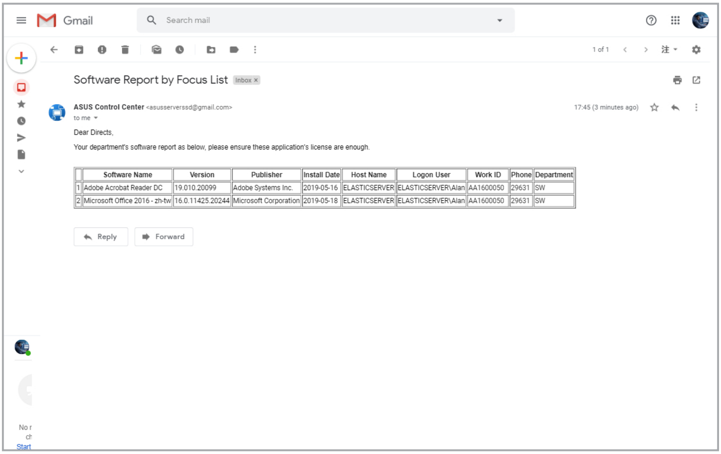
ASUS Control Center <asusserverssd@gmail.com>
to me
16:28 (2 minutes ago)

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	Logon User	Work ID	Phone	Department
1	HeavyLoad V3.5.1 (64 bit)	3.5.1	JAM Software	2019-05-10	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
2	Conexant HD Audio	8.66.65.54	Conexant	2019-05-11	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
3	Intel(R) Management Engine Components	1.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
4	Microsoft VC++ redistributables repacked	12.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
5	Vulkan Run Time Libraries 1.0.65.1	1.0.65.1	LunarG, Inc.	2019-05-13	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
6	NetBeans IDE 8.2	8.2	NetBeans.org	2019-05-14	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
7	MySQL Workbench 6.3 CE	6.3.10	Oracle Corporation	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
8	PuTTY release 0.71 (64-bit)	0.71.0.0	Simon Tatham	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
9	Python 3.6.4 pip Bootstrap (32-bit)	3.6.4150.0	Python Foundation	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
10	libwebp	0.3.0	CentOS	2019-05-17	KubernetesMaster	KubernetesMaster\Charles	AA1600053	29768	SW
11	webkitgtk4-plugin-process-gtk2	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	PackageKit-gstreamer-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

- Report as a result of applying **Focus Software Asset**. (Only shows applications on the focus list)



Software Report by Focus List Inbox ×

ASUS Control Center <asusserverssd@gmail.com>
to me
17:45 (3 minutes ago)

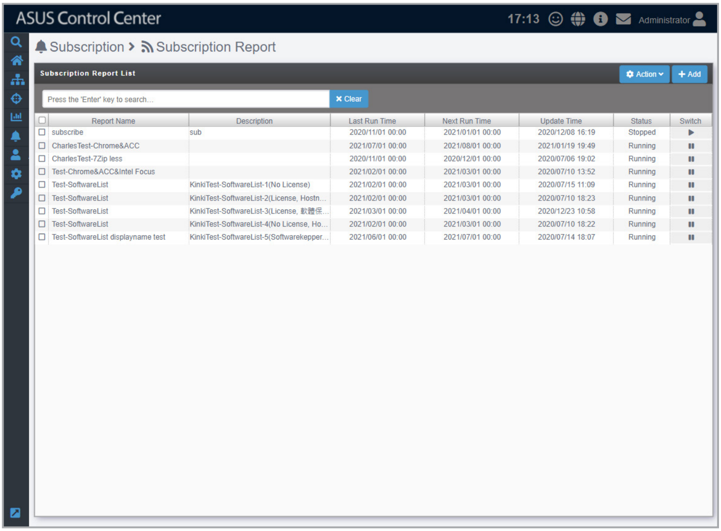
Dear Directs,

Your department's software report as below, please ensure these application's license are enough.

	Software Name	Version	Publisher	Install Date	Host Name	Logon User	Work ID	Phone	Department
1	Adobe Acrobat Reader DC	19.010.20099	Adobe Systems Inc.	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW
2	Microsoft Office 2016 - zh-tw	16.0.11425.20244	Microsoft Corporation	2019-05-18	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	SW

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.

16. Your new report subscription should appear in the Subscription Report List on the main screen of **Subscription Report**.

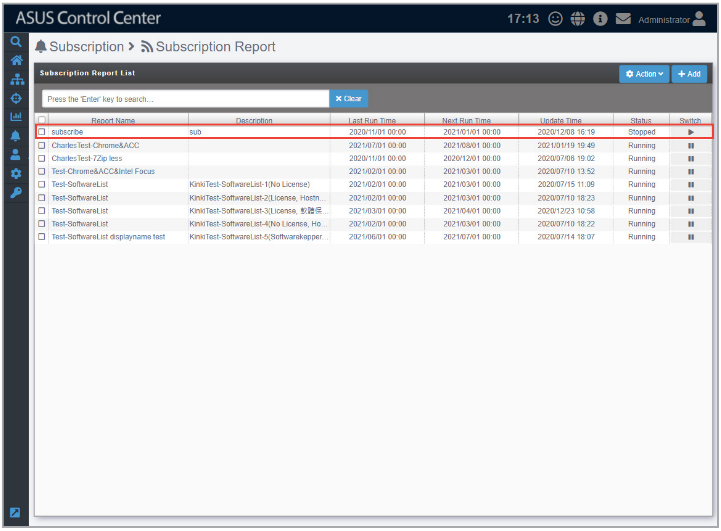

ASUS Control Center
17:13
Administrator
Subscription > Subscription Report
Action
+ Add
Press the 'Enter' key to search...
× Clear

Subscription Report List

□	Report Name	Description	Last Run Time	Next Run Time	Update Time	Status	Switch
□	subscribe	sub	2020/11/01 00:00	2021/01/01 00:00	2020/12/08 16:19	Stopped	▶
□	CharlesTest-Chrome&ACC		2021/07/01 00:00	2021/08/01 00:00	2021/01/19 19:49	Running	❚❚
□	CharlesTest-7Zip less		2020/11/01 00:00	2020/12/01 00:00	2020/07/06 19:02	Running	❚❚
□	Test-Chrome&ACC&Intel Focus		2021/02/01 00:00	2021/03/01 00:00	2020/07/10 13:52	Running	❚❚
□	Test-SoftwareList	KinkiTest-SoftwareList-1(No License)	2021/02/01 00:00	2021/03/01 00:00	2020/07/15 11:09	Running	❚❚
□	Test-SoftwareList	KinkiTest-SoftwareList-2(License, Hostn...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:23	Running	❚❚
□	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	❚❚
□	Test-SoftwareList	KinkiTest-SoftwareList-4(No License, Ho...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:22	Running	❚❚
□	Test-SoftwareList displayname test	KinkiTest-SoftwareList-5(Softwarekepper...	2021/06/01 00:00	2021/07/01 00:00	2020/07/14 18:07	Running	❚❚

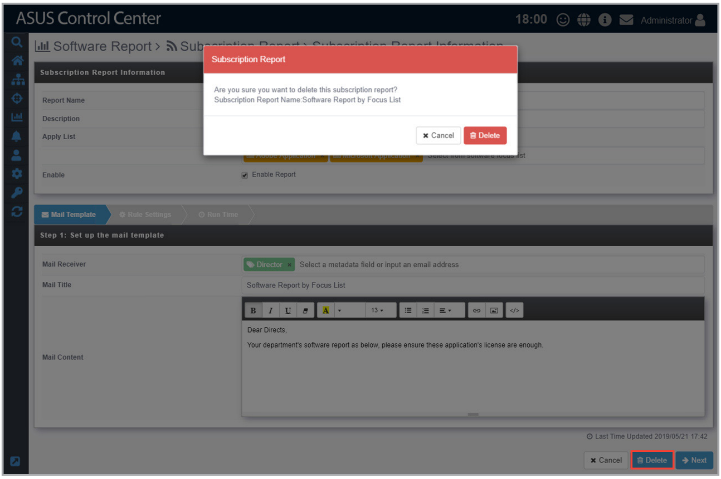
To edit or delete a subscription report:

1. Click on the subscription report you wish to edit.



☐	Report Name	Description	Last Run Time	Next Run Time	Update Time	Status	Switch
☐	subscribe	sub	2020/11/01 00:00	2021/01/01 00:00	2020/12/08 16:19	Stopped	▶
☐	CharlesTest-Chrome&ACC		2021/07/01 00:00	2021/08/01 00:00	2021/01/19 19:49	Running	❚❚
☐	CharlesTest-7Zip less		2020/11/01 00:00	2020/12/01 00:00	2020/07/06 19:02	Running	❚❚
☐	Test-Chrome&ACC&Intel Focus		2021/02/01 00:00	2021/03/01 00:00	2020/07/10 13:52	Running	❚❚
☐	Test-SoftwareList	KinkiTest-SoftwareList-1(No License)	2021/02/01 00:00	2021/03/01 00:00	2020/07/15 11:09	Running	❚❚
☐	Test-SoftwareList	KinkiTest-SoftwareList-2(License, Hostn...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:23	Running	❚❚
☐	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	❚❚
☐	Test-SoftwareList	KinkiTest-SoftwareList-4(No License, Ho...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:22	Running	❚❚
☐	Test-SoftwareList displayname test	KinkiTest-SoftwareList-5(Softwarekepper...	2021/06/01 00:00	2021/07/01 00:00	2020/07/14 18:07	Running	❚❚

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.



Subscription Report

Are you sure you want to delete this subscription report?
Subscription Report Name:Software Report by Focus List

✖ Cancel Delete

☑ Enable Report

Step 1: Set up the mail template

Mail Receiver: Director ✕ Select a metadata field or input an email address

Mail Title: Software Report by Focus List

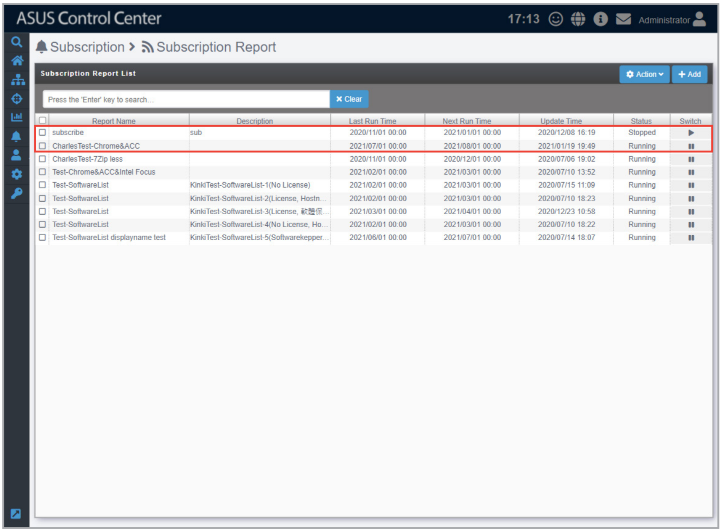
Dear Directs,

Your department's software report as below, please ensure these application's license are enough.

Last Time Updated 2019/05/21 17:42

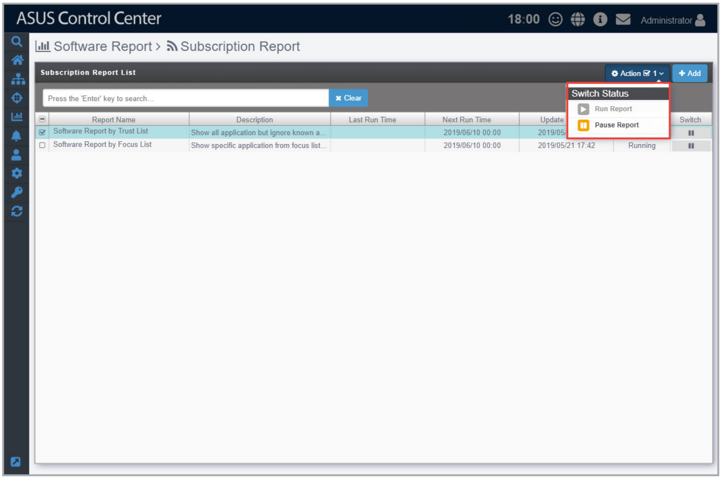
Switching the status of a subscription reports:

1. Click on the subscription reports you wish to switch the subscription status of.



☐	Report Name	Description	Last Run Time	Next Run Time	Update Time	Status	Switch
☐	subscribe	sub	2020/11/01 00:00	2021/01/01 00:00	2020/12/08 16:19	Stopped	▶
☐	CharlesTest-Chrome&ACC		2021/07/01 00:00	2021/08/01 00:00	2021/01/19 19:49	Running	⏸
☐	CharlesTest-7Zip less		2020/11/01 00:00	2020/12/01 00:00	2020/07/06 19:02	Running	⏸
☐	Test-Chrome&ACC&Intel Focus		2021/02/01 00:00	2021/03/01 00:00	2020/07/10 13:52	Running	⏸
☐	Test-SoftwareList	KinkiTest-SoftwareList-1(No License)	2021/02/01 00:00	2021/03/01 00:00	2020/07/15 11:09	Running	⏸
☐	Test-SoftwareList	KinkiTest-SoftwareList-2(License, Hostn...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:23	Running	⏸
☐	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	⏸
☐	Test-SoftwareList	KinkiTest-SoftwareList-4(No License, Ho...	2021/02/01 00:00	2021/03/01 00:00	2020/07/10 18:22	Running	⏸
☐	Test-SoftwareList displayname test	KinkiTest-SoftwareList-5(Softwarekepper...	2021/06/01 00:00	2021/07/01 00:00	2020/07/14 18:07	Running	⏸

2. Click on **Action**, then select if you want to pause or run the report.



⊟	Report Name	Description	Last Run Time	Next Run Time	Update		Switch
☑	Software Report by Trust List	Show all application but ignore known a...		2019/06/10 00:00	2019/05		⏸
☐	Software Report by Focus List	Show specific application from focus list...		2019/06/10 00:00	2019/05/21 17:42	Running	⏸

Chapter 7

Account Management

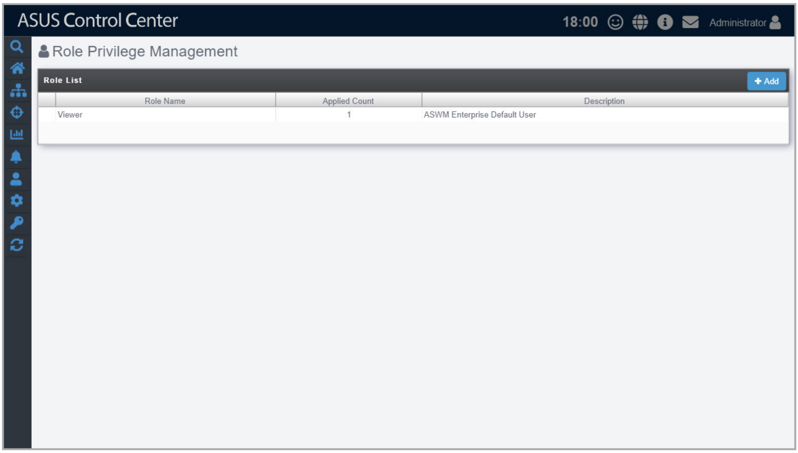
This chapter describes how to add and edit accounts and roles for different users.

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.

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**.

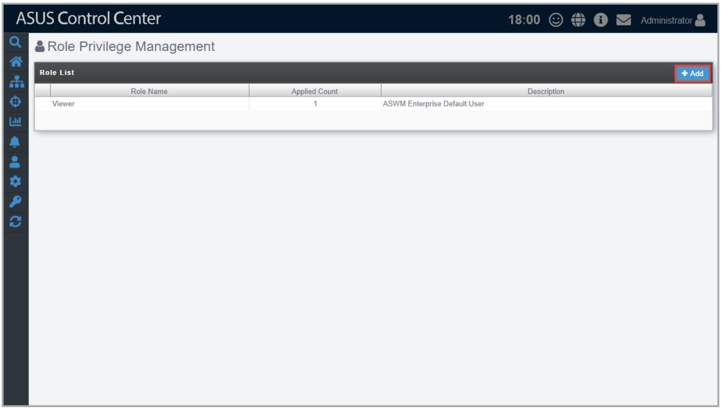


Role Name	Applied Count	Description
Viewer	1	ASWM Enterprise Default User

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**.



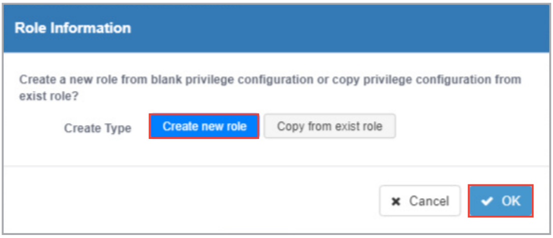
Role Privilege Management

Role List

Role Name	Applied Count	Description
Viewer	1	ASWM Enterprise Default User

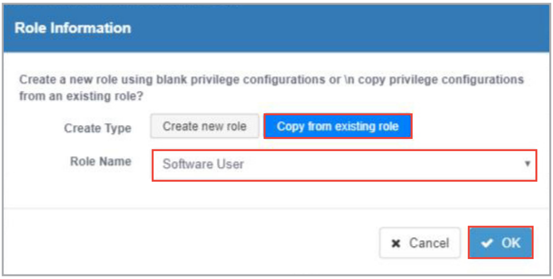
2. Select between **Create new role** and **Copy from exist role**, then click **OK**.

- **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.


Role Information

Create a new role from blank privilege configuration or copy privilege configuration from exist role?

Create Type: Create new role


Role Information

Create a new role using blank privilege configurations or \n copy privilege configurations from an existing role?

Create Type: Copy from existing role

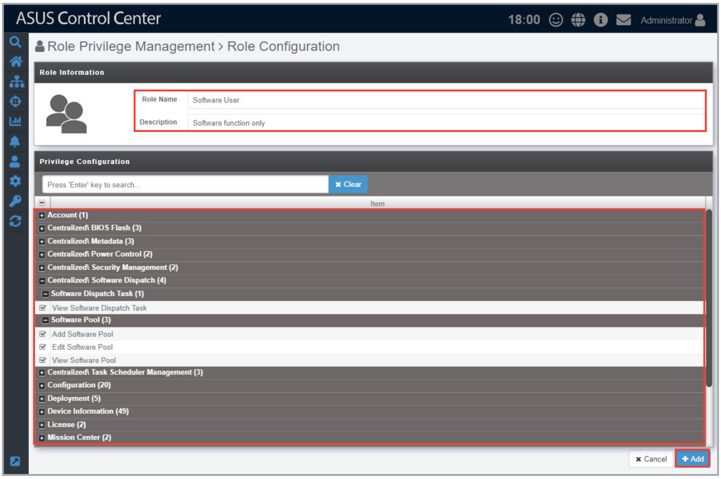
Role Name: Software User

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.

- 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.



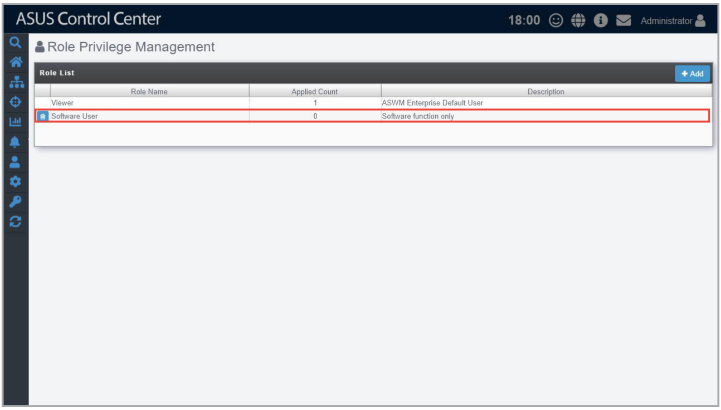
Role Name: Software User

Description: Software function only

⊞ Account (1)
⊞ Centralized\ BIOS Flash (3)
⊞ Centralized\ Metadata (3)
⊞ Centralized\ Power Control (2)
⊞ Centralized\ Security Management (2)
⊟ Centralized\ Software Dispatch (4)
⊟ Software Dispatch Task (1)
☑ View Software Dispatch Task
⊟ Software Pool (3)
☑ Add Software Pool
☑ Edit Software Pool
☑ View Software Pool
⊞ Centralized\ Task Scheduler Management (3)
⊞ Configuration (20)
⊞ Deployment (5)
⊞ Device Information (49)
⊞ License (2)
⊞ Mission Center (2)

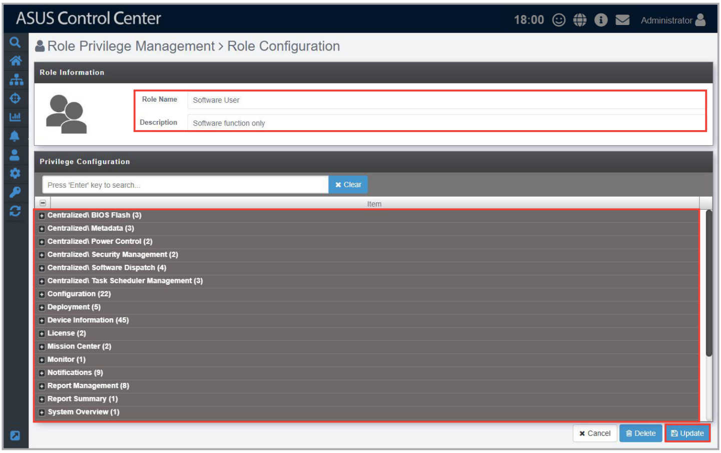
Editing a role

1. Click on the role you wish to edit from the Role List block.



Role Name	Applied Count	Description
Viewer	1	ASWM Enterprise Default User
Software User	0	Software function only

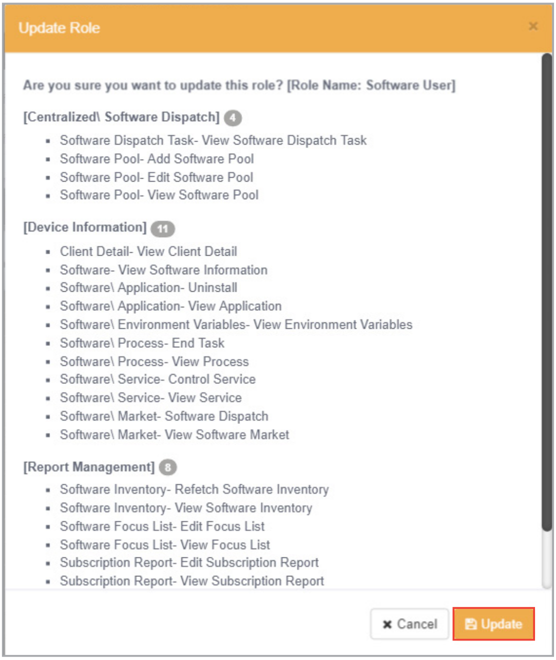
2. You can edit the **Role Name** and **Description**, and also configure the permissions in the Privilege Configuration list. Once you are finished click on **Update**.



Role Name	Software User
Description	Software function only

- Centralized\ BIOS Flash (3)
- Centralized\ Metadata (3)
- Centralized\ Power Control (2)
- Centralized\ Security Management (2)
- Centralized\ Software Dispatch (4)
- Centralized\ Task Scheduler Management (3)
- Configuration (22)
- Deployment (5)
- Device Information (45)
- License (2)
- Mission Center (2)
- Monitor (1)
- Notifications (9)
- Report Management (8)
- Report Summary (1)
- System Overview (1)

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.



Are you sure you want to update this role? [Role Name: Software User]

[Centralized\ Software Dispatch] 4

- Software Dispatch Task- View Software Dispatch Task
- Software Pool- Add Software Pool
- Software Pool- Edit Software Pool
- Software Pool- View Software Pool

[Device Information] 11

- Client Detail- View Client Detail
- Software- View Software Information
- Software\ Application- Uninstall
- Software\ Application- View Application
- Software\ Environment Variables- View Environment Variables
- Software\ Process- End Task
- Software\ Process- View Process
- Software\ Service- Control Service
- Software\ Service- View Service
- Software\ Market- Software Dispatch
- Software\ Market- View Software Market

[Report Management] 8

- Software Inventory- Refetch Software Inventory
- Software Inventory- View Software Inventory
- Software Focus List- Edit Focus List
- Software Focus List- View Focus List
- Subscription Report- Edit Subscription Report
- Subscription Report- View Subscription Report

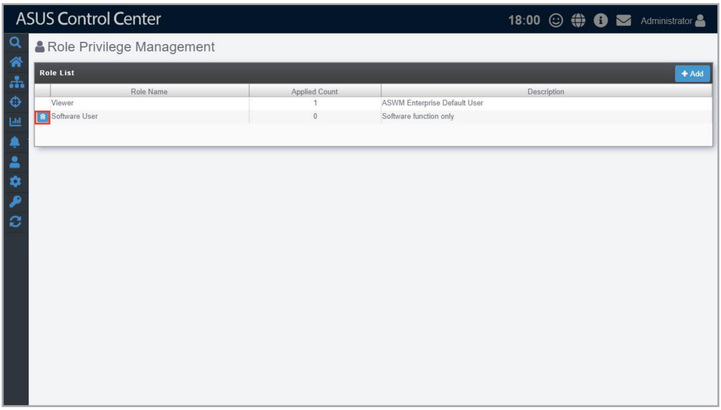
Deleting a role

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:

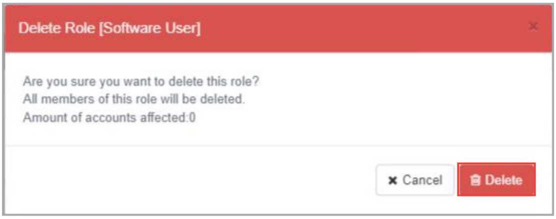
- Deleting the role from the Role List

1. Click on 🗑 next to the role you wish to delete.



	Role Name	Applied Count	Description
	Viewer	1	ASWM Enterprise Default User
🗑	Software User	0	Software function only

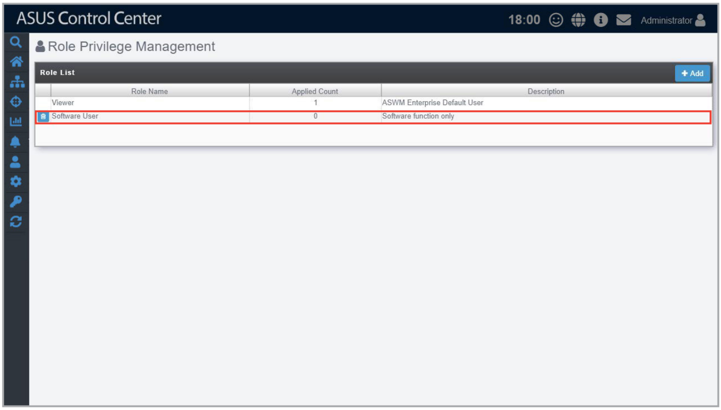
2. Click Delete to delete the role.



Are you sure you want to delete this role?
All members of this role will be deleted.
Amount of accounts affected:0

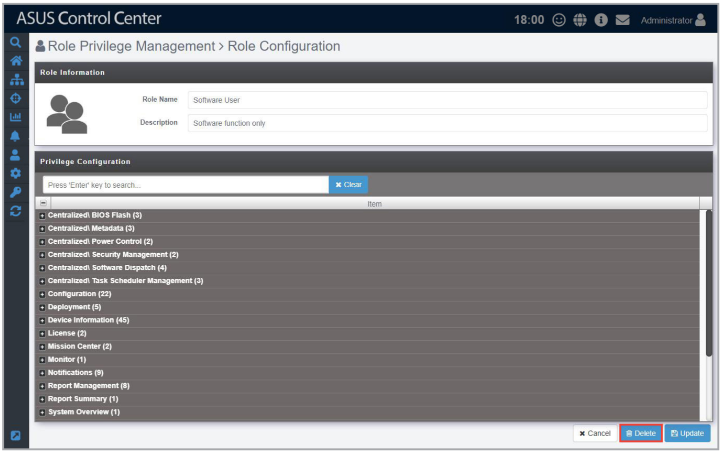
- Deleting the role from Role Configuration

  1. Click on the role you wish to delete from the **Role List** block.



Role Name	Applied Count	Description
Viewer	1	ASWM Enterprise Default User
Software User	0	Software function only

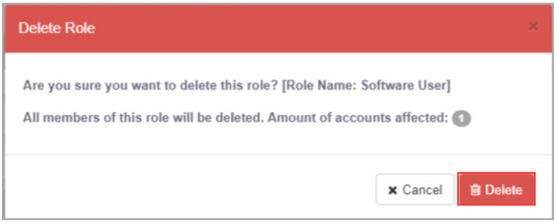
  2. Click Delete to delete the role.



Role Name: Software User

Description: Software function only

- Centralized\ BIOS Flash (3)
- Centralized\ Metadata (3)
- Centralized\ Power Control (2)
- Centralized\ Security Management (2)
- Centralized\ Software Dispatch (4)
- Centralized\ Task Scheduler Management (3)
- Configuration (22)
- Deployment (5)
- Device Information (45)
- License (2)
- Mission Center (2)
- Monitor (1)
- Notifications (9)
- Report Management (8)
- Report Summary (1)
- System Overview (1)



Are you sure you want to delete this role? [Role Name: Software User]

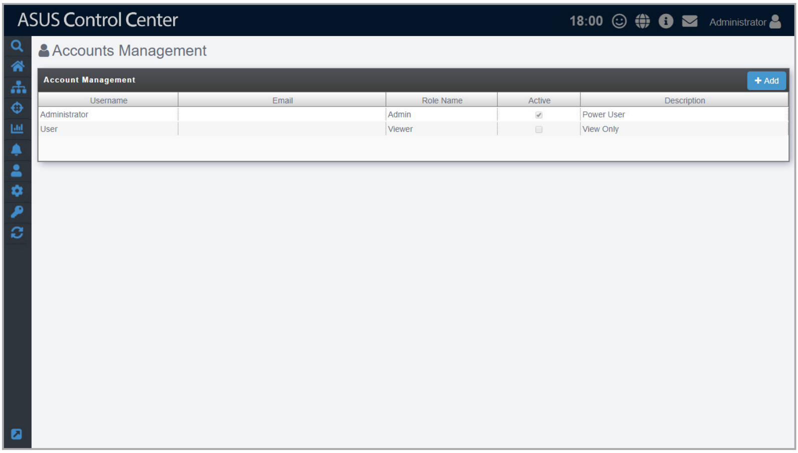
All members of this role will be deleted. Amount of accounts affected: 1

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**.



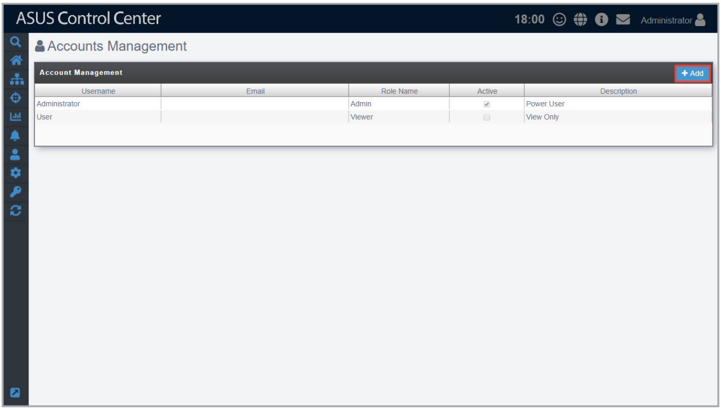
Username	Email	Role Name	Active	Description
Administrator		Admin	☑	Power User
User		Viewer	□	View Only

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.

For more details on role privileges, please refer to the **Role Privilege Management** section.

1. Click on **Add**.



Username	Email	Role Name	Active	Description
Administrator		Admin	☑	Power User
User		Viewer	□	View Only

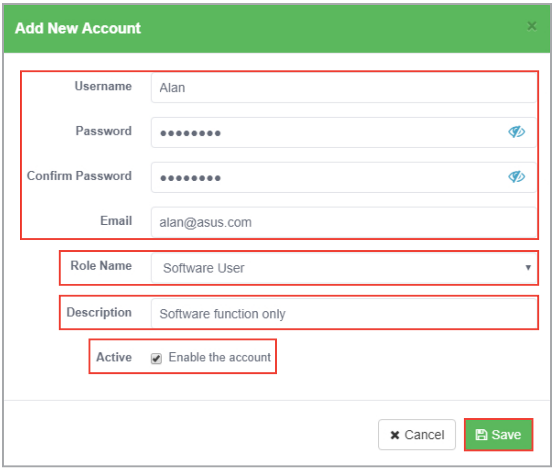
2. Enter the username, password, and email of the new account.
3. Select a role in the **Role Name** field.

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.

This option is set to enabled by default.

6. Click on **Save** once you have finished.



Add New Account

Username: Alan

Password: ••••••••

Confirm Password: ••••••••

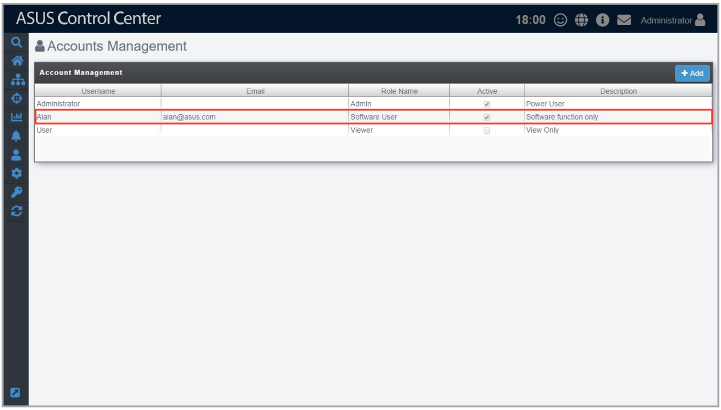
Email: alan@asus.com

Role Name: Software User ▾

Description: Software function only

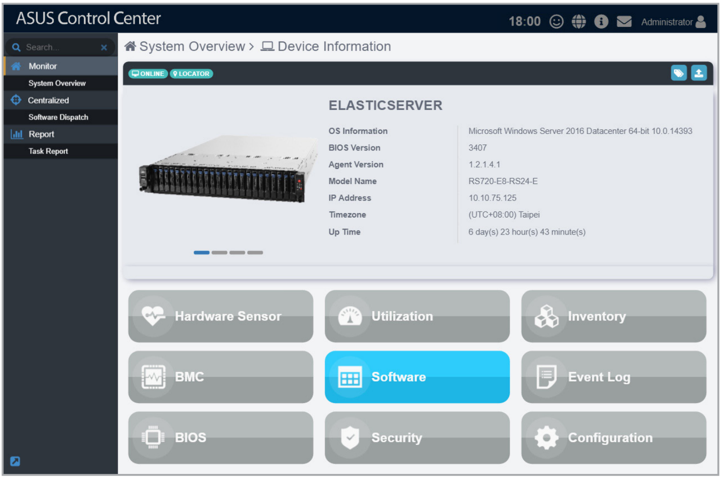
Active: ☑ Enable the account

7. Your newly created account should appear in the **Account Management** list.



Username	Email	Role Name	Active	Description
Administrator		Admin	☑	Power User
Alan	alan@asus.com	Software User	☑	Software function only
User		Viewer	□	View Only

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.

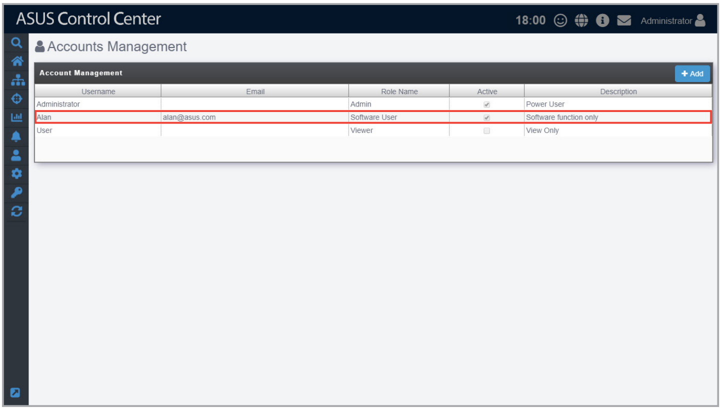


ELASTICSERVER

OS Information: Microsoft Windows Server 2016 Datacenter 64-bit 10.0.14393
BIOS Version: 3407
Agent Version: 1.2.1.4.1
Model Name: RS720-E8-RS24-E
IP Address: 10.10.75.125
Timezone: (UTC+08:00) Taipei
Up Time: 6 day(s) 23 hour(s) 43 minute(s)

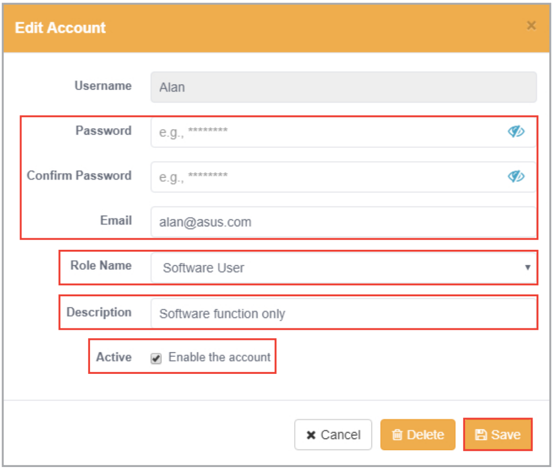
Editing an account

1. Click on the account you wish to edit.



Username	Email	Role Name	Active	Description
Administrator		Admin	☑	Power User
Alan	alan@asus.com	Software User	☑	Software function only
User		Viewer	□	View Only

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.

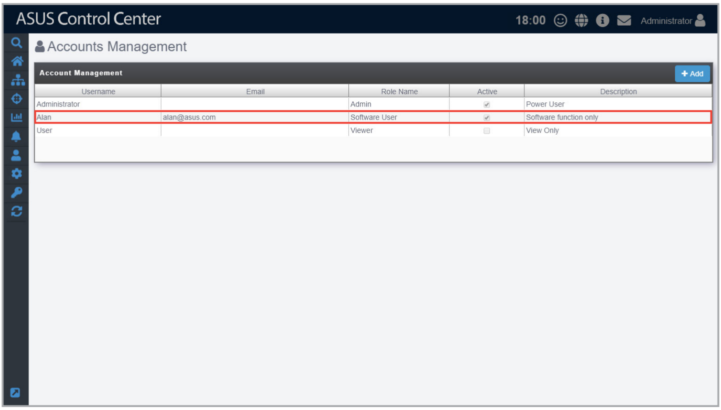


Username	Alan
Password	e.g., ********
Confirm Password	e.g., ********
Email	alan@asus.com
Role Name	Software User ▾
Description	Software function only
Active	☑ Enable the account

Deleting an account

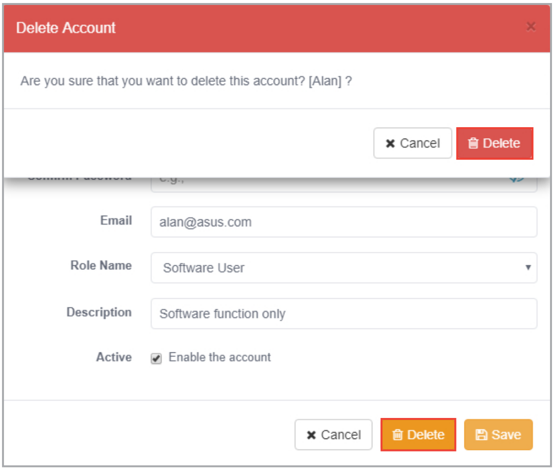
The default **Administrator** and **User** accounts cannot be deleted.

1. Click on the account you wish to delete.



Username	Email	Role Name	Active	Description
Administrator		Admin	☑	Power User
Alan	alan@asus.com	Software User	☑	Software function only
User		Viewer	□	View Only

2. Click on **Delete**, then click on **Delete** again on the confirmation pop-up to delete the account.



Are you sure that you want to delete this account? [Alan] ?

Email: alan@asus.com

Role Name: Software User

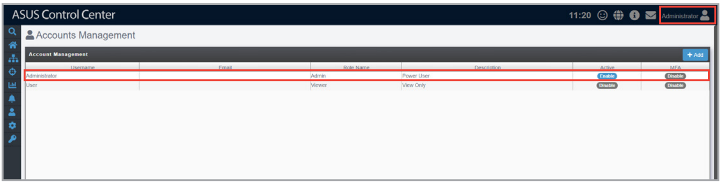
Description: Software function only

Active: ☑ Enable the account

Enabling multi-factor authentication (MFA)

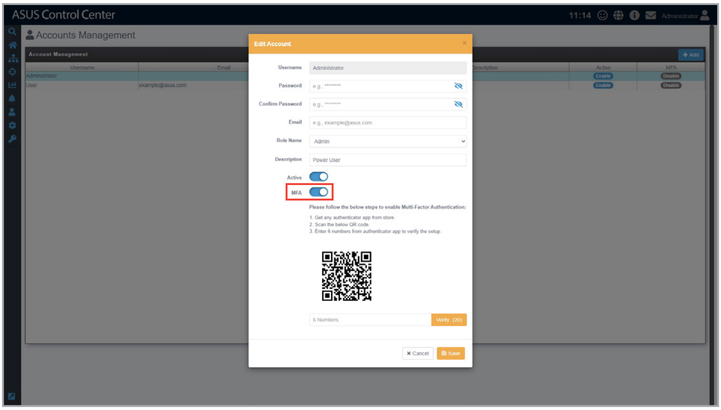
It is only possible to enable or disable MFA for currently logged in account.

1. Click on the currently logged in account.



Username	Email	Role Name	Description	Active	MFA
Administrator		Admin	Power User	Enable	Disable
User		Viewer	View Only	Disable	Disable

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.



Username: Administrator

Password: e.g., ********

Confirm Password: e.g., ********

Email: e.g., example@asus.com

Role Name: Admin

Description: Power User

Active

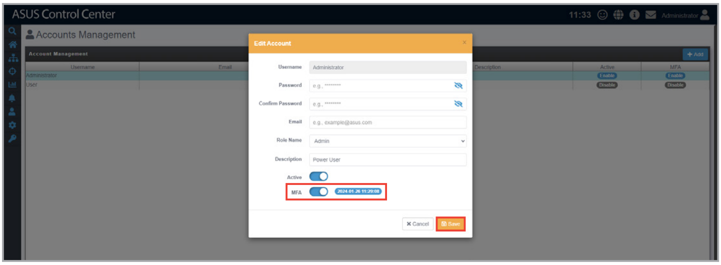
MFA

Please follow the below steps to enable Multi-Factor Authentication:

1. Get any authenticator app from store.
2. Scan the below QR code.
3. Enter 6 numbers from authenticator app to verify the setup.

6 Numbers

3. Once MFA is enabled, the MFA field will show when MFA was enabled for this account. Click **Save**.



Username: Administrator

Password: e.g., ********

Confirm Password: e.g., ********

Email: e.g., example@asus.com

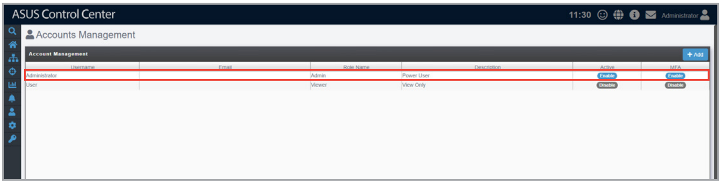
Role Name: Admin

Description: Power User

Active

MFA 2024-01-26 11:29:08

4. Click on the currently logged in account again.

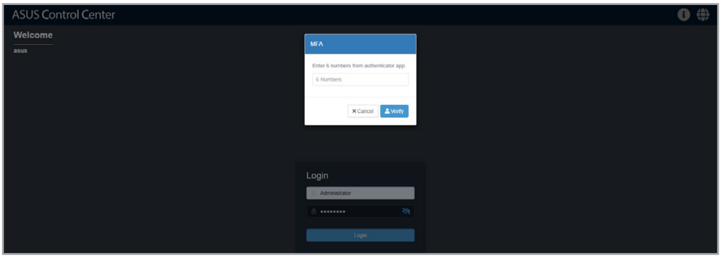


Account Management

+ Add

Username	Email	Role Name	Description	Active	MFA
Administrator		Admin	Power User	Enable	Enable
User		Viewer	View Only	Disable	Disable

5. Enter the 6-digit passcode from the authenticator app, then click **Verify**.



MFA

Enter 6 numbers from authenticator app.

6 Numbers

Login

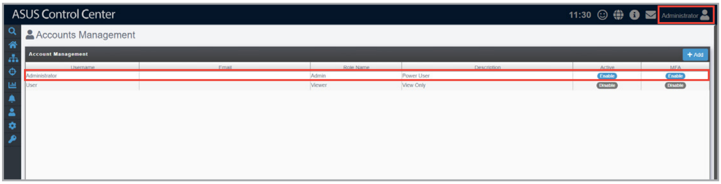
Administrator

•••••••••

Disabling multi-factor authentication (MFA)

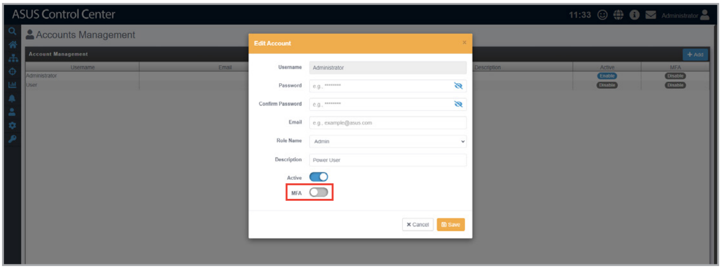
- It is only possible to enable or disable MFA for the currently logged in account.
- Only the default Administrator account can view the MFA status of other accounts.

1. Click on the currently logged in account.



Username	Email	Role Name	Description	Active	MFA
Administrator		Admin	Power User	Enable	Enable
User		Viewer	View Only	Disable	Disable

2. Disable the **MFA** option.



Username: Administrator

Password: e.g., ********

Confirm Password: e.g., ********

Email: e.g., example@asus.com

Role Name: Admin

Description: Power User

Active: ●

MFA: ○

Chapter 8

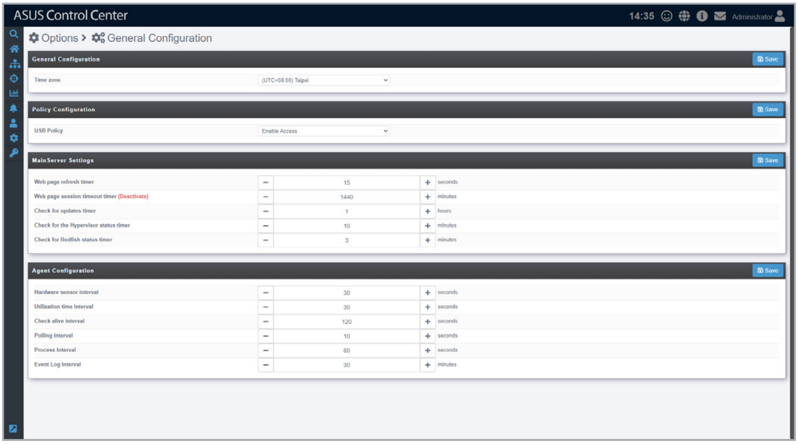
This chapter describes system, network, appearance, security, SMTP, backup and restore, maintenance, DBExpose, update, access control, sensor threshold, and software list configuration options.

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**.



General Configuration

Time zone: (UTC+08:00) Taipei

Policy Configuration

USB Policy: Enable Access

MainServer Settings

Web page refresh timer: 15 seconds

Web page session timeout timer (Deactivate): 1440 minutes

Check for updates timer: 1 hours

Check for the Hypervisor status timer: 10 minutes

Check for Redfish status timer: 3 minutes

Agent Configuration

Hardware sensor interval: 30 seconds

Utilization time interval: 30 seconds

Check alive interval: 120 seconds

Polling interval: 10 seconds

Process Interval: 60 seconds

Event Log Interval: 30 minutes

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	Adjust the time zone of the underlying Linux system the ASUS Control Center's main server is installed on. • The time zone set here should match the time zone of the system of the VM with ASUS Control Center installed. • 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.

Policy Configuration	
USB Policy	Set the default USB policy to enable or disable USB devices on new managed devices.

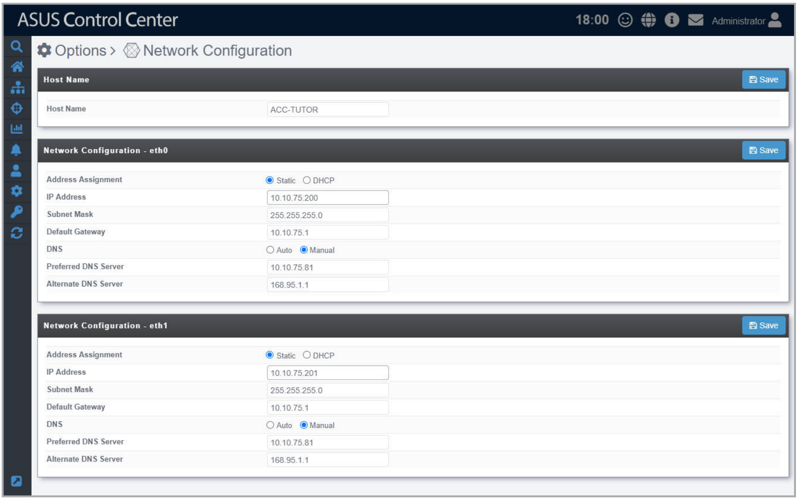
Main Server Settings	
Web page refresh timer	Set the time interval in seconds between each refresh of data on all webpages of the main server. This setting will affect the response time for items such as **System Overview** and **Event Log**.
Web page session timeout timer	Set the time interval in seconds 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.
Check for updates timer	Set the time interval in hours for the main server and agent update check. This setting will affect the main server and agent version check timer in the **Updates** page, and may require an Internet connection.
Check for the Hypervisor status timer	Set the time interval in minutes ASUS Control Center should perform a status check on managed vSpheres. This setting will affect the response times for items in the **VM Overview** page such as vSphere hardware sensors and utilization .
Check for Redfish status timer	Set the time interval in minutes ASUS Control Center should perform a status check on managed Redfish devices.

Agent Configuration	
Hardware sensor interval	Set the time interval in seconds for the agents of all managed devices to return **Hardware Sensor** values. The default setting is 30 seconds, which means that the agents need to report **Hardware Sensor** 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 **Utilization** 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. 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. 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**.



Host Name

Host Name	ACC-TUTOR

Network Configuration - eth0

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

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	The name of the ASUS Control Center main server. You will need to refer to the **Host Name** set here when manually installing Windows agents to devices.

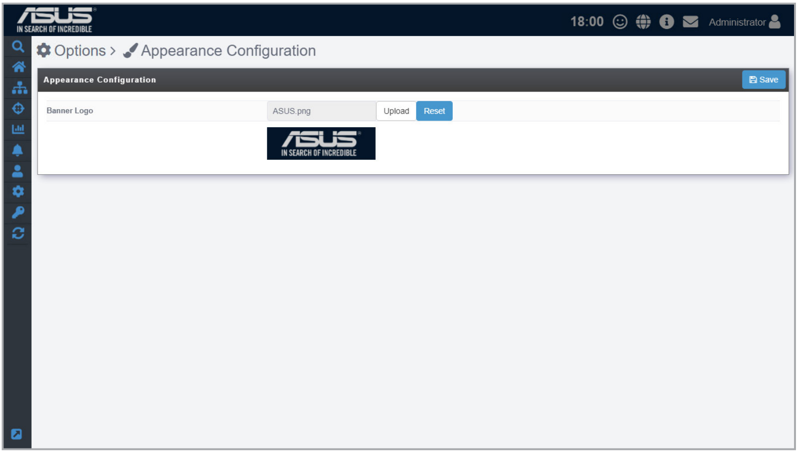
Network Configuration	
Address Assignment	Select **DHCP** to automatically set the **IP address** and **Subnet Mask**. Select **Static** to enter the **IP address** and **Subnet Mask** manually.
IP Address	Enter the IP adress for this network card. You can only set the **IP Address** manually if you selected **Static** in the **Address Assignment** field.
Subnet Mask	Enter the Subnet Mask for this network card. 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 **Auto** to automatically set the **DNS Server**, or select **Manual** to manually configure the **DNS Server**.
Preferred DNS Server	Enter the Preferred DNS Server for this network card. 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. You can only set the **Alternate DNS Server** manually if you selected **Manual** in the **DNS** field.

- 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**.

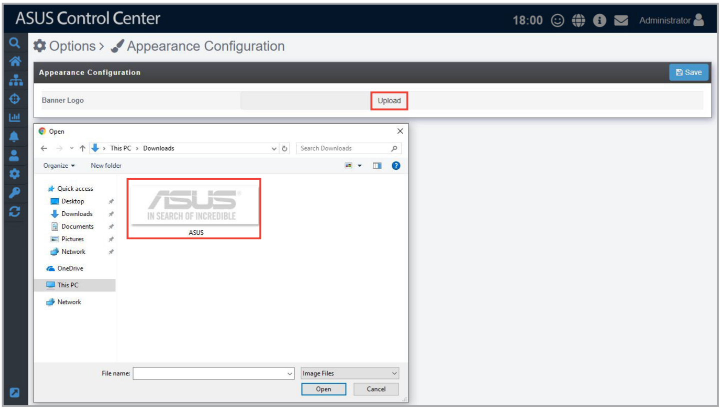


Banner Logo ASUS.png

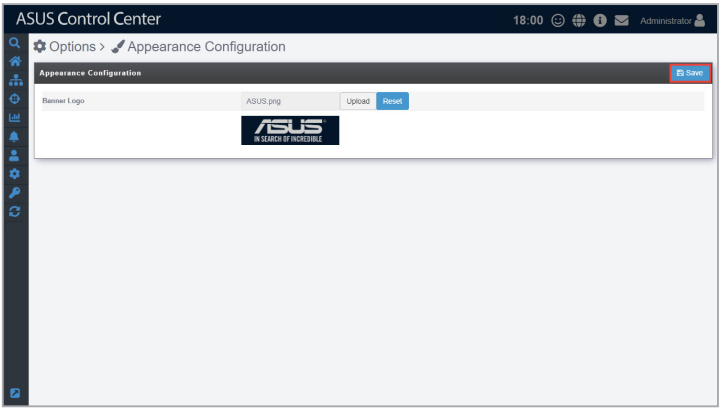
Setting a custom banner logo

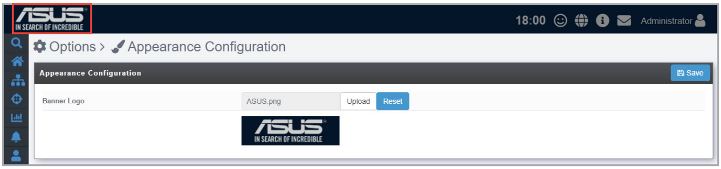
1. Click on **Upload**, then select your new banner logo.

The height dimension of the logo image file should be 56 pixels.



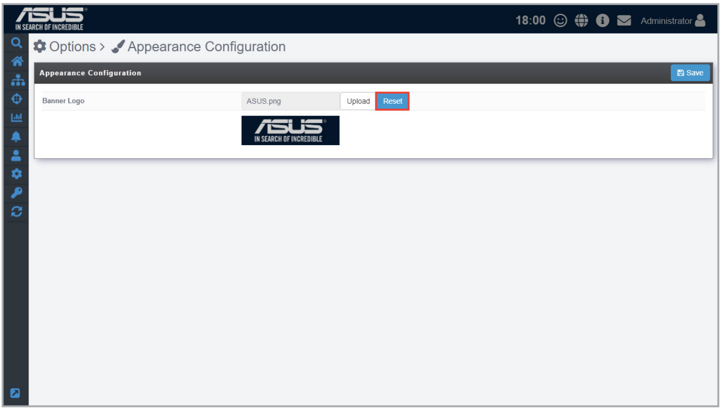
2. Once you have finished uploading the new banner logo, click on **Save**.



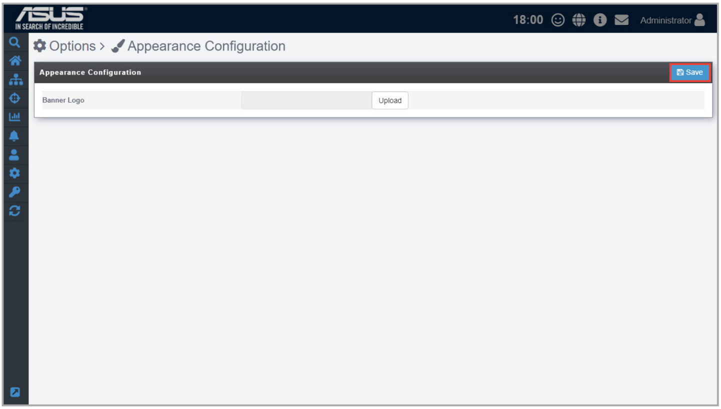


Resetting the banner logo

1. Click on **Reset** to reset your banner logo to the default banner logo.



2. Click on **Save** to save the changes made.



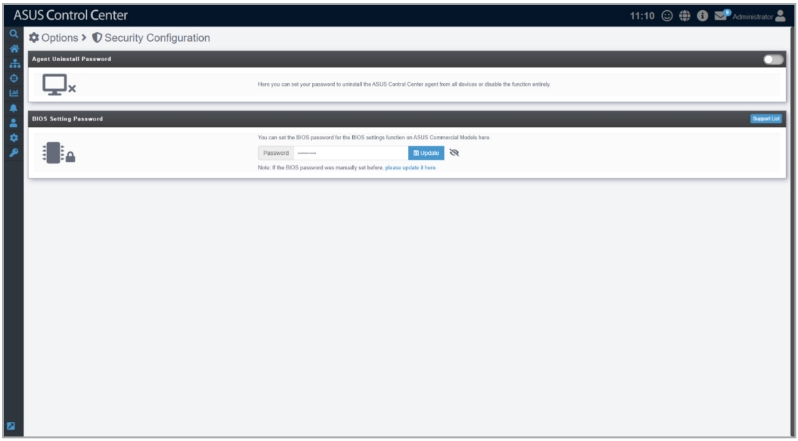
8.4 Security Configuration

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**.



Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

You can set the BIOS password for the BIOS settings function on ASUS Commercial Models here.

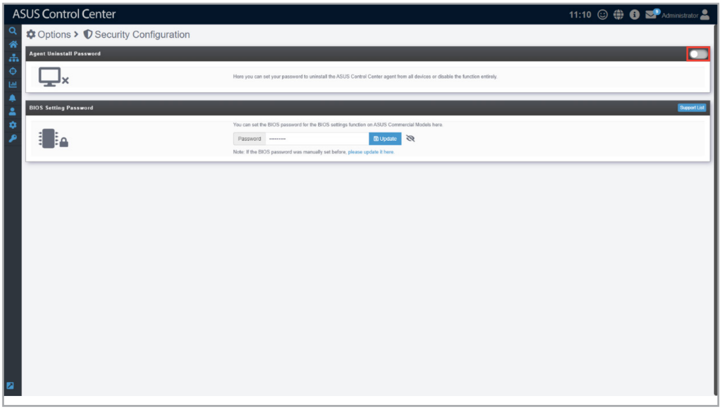
Password ·········

Note: If the BIOS password was manually set before, please update it here.

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.



Agent Uninstall Password

Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

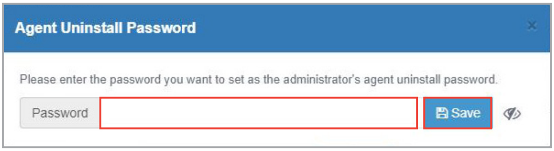
BIOS Setting Password

You can set the BIOS password for the BIOS settings function on ASUS Commercial Models here.

Password ········· Update

Note: If the BIOS password was manually set before, please update it here.

2. Enter the password you wish to set as the Administrator’s Agent Uninstall Password, then click **Save** to set the new password.



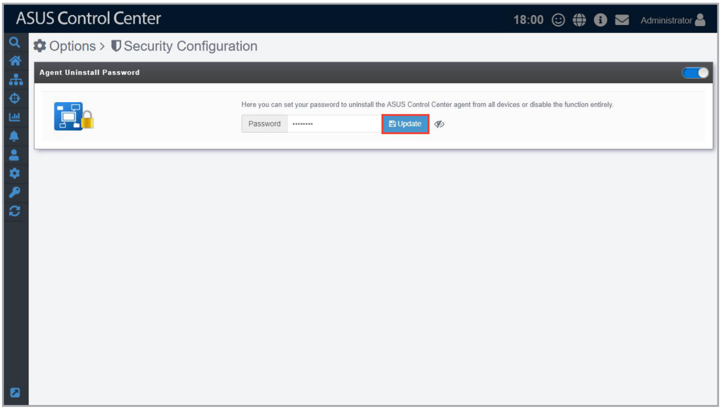
Agent Uninstall Password

Please enter the password you want to set as the administrator's agent uninstall password.

Password

Editing the password

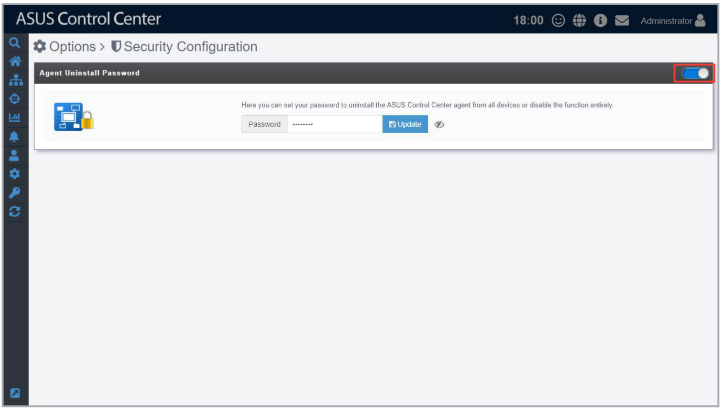
Click on the **Update** button, then re-enter your new password and click on **Save** to save your new password.



Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

Disabling the password

Click on the button located at the top right to disable the Administrator's Agent Uninstall Password.



Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

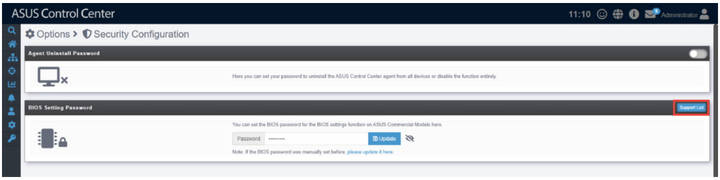
8.4.2 BIOS Setting Password

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.

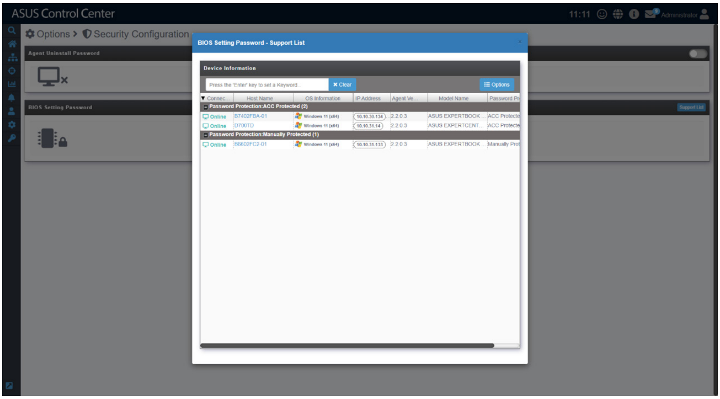


Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

You can set the BIOS password for the BIOS settings function on ASUS Commercial Models here.

Password: ••••••••

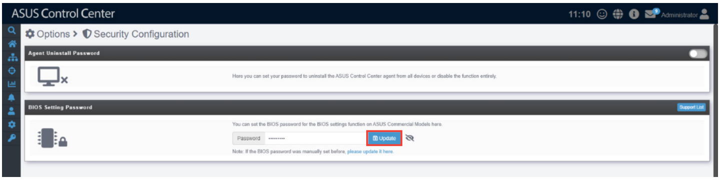
Note: If the BIOS password was manually set before, please update it here.



Connec...	Host Name	OS Information	IP Address	Agent Ve...	Model Name	Password Pr
Password Protection:ACC Protected (2)						
Online	B7402FBA-01	Windows 11 (x64)	10.10.30.134	2.2.0.3	ASUS EXPERTBOOK ...	ACC Protecte
Online	D700TD	Windows 11 (x64)	10.10.31.14	2.2.0.3	ASUS EXPERTCENT...	ACC Protecte
Password Protection:Manually Protected (1)						
Online	B6602FC2-01	Windows 11 (x64)	10.10.31.133	2.2.0.3	ASUS EXPERTBOOK ...	Manually Prot

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.

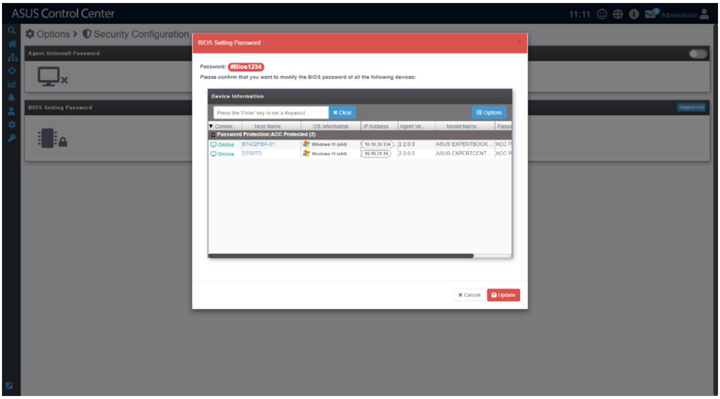


Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

You can set the BIOS password for the BIOS settings function on ASUS Commercial Models here.

Password ········· Update

Note: If the BIOS password was manually set before, please update it here.



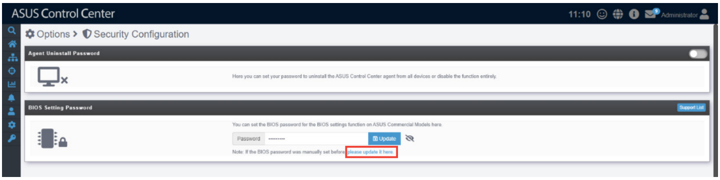
Password: #Bios1234

Please confirm that you want to modify the BIOS password of all the following devices:

Connec...	Host Name	OS Information	IP Address	Agent Ve...	Model Name	Passw
Password Protection:ACC Protected (2)						
Online	B7402FBA-01	Windows 11 (x64)	10.10.30.134	2.2.0.3	ASUS EXPERTBOOK ...	ACC P
Online	D700TD	Windows 11 (x64)	10.10.31.14	2.2.0.3	ASUS EXPERTCENT...	ACC P

Updating manually protected BIOS passwords

1. Click **Please update it here** to open a list of manually protected devices.



Here you can set your password to uninstall the ASUS Control Center agent from all devices or disable the function entirely.

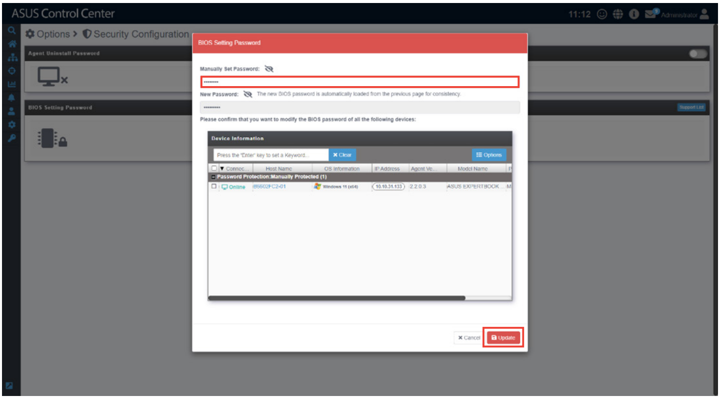
You can set the BIOS password for the BIOS settings function on ASUS Commercial Models here.

Password ••••••••• Update

Note: If the BIOS password was manually set before please update it here.

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".

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.



Manually Set Password: •••••••••

New Password: The new BIOS password is automatically loaded from the previous page for consistency.

••••••••••

Please confirm that you want to modify the BIOS password of all the following devices:

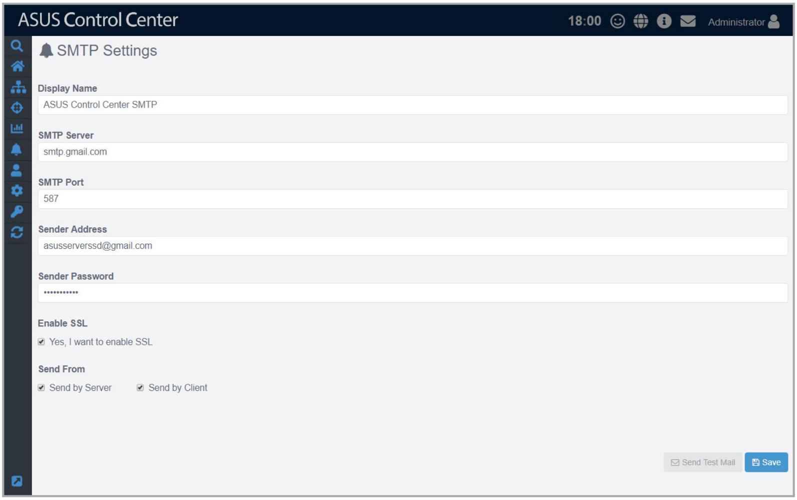
□	Connec...	Host Name	OS Information	IP Address	Agent Ve...	Model Name
Password Protection:Manually Protected (1)						
□	Online	B6602FC2-01	Windows 11 (x64)	10.10.31.133	2.2.0.3	ASUS EXPERTBOOK ...

8.5 SMTP Settings

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**.



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

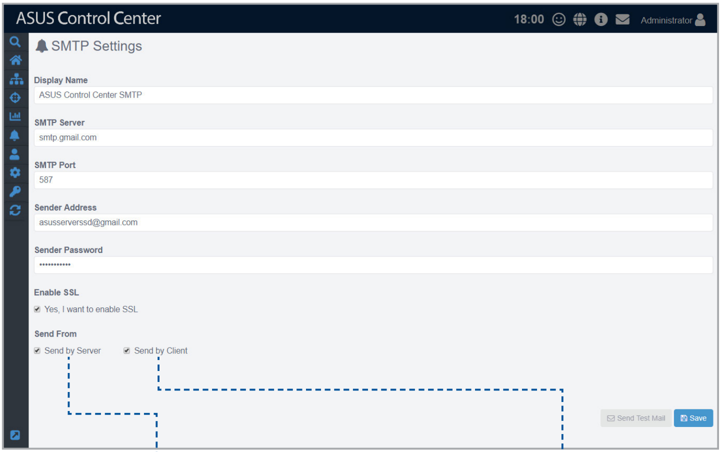
Send From
☑ Send by Server ☑ Send by Client

To set up the SMTP Server:

1. Fill in or check the following fields:

Display Name	The name of this SMTP setting. The display name will not appear on sent emails.
SMTP Server	The SMTP server responsible for collecting and sending emails
SMTP Port	Service port for SMTP. Common ports used are 25 (SMTP former default port), 465 (encrypted SMTP), and 587 (new SMTP default)
Sender Address	The email of the ACC notification sender. This email address must exist within the SMTP Server service
Sender Password	The password for the ACC notification email sender
Enable SSL	Enables mail sent or forwarded through this SMTP server are SSL encrypted
Send by Server*	When there are issues with managed devices whilst within the same domain as ACC, ACC will send emails using the SMTP server
Send by Client*	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

* **Refer to the flow charts at the bottom of the page for more details on the difference between Send by Server and Send by Client.**



SMTP Settings

Display Name
ASUS Control Center SMTP

SMTP Server
smtp.gmail.com

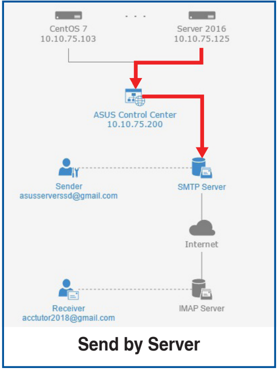
SMTP Port
587

Sender Address
asusserverssd@gmail.com

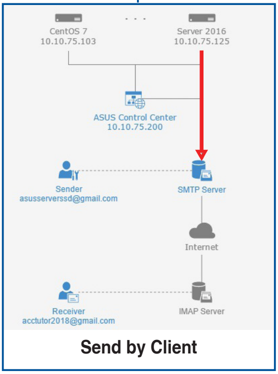
Sender Password
•••••••••••

Enable SSL
☑ Yes, I want to enable SSL

Send From
☑ Send by Server ☑ Send by Client

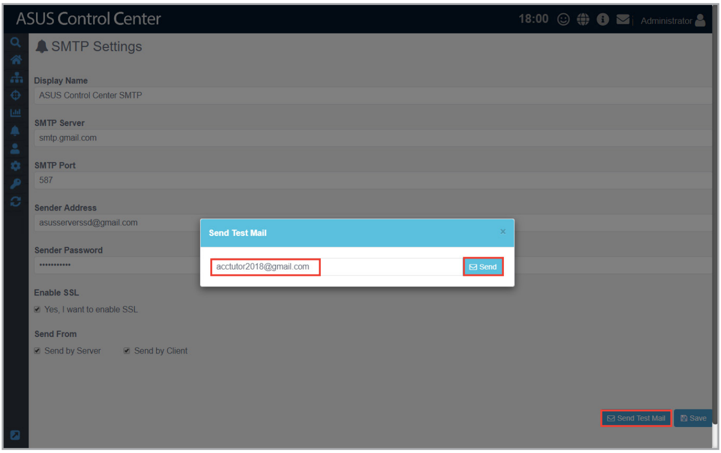


Send by Server



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.



SMTP Settings

Display Name
ASUS Control Center SMTP

SMTP Server
smtp.gmail.com

SMTP Port
587

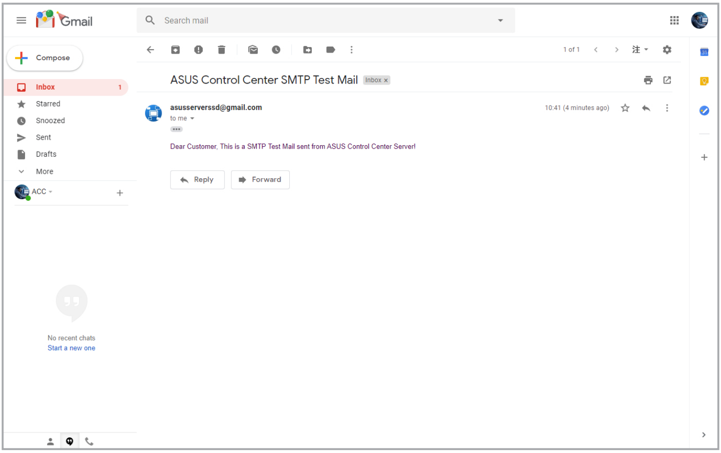
Sender Address
asusserverssd@gmail.com

Sender Password
••••••••••••

Enable SSL
☑ Yes, I want to enable SSL

Send From
☑ Send by Server ☑ Send by Client

Send Test Mail: acctutor2018@gmail.com

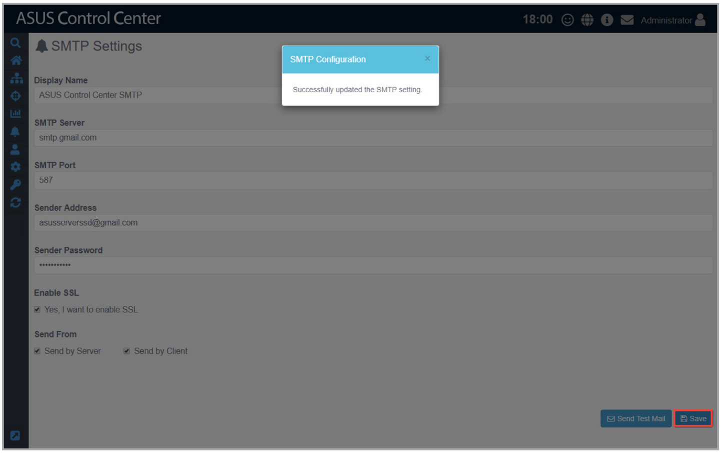


ASUS Control Center SMTP Test Mail

asusserverssd@gmail.com
to me
10:41 (4 minutes ago)

Dear Customer, This is a SMTP Test Mail sent from ASUS Control Center Server!

3. Click **Save** to save the changes made.



SMTP Settings

SMTP Configuration

Successfully updated the SMTP setting.

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

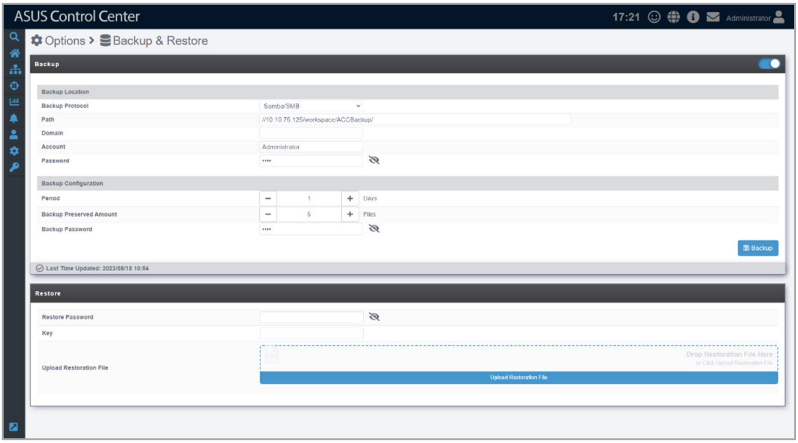
Send From
☑ Send by Server ☑ Send by Client

8.6 Backup & Restore

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**.



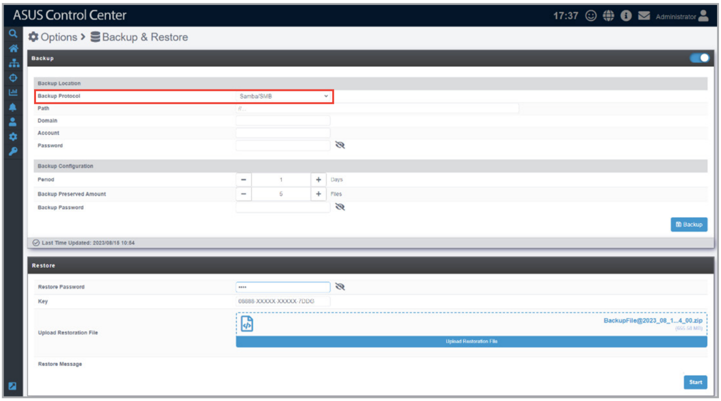
Backup Location	
Backup Protocol	Samba/SMB
Path	//10.10.75.125/workspace/ACCBackup/
Domain	
Account	Administrator
Password	••••
Backup Configuration	
Period	1 Days
Backup Preserved Amount	5 Files
Backup Password	••••

Last Time Updated: 2023/08/15 10:54

Restore Password	
Key	
Upload Restoration File	Drop Restoration File Here or Click Upload Restoration File

Enabling periodic backup

1. Select a Backup Protocol (currently only supports Samba / SMB protocols).



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: 2023/08/15 10:54

Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message

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`.

- <u>For Debian, Ubuntu</u>

  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.

- <u>Enable write permissions for the destination folder</u>

  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`.

- <u>Modify the Samba configuration file</u>

  a. Open /etc/samba/smb.conf.

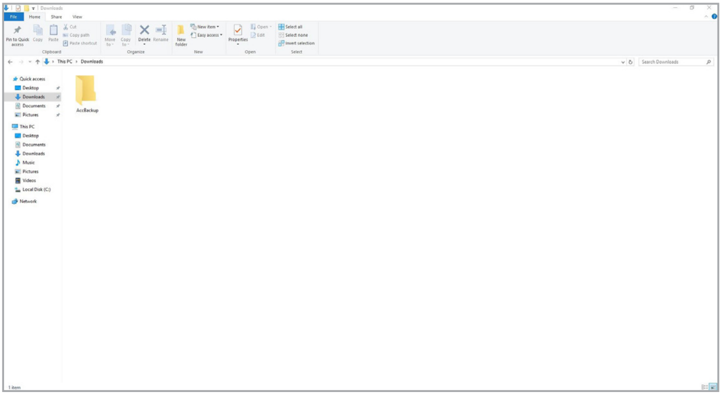
  b. Set the **security** variable in **Galbol Setting** to “user”.

  c. Set the **writable** variable in **Share Definitions** to “yes”.

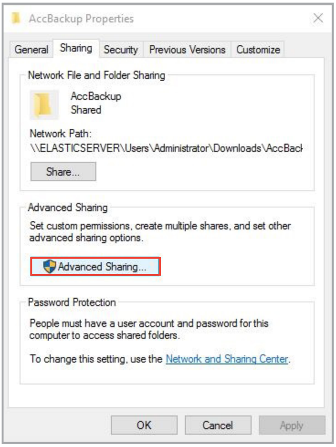
If you wish to back up your ACC to a Windows OS device’s SMB folder, do the following on the Windows OS device you wish to backup to:

- <u>Create, share, and enable permissions for the destination folder</u>

  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...**.



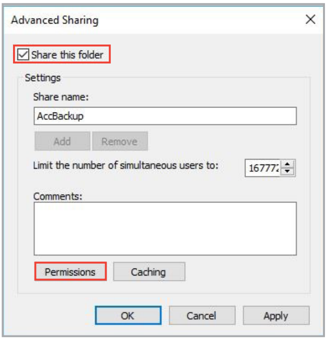
Network Path:
\\ELASTICSERVER\Users\Administrator\Downloads\AccBack

Set custom permissions, create multiple shares, and set other advanced sharing options.

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

c. Check **Share this folder**, then click on **Permissions**.

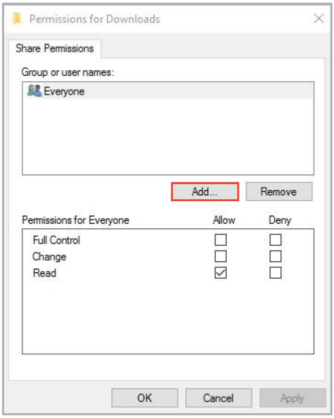


☑ Share this folder

Share name: AccBackup

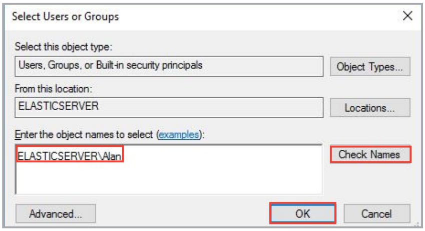
Limit the number of simultaneous users to: 16777

d. Click on **Add...**, then enter the users you would like to allow permissions for, click on **Check Names** and click **OK**.



Group or user names:
Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

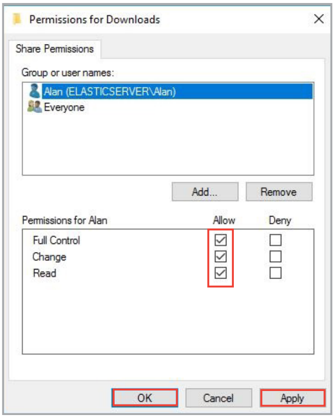


Select this object type:
Users, Groups, or Built-in security principals

From this location:
ELASTICSERVER

Enter the object names to select (examples):
ELASTICSERVER\Alan

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**.



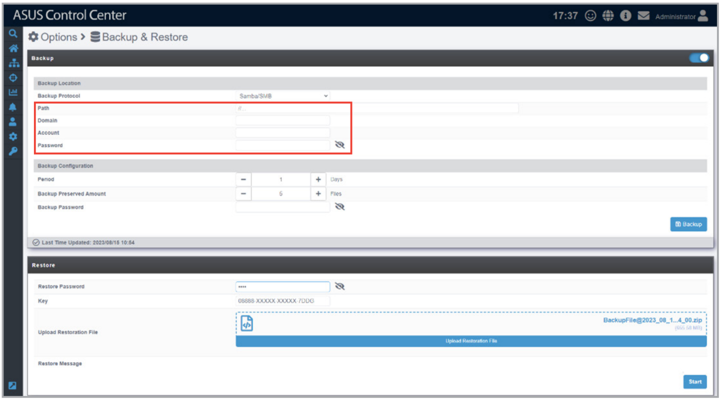
Group or user names:
Alan (ELASTICSERVER\Alan)
Everyone

Permissions for Alan	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

f. Return to your ASUS Control Center main server.

2. Fill in the **Path**, **Domain**, **Account**, and **Password** fields.

- 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.



Backup Protocol: Samba/SMB

Path: //...

Domain

Account

Password

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password

Last Time Updated: 2023/08/15 10:54

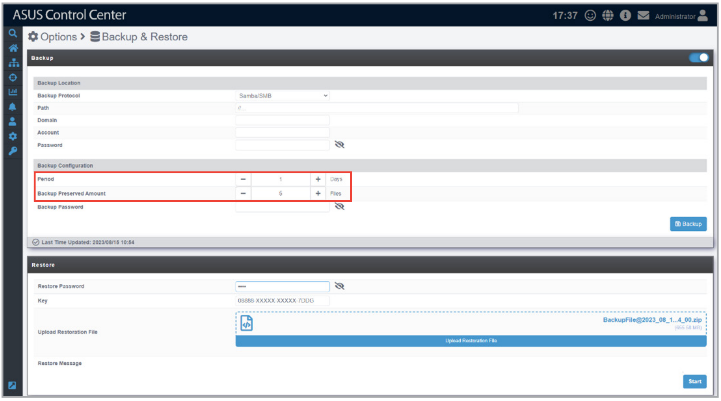
Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

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.



Backup Protocol: Samba/SMB

Path: //...

Domain

Account

Password

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password

Last Time Updated: 2023/08/15 10:54

Restore Password: ••••

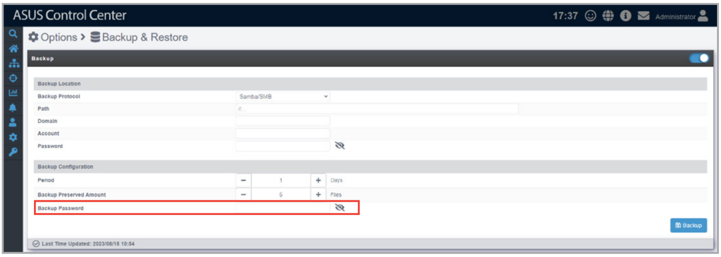
Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message

4. Enter a backup password. This password is required when you use the **Restore** function.

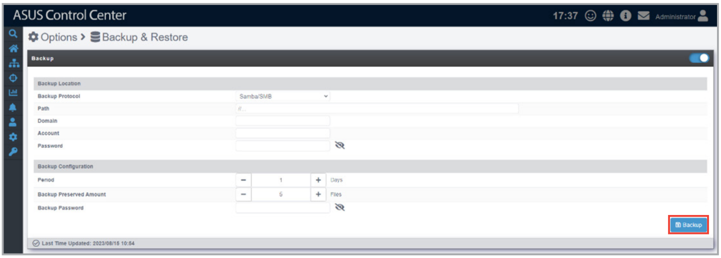
> Store the backup password in a safe place. If the backup password is lost, you will not be able to restore from the backup file.



Backup Location
Backup Protocol: Samba/SMB
Path: //...
Domain
Account
Password
Backup Configuration
Period: 1 Days
Backup Preserved Amount: 5 Files
Backup Password

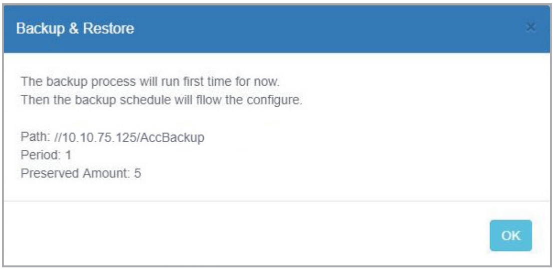
Last Time Updated: 2023/08/15 10:54

5. Click **Backup** to save the backup settings and start the initial 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: 2023/08/15 10:54



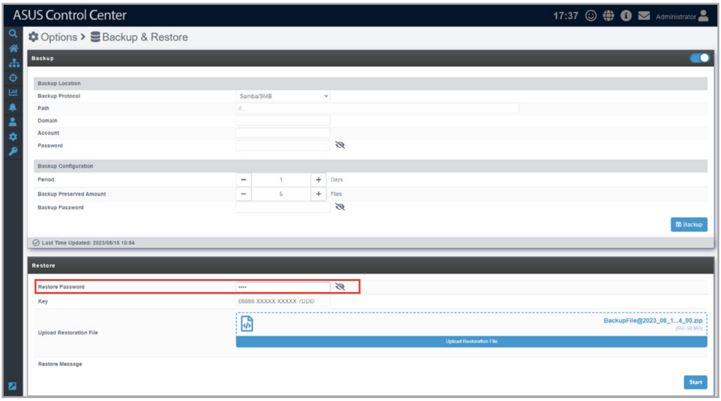
Backup & Restore

The backup process will run first time for now.
Then the backup schedule will fllow the configure.

Path: //10.10.75.125/AccBackup
Period: 1
Preserved Amount: 5

Restoring the backup file

1. Enter the **Backup Password** previously set when enabling periodic backup into the **Restore Password** field.



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: 2023/08/15 10:54

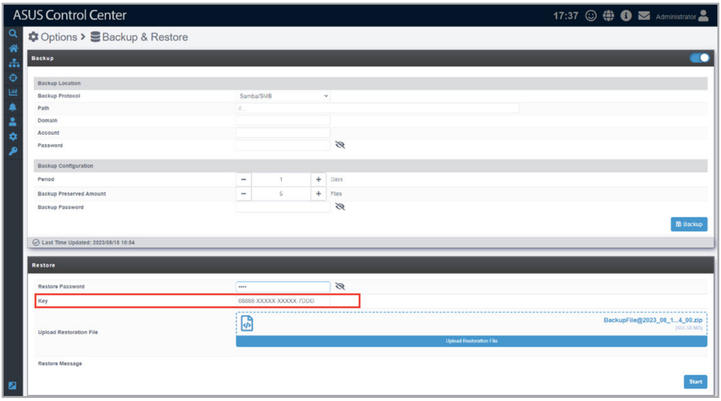
Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message

2. Enter the license key in the **Key** field.



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: 2023/08/15 10:54

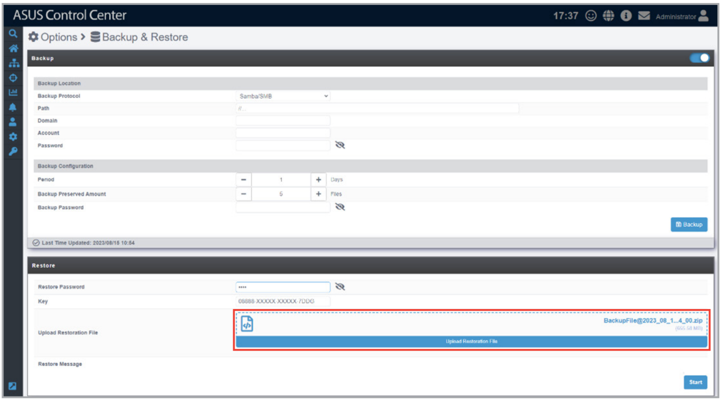
Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message

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.



Backup Protocol: Samba/SMB

Path: //...

Domain:

Account:

Password:

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/08/15 10:54

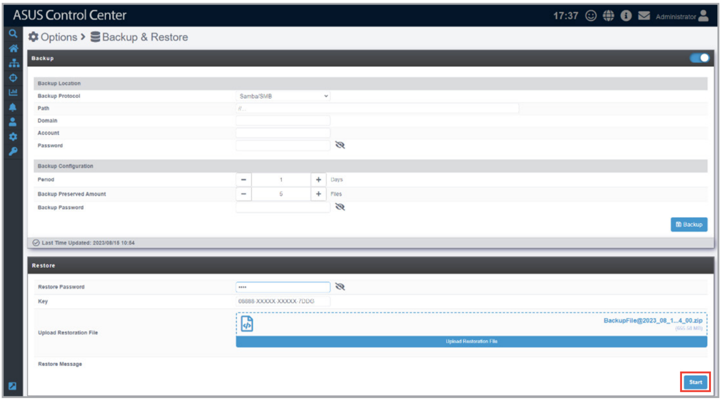
Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message:

4. Click **Start** to restore from the selected backup file.



Backup Protocol: Samba/SMB

Path: //...

Domain:

Account:

Password:

Period: 1 Days

Backup Preserved Amount: 5 Files

Backup Password:

Last Time Updated: 2023/08/15 10:54

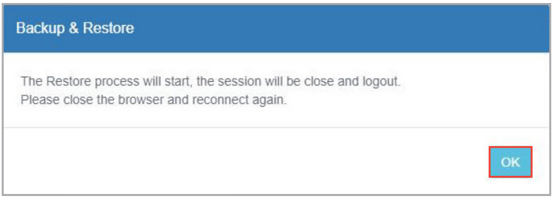
Restore Password: ••••

Key: 08888-XXXXX-XXXXX-7DDG

Upload Restoration File: BackupFile@2023_08_1...4_00.zip (655.58 MB)

Restore Message:

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.

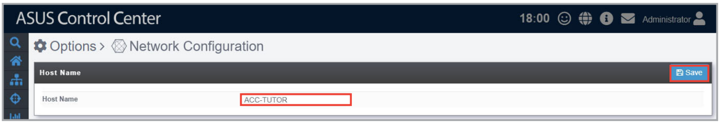


The Restore process will start, the session will be close and logout.
Please close the browser and reconnect again.

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**.

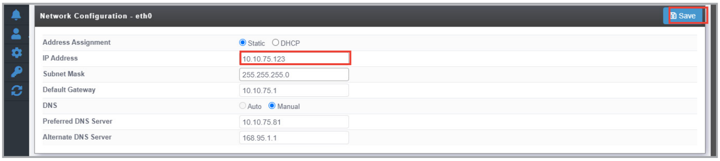
   For example, if the backed up ACC's host name was ACC TUTOR, then after restoring it to an ACC main server with the host name ACC NWONE, change the host name ACC NWONE to ACC TUTOR.



Host Name: 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.

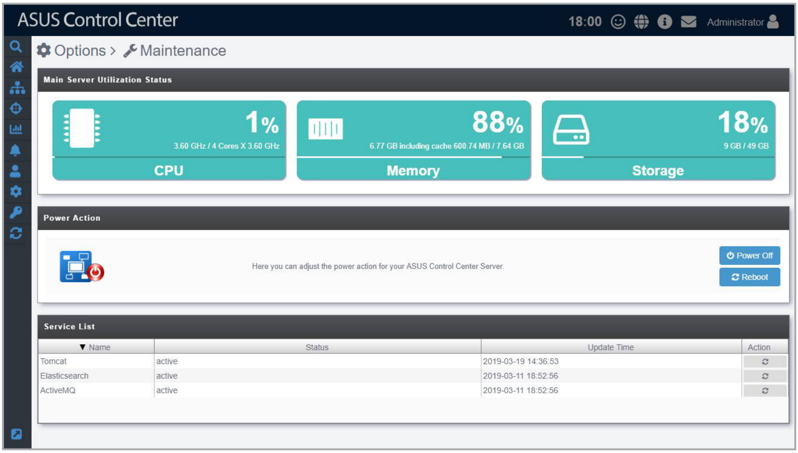


Address Assignment	● Static ○ DHCP
IP Address	10.10.75.123
Subnet Mask	255.255.255.0
Default Gateway	10.10.75.1
DNS	○ Auto ● Manual
Preferred DNS Server	10.10.75.81
Alternate DNS Server	168.95.1.1

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**.

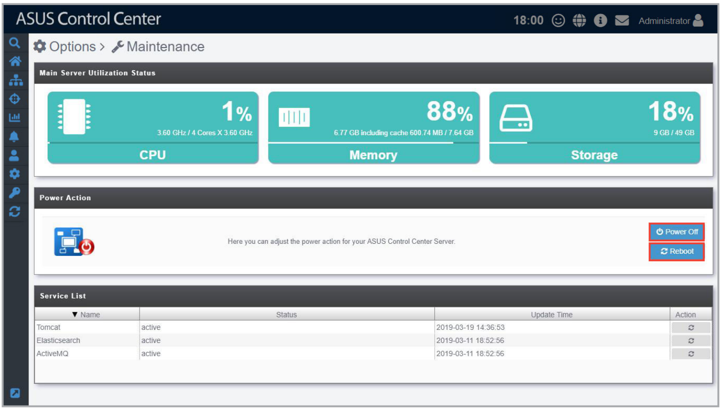


Here you can adjust the power action for your ASUS Control Center Server.

▼ Name	Status	Update Time	Action
Tomcat	active	2019-03-19 14:36:53	⟳
Elasticsearch	active	2019-03-11 18:52:56	⟳
ActiveMQ	active	2019-03-11 18:52:56	⟳

Cofiguring the power option of Hypervisors

1. Click on **Power Off** or **Reboot** to power off or reboot the hypervisor.

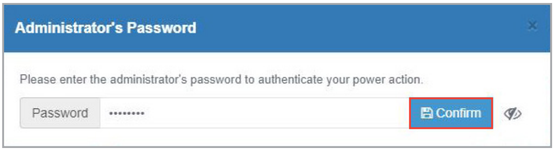


Here you can adjust the power action for your ASUS Control Center Server.

▼ Name	Status	Update Time	Action
Tomcat	active	2019-03-19 14:36:53	⟳
Elasticsearch	active	2019-03-11 18:52:56	⟳
ActiveMQ	active	2019-03-11 18:52:56	⟳

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.

For more information on Accounts and Roles, please refer to the **Account Management** chapter.



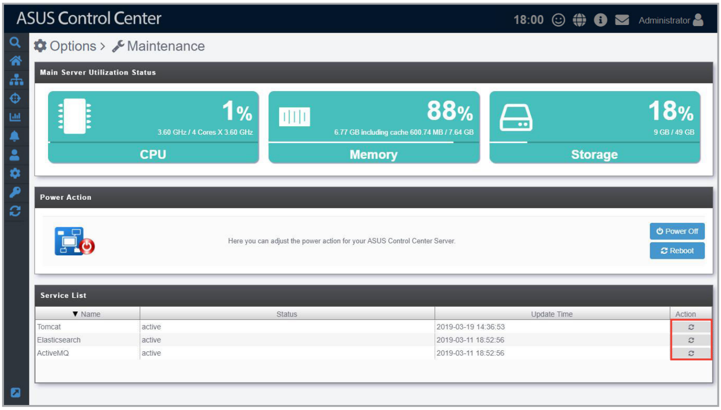
Administrator's Password

Please enter the administrator's password to authenticate your power action.

Password ••••••••

Restarting the Services

Click on the restart button next to the service you wish to restart.



Main Server Utilization Status

CPU 1% 3.60 GHz / 4 Cores X 3.60 GHz

Memory 88% 6.77 GB including cache 600.74 MB / 7.64 GB

Storage 18% 9 GB / 49 GB

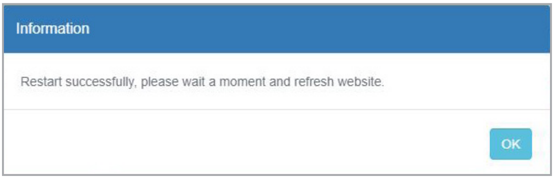
Power Action

Here you can adjust the power action for your ASUS Control Center Server.

Service List

▼ Name	Status	Update Time	Action
Tomcat	active	2019-03-19 14:36:53	
Elasticsearch	active	2019-03-11 18:52:56	
ActiveMQ	active	2019-03-11 18:52:56	

This will end your session and you will be logged out of ASUS Control Center. Please login again once the restoration is complete.



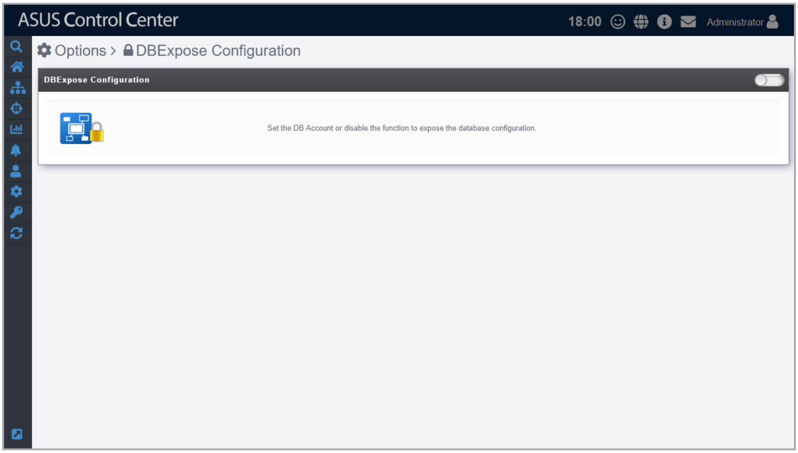
Information

Restart successfully, please wait a moment and refresh website.

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.

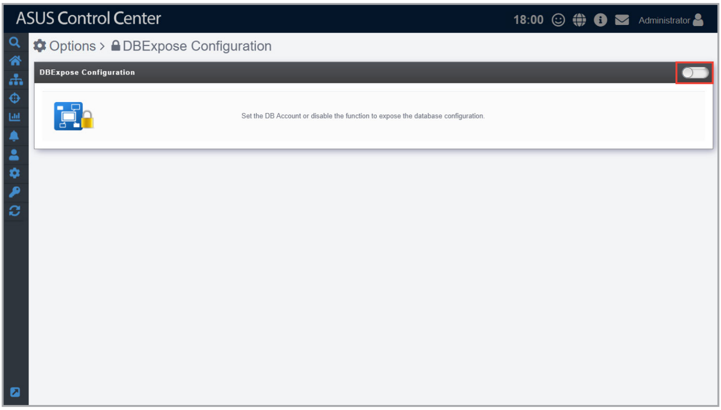
To access **DBExpose Configuration**, click ⚙ in the left menu, then click on **DBExpose Configuration**.



Set the DB Account or disable the function to expose the database configuration.

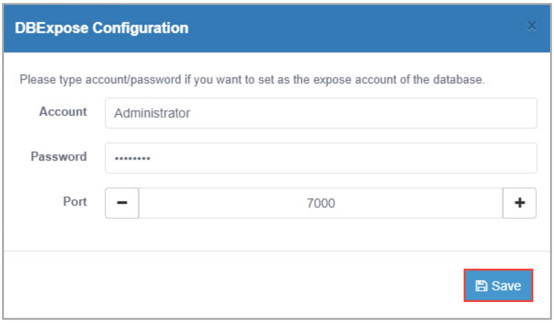
To set the DBExpose account and password

1. Click on the slide button on the top right of the main screen.



Set the DB Account or disable the function to expose the database configuration.

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**.



DBExpose Configuration

Please type account/password if you want to set as the expose account of the database.

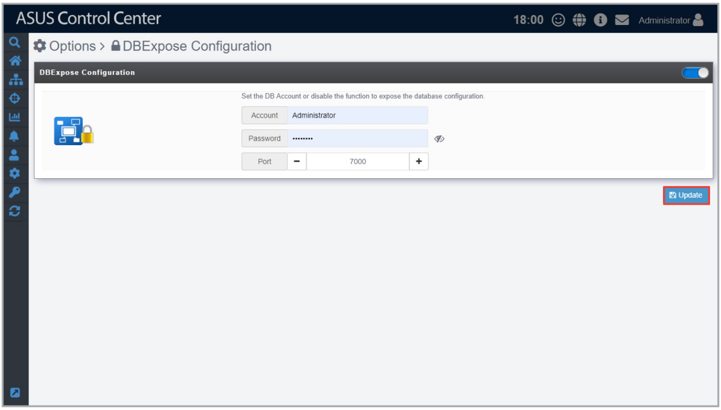
Account: Administrator

Password: ••••••••

Port: 7000

To edit the DBExpose account information

Edit the account, password, and port information then click on **Update** to save the changes made.

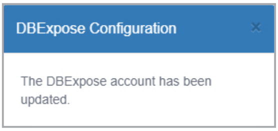


Set the DB Account or disable the function to expose the database configuration.

Account: Administrator

Password: ••••••••

Port: 7000

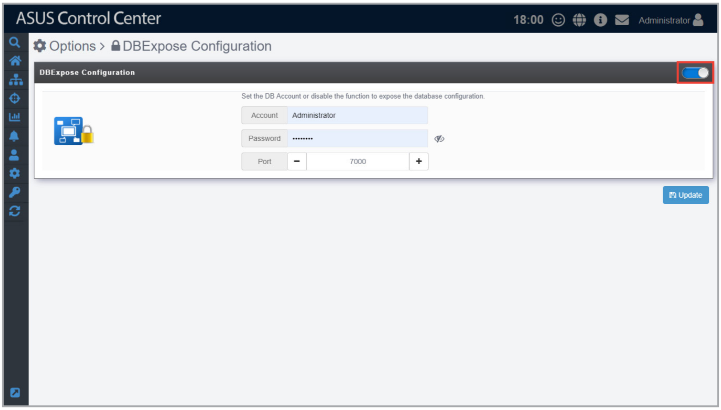


DBExpose Configuration

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.

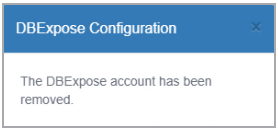


Set the DB Account or disable the function to expose the database configuration.

Account: Administrator

Password: ••••••••

Port: 7000



DBExpose Configuration

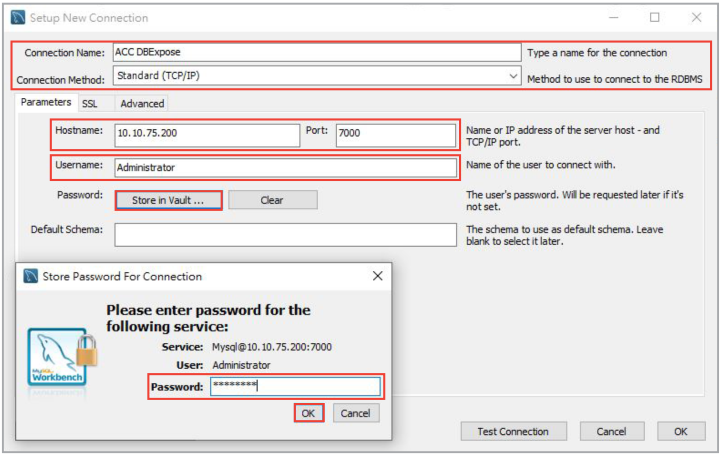
The DBExpose account has been removed.

Access ASUS Control Center with third-party software

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**.



Setup New Connection

Connection Name: ACC DBExpose — Type a name for the connection

Connection Method: Standard (TCP/IP) — Method to use to connect to the RDBMS

Hostname: 10.10.75.200 Port: 7000 — Name or IP address of the server host - and TCP/IP port.

Username: Administrator — Name of the user to connect with.

Password: — The user's password. Will be requested later if it's not set.

Default Schema: — The schema to use as default schema. Leave blank to select it later.

Store Password For Connection

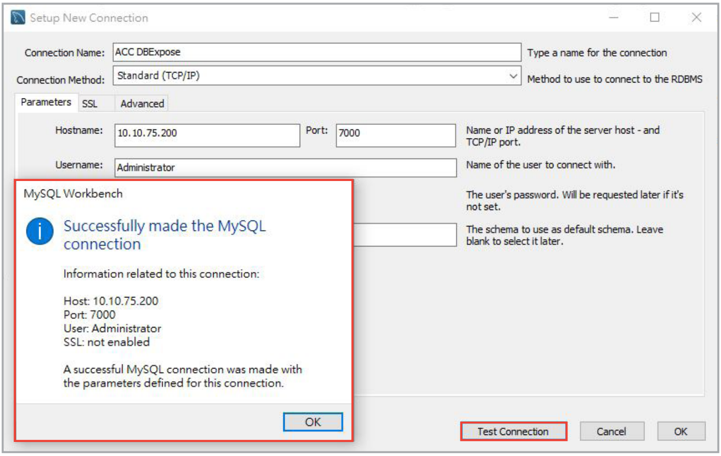
Please enter password for the following service:

Service: Mysql@10.10.75.200:7000

User: Administrator

Password: ********

5. Click on **Test Connection** to test if the connection to ASUS Control Center was successfully created.



Setup New Connection

Connection Name: ACC DBExpose — Type a name for the connection

Connection Method: Standard (TCP/IP) — Method to use to connect to the RDBMS

Hostname: 10.10.75.200 Port: 7000 — Name or IP address of the server host - and TCP/IP port.

Username: Administrator — Name of the user to connect with.

The user's password. Will be requested later if it's not set.

The schema to use as default schema. Leave blank to select it later.

MySQL Workbench

Successfully made the MySQL connection

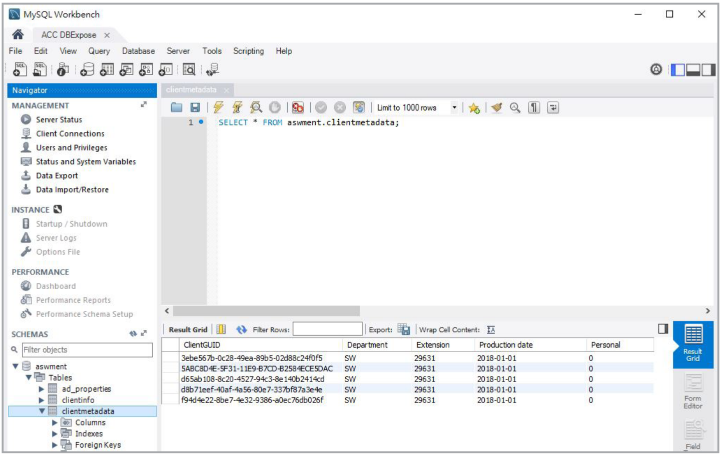
Information related to this connection:

Host: 10.10.75.200
Port: 7000
User: Administrator
SSL: not enabled

A successful MySQL connection was made with the parameters defined for this connection.

6. Save the connection settings, now when using MySQL Workbench, you should be able to access some of the data on ASUS Control Center.

The screenshot below is an example of accessing the metadata of ASUS Control Center.



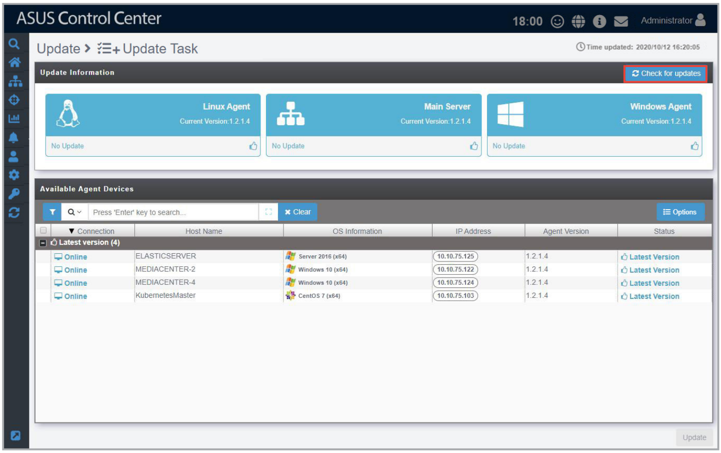
```
SELECT * FROM aswment.clientmetadata;
```

ClientGUID	Department	Extension	Production date	Personal
3ebe567b-0c28-49ea-89b5-02d88c24f0f5	SW	29631	2018-01-01	0
5ABC8D4E-5F31-11E9-B7CD-B2584ECE5DAC	SW	29631	2018-01-01	0
d65ab108-8c20-4527-94c3-8e140b2414cd	SW	29631	2018-01-01	0
d8b71eef-40af-4a56-80e7-337bf87a3e4e	SW	29631	2018-01-01	0
f94d4e22-8be7-4e32-9386-a0ec76db026f	SW	29631	2018-01-01	0

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**.

- Ensure to add *asuscontrolcenter.asus.com/** to your firewall exceptions list to enable update checks.
- Ensure you have a stable Internet connection.



Linux Agent
Current Version:1.2.1.4
No Update

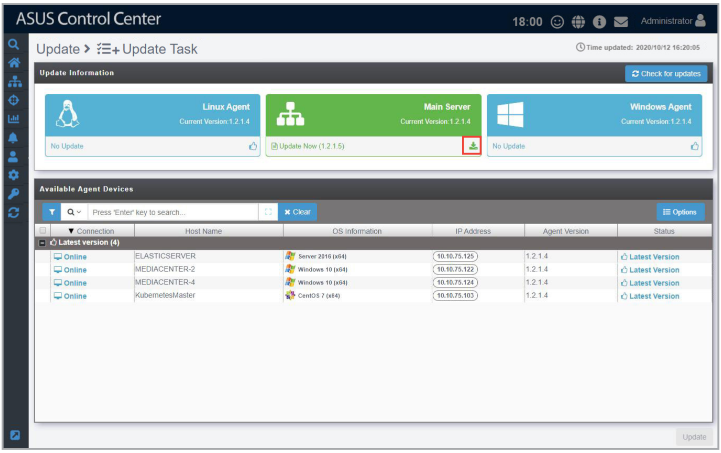
Main Server
Current Version:1.2.1.4
No Update

Windows Agent
Current Version:1.2.1.4
No Update

□	▼ Connection	Host Name	OS Information	IP Address	Agent Version	Status
	Latest version (4)					
	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	1.2.1.4	Latest Version
	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	1.2.1.4	Latest Version
	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	1.2.1.4	Latest Version
	Online	KubernetesMaster	CentOS 7 (x64)	10.10.75.103	1.2.1.4	Latest Version

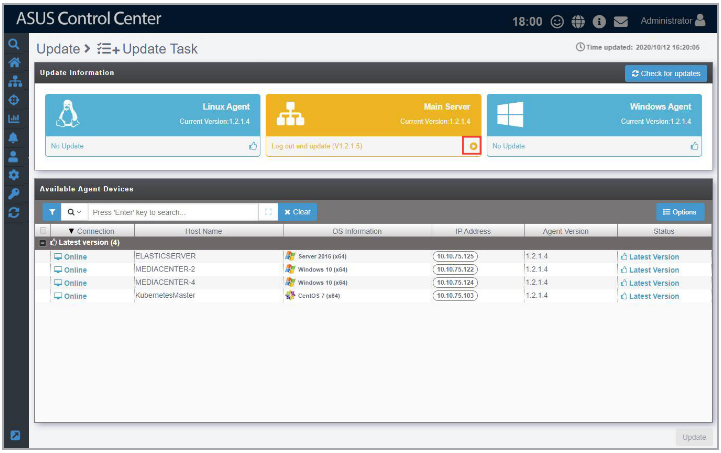
Updating ASUS Control Center main server

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.



Connection	Host Name	OS Information	IP Address	Agent Version	Status
Latest version (4)					
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	1.2.1.4	Latest Version
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	1.2.1.4	Latest Version
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	1.2.1.4	Latest Version
Online	KubernetesMaster	CentOS 7 (x64)	10.10.75.103	1.2.1.4	Latest Version

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.



Connection	Host Name	OS Information	IP Address	Agent Version	Status
Latest version (4)					
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	1.2.1.4	Latest Version
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	1.2.1.4	Latest Version
Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	1.2.1.4	Latest Version
Online	KubernetesMaster	CentOS 7 (x64)	10.10.75.103	1.2.1.4	Latest Version

3. Log into ASUS Control Center again after the update is completed.

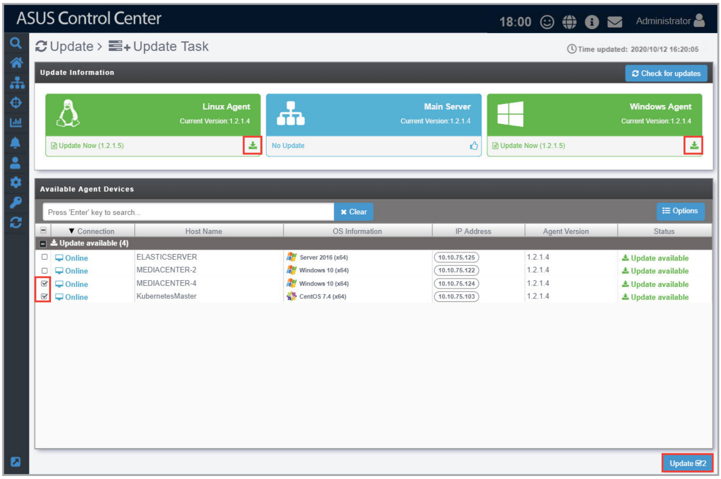
Updating Windows and Linux agents

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.

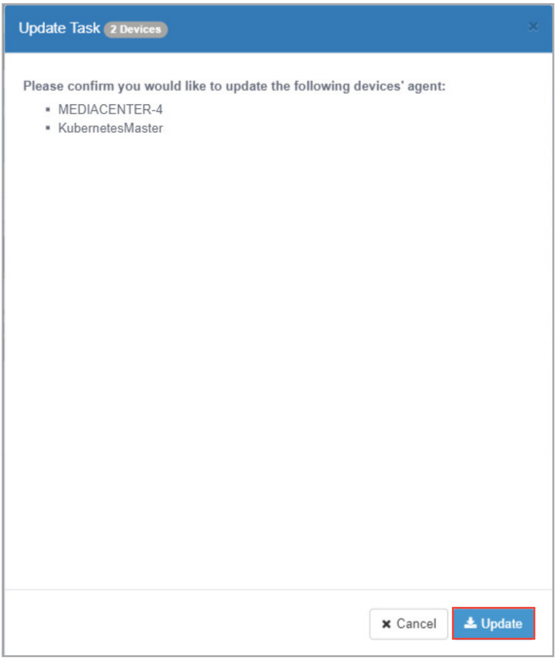
4. Click on **Update**.



⊟	▼ Connection	Host Name	OS Information	IP Address	Agent Version	Status
⊟	Update available (4)					
□	Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	1.2.1.4	Update available
□	Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	1.2.1.4	Update available
☑	Online	MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	1.2.1.4	Update available
☑	Online	KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103	1.2.1.4	Update available

5. Click **Update** on the confirmation pop-up window to start the update process.

You do not need to uninstall the agents on the selected devices before updating.

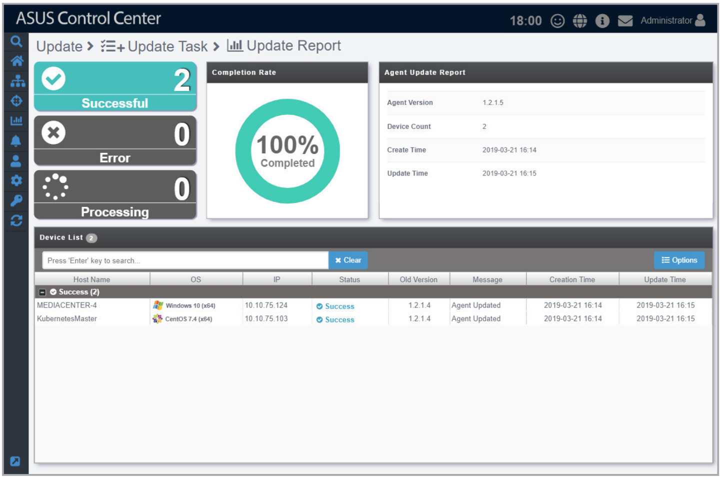


Please confirm you would like to update the following devices' agent:

- MEDIACENTER-4
- KubernetesMaster

6. After the agent updates have been completed, you will be redirected to the Agent Update Report screen.

For more details on the Agent Update Report, refer to the **Agent Update Report** section.



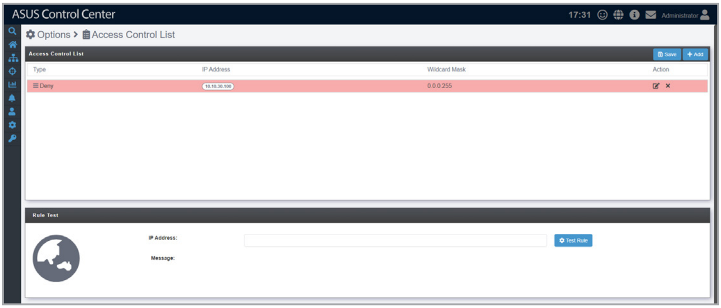
Agent Update Report

Agent Version	1.2.1.5
Device Count	2
Create Time	2019-03-21 16:14
Update Time	2019-03-21 16:15

Host Name	OS	IP	Status	Old Version	Message	Creation Time	Update Time
⊟ Success (2)							
MEDIACENTER-4	Windows 10 (x64)	10.10.75.124	Success	1.2.1.4	Agent Updated	2019-03-21 16:14	2019-03-21 16:15
KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103	Success	1.2.1.4	Agent Updated	2019-03-21 16:14	2019-03-21 16:15

8.10 Access Control List

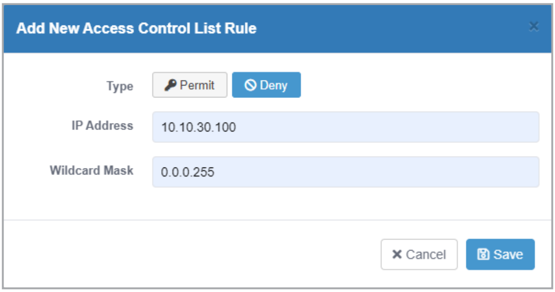
The **Access Control List** allows you to configure rules to permit or deny access to ASUS Control Center from specified IP addresses.



Type	IP Address	Wildcard Mask	Action
Deny	10.10.30.100	0.0.0.255	

IP Address:

Message:



Type: 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**.

- 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.

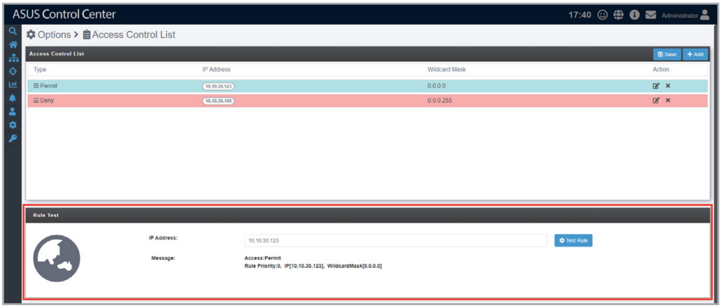
To adjust the priority of an access control rule

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.

> 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.



Access Control List

Type	IP Address	Wildcard Mask	Action
☰ Permit	10.10.30.123	0.0.0.0	✎ ✕
☰ Deny	10.10.30.100	0.0.0.255	✎ ✕

Rule Test

IP Address: 10.10.30.123

Message: Access:Permit
Rule Priority:0, IP[10.10.30.123], WildcardMask[0.0.0.0]

To edit an access control rule

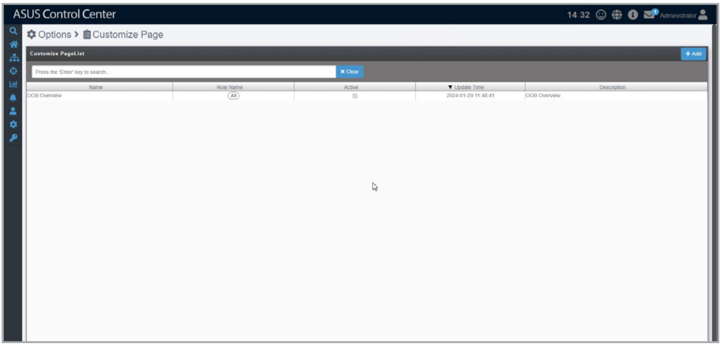
1. Click ✎ to start editing a new access control rule.
2. After making the desired changes, click Save to save the access control rule, then click **OK** in the popup window to confirm your changes.

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

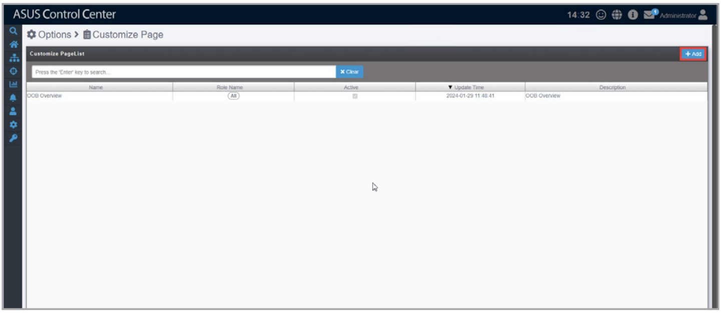
Customize Page allows you to create and edit custom pages.



Name	Role Name	Active	▼ Update Time	Description
OOB Overview	All	☑	2024-01-29 11:48:41	OOB Overview

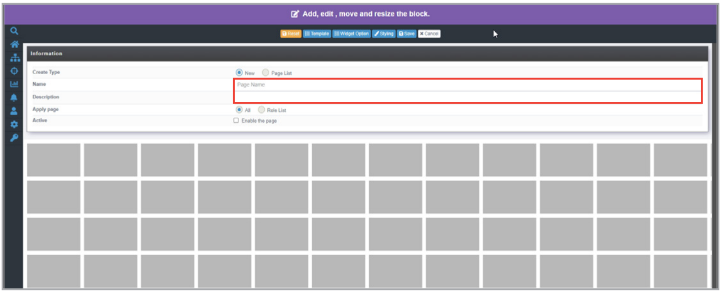
Adding a blank custom page

1. Click **Add** to open the custom page editor and create a blank custom page.



Name	Role Name	Active	▼ Update Time	Description
OOB Overview	All	☑	2024-01-29 11:48:41	OOB Overview

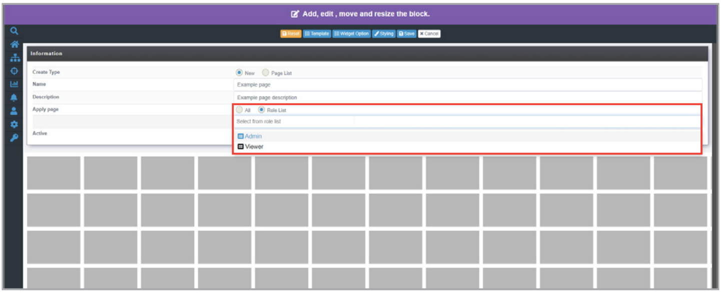
2. Fill in the **Name** and **Description** fields.



Information

Create Type	● New ○ Page List
Name	Page Name
Description	
Apply page	● All ○ Role List
Active	□ Enable the page

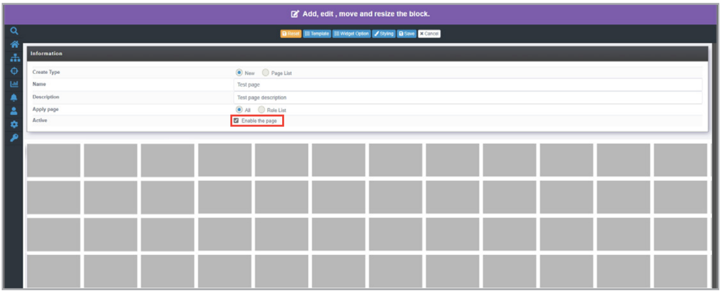
3. Select the **Role List** option in the **Apply page** field, then select a role from the drop down menu to specify which roles should have access to the custom page (optional).



Information

Create Type	● New ○ Page List
Name	Example page
Description	Example page description
Apply page	○ All ● Role List Select from role list Admin Viewer
Active	

4. Tick **Enable this page** to enable the custom page.

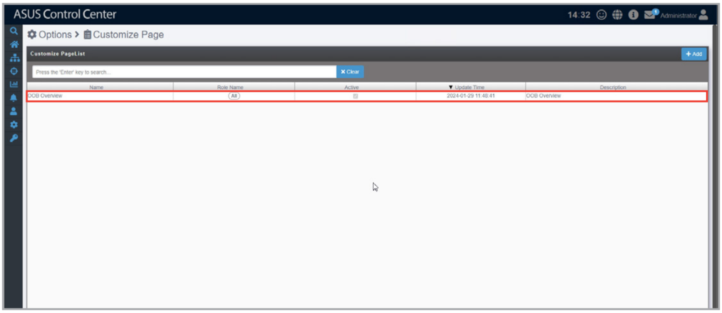


Information

Create Type	● New ○ Page List
Name	Test page
Description	Test page description
Apply page	● All ○ Role List
Active	☑ Enable the page

Editing an existing customized page

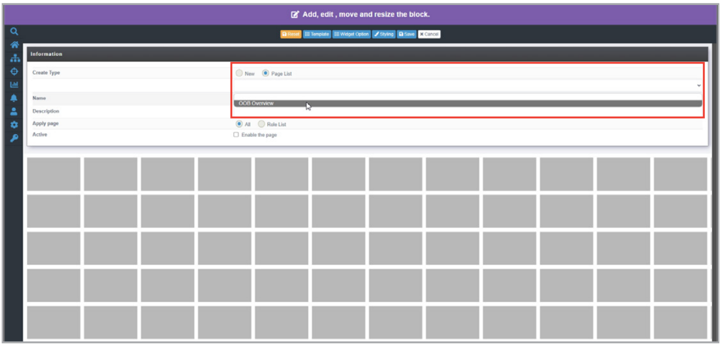
Select an existing custom page to open the custom page editor.



Name	Role Name	Active	▼ Update Time	Description
OOB Overview	All	□	2024-01-29 11:48:41	OOB Overview

Using an existing custom page as a template

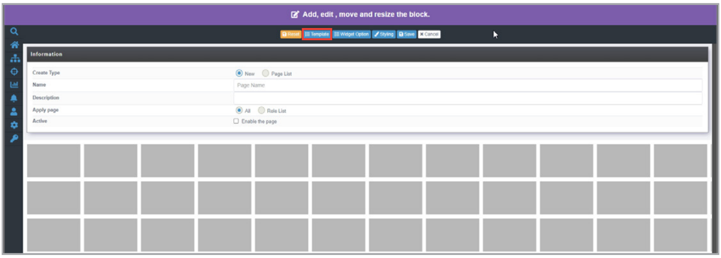
In the custom page editor, select the **Page List** option in the **Create Type** field, then select a custom page from the drop down list to use as a template.



Create Type	○ New ● Page List
	OOB Overview
Name	
Description	
Apply page	● All ○ Role List
Active	□ Enable the page

Loading a custom page template

1. In the custom page editor, click **Template**.



Create Type ● New ○ Page List

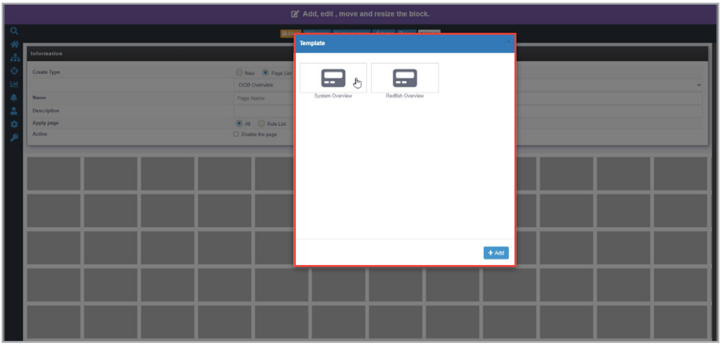
Name Page Name

Description

Apply page ● All ○ Role List

Active □ Enable the page

2. Select a template, then click **Add**.



Create Type ○ New ● Page List

OOB Overview

Name Page Name

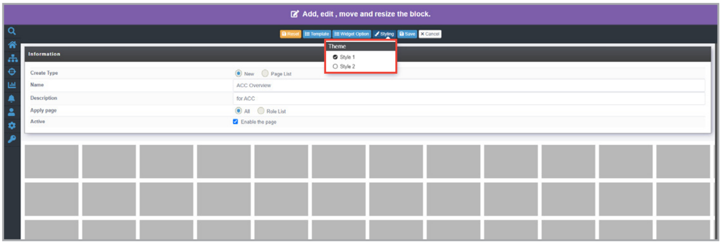
Description

Apply page ● All ○ Role List

Active □ Enable the page

Changing the theme of the custom page

In the custom page editor, click **Styling**, then select a theme from the drop down menu.



Create Type ● New ○ Page List

Name ACC Overview

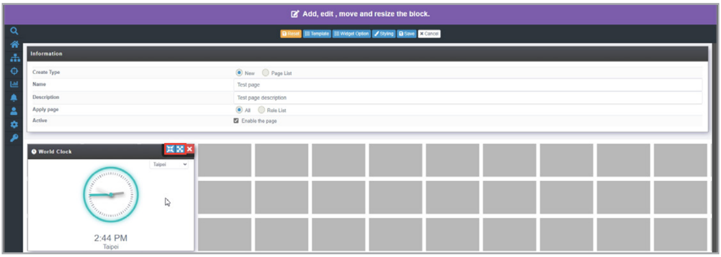
Description for ACC

Apply page ● All ○ Role List

Active ☑ Enable the page

Changing the size of widgets

Click the enlarge or shrink button in the title bar of the widget.



Create Type ● New ○ Page List

Name: Test page

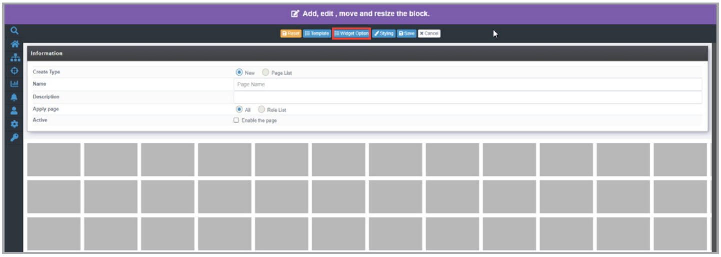
Description: Test page description

Apply page ● All ○ Role List

Active ☑ Enable the page

Adding a widget using the widget gallery

1. In the custom page editor, click **Widget Option**.



Create Type ● New ○ Page List

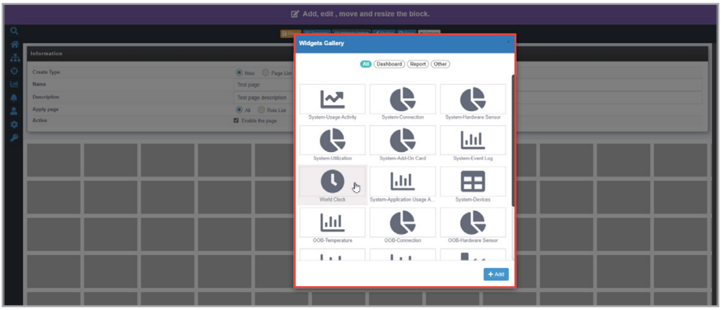
Name:

Description:

Apply page ● All ○ Role List

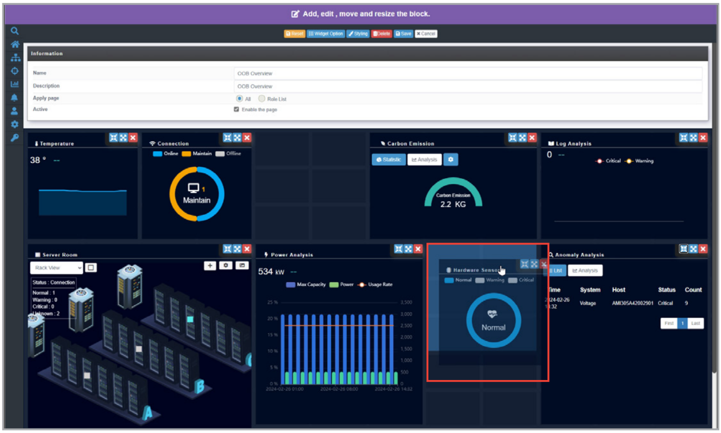
Active □ Enable the page

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.

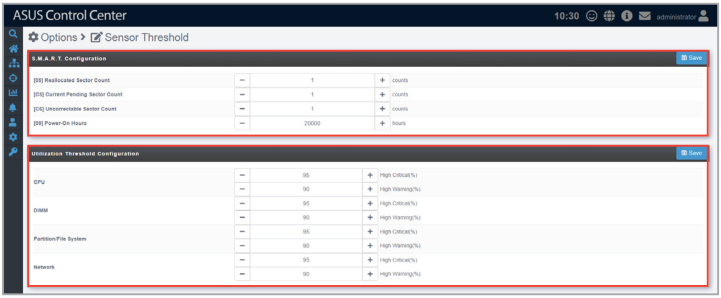


Name: OOB Overview
Description: OOB Overview
Apply page: ● All ○ Role List
Active: ☑ Enable the page

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**.



S.M.A.R.T. Configuration

[05] Reallocated Sector Count	1	counts
[C5] Current Pending Sector Count	1	counts
[C6] Uncorrectable Sector Count	1	counts
[09] Power-On Hours	20000	hours

Utilization Threshold Configuration

CPU	95	High Critical(%)
	90	High Warning(%)
DIMM	95	High Critical(%)
	90	High Warning(%)
Partition/File System	95	High Critical(%)
	90	High Warning(%)
Network	95	High Critical(%)
	90	High Warning(%)

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

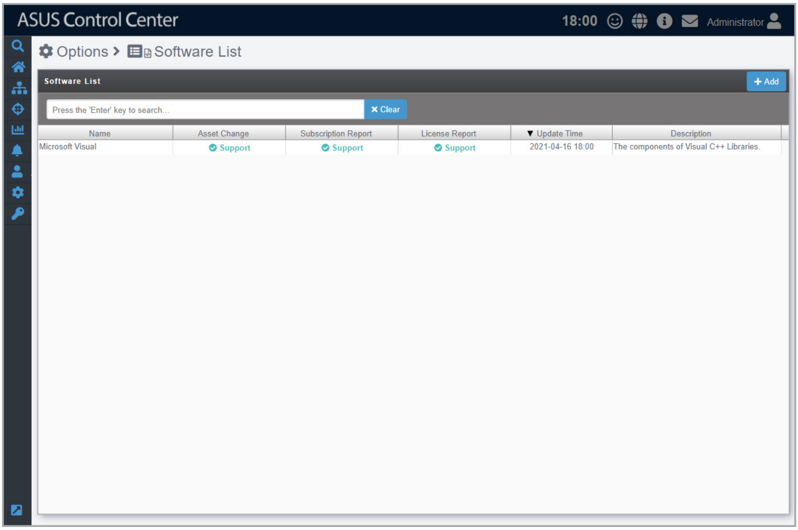
Adjust the threshold at which warnings and critical warnings will be shown, then click **Save** to save and apply the changes made to all managed devices.

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.

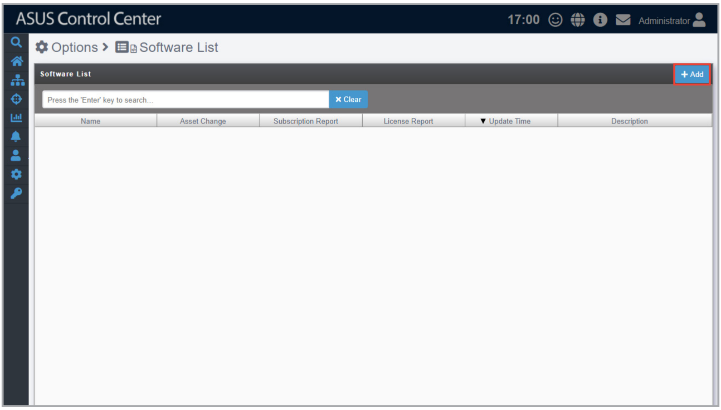
To access **Software List**, click ⚙ in the left menu, then click on **Software List** in the Definition block.



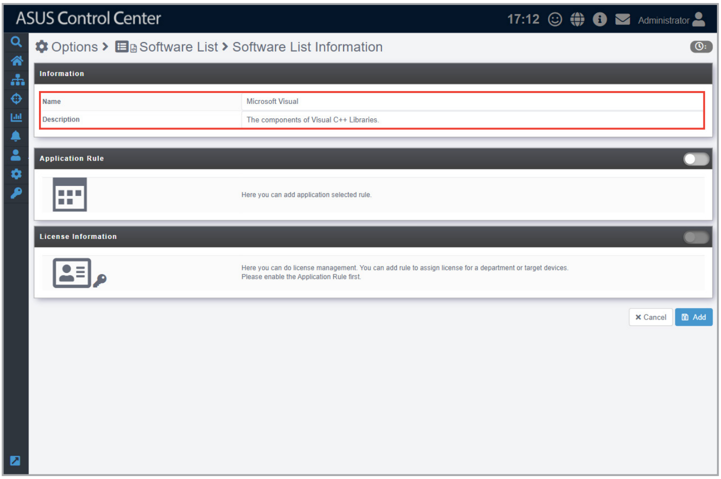
Name	Asset Change	Subscription Report	License Report	▼ Update Time	Description
Microsoft Visual	✓ Support	✓ Support	✓ Support	2021-04-16 18:00	The components of Visual C++ Libraries.

Adding a software list

1. Click on **Add**.



2. Enter the **Name** and **Description** of the software list.

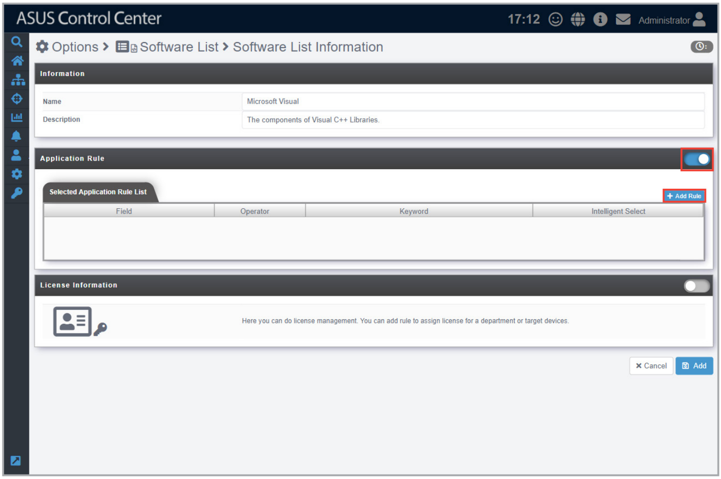


Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Here you can add application selected rule.

Here you can do license management. You can add rule to assign license for a department or target devices. Please enable the Application Rule first.

3. Click on the slide button in the **Application Rule** block, then click on **Add Rule**.



Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Field	Operator	Keyword	Intelligent Select

Here you can do license management. You can add rule to assign license for a department or target devices.

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.

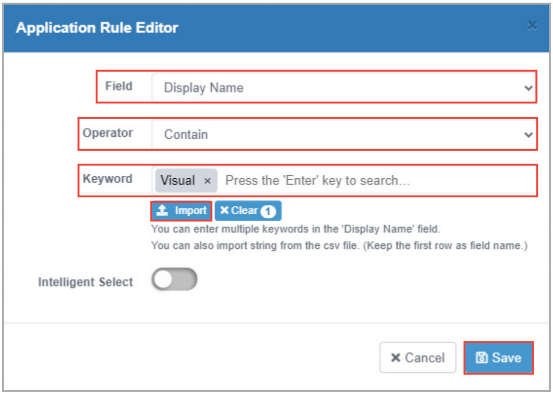
- Using Conditions (Display Name, Publisher, Version)

   a. Select a **Field**.

   b. Select the Operator (**Equal**, **Contain**, **Not Contain**), this will allow you to set the conditions for the keywords you enter.

   c. Enter keyword(s) or use the **Import** button to import keywords from a .csv file.

   d. Click on **Save** once you are finished adding keywords.



Field: Display Name

Operator: Contain

Keyword: Visual × Press the 'Enter' key to search...

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: ○

- Using Intelligent Select (Display Name)

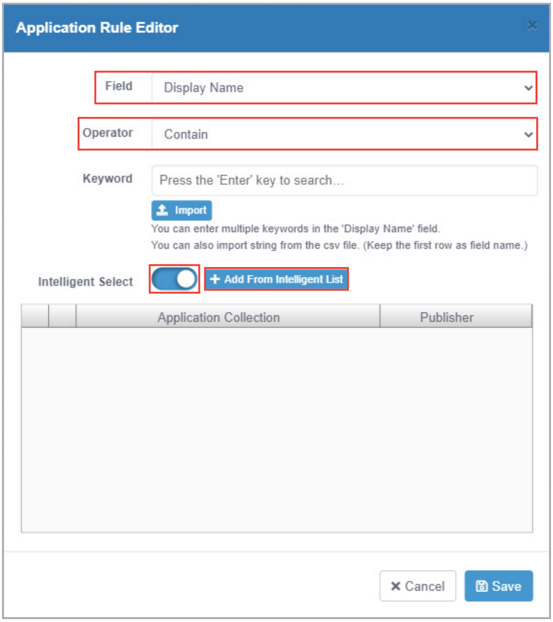
  Intelligent Select will group softwares with slight differences in software name, publisher or version. For example the *Microsoft Visual Studio* Application Collection will include both *Microsoft Visual Studio 2016* and *Microsoft Visual Studio 2019*.

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**.


Application Rule Editor

Field: Display Name

Operator: Contain

Keyword: Press the 'Enter' key to search...

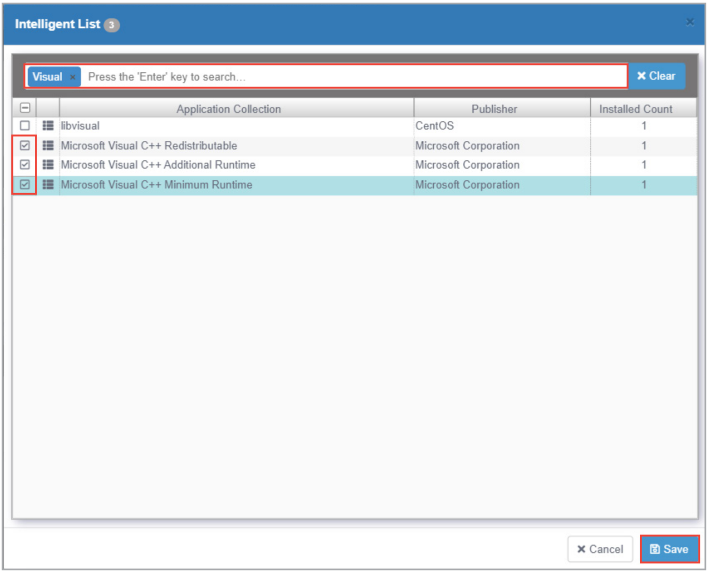
You can enter multiple keywords in the 'Display Name' field.
You can also import string from the csv file. (Keep the first row as field name.)

Intelligent Select

		Application Collection	Publisher

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.

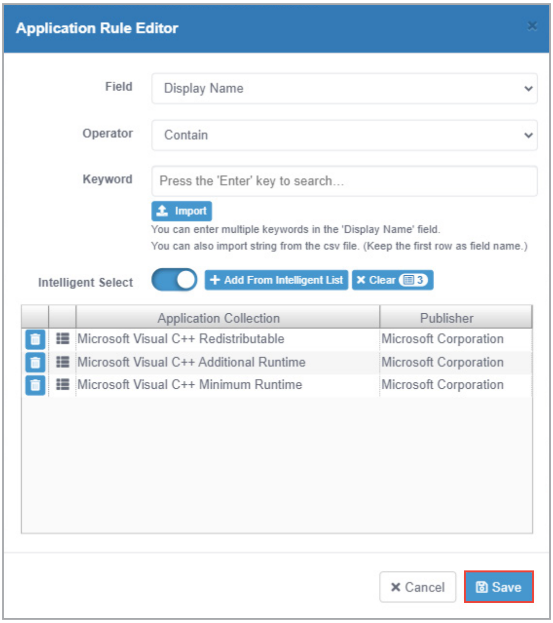
Click on ☰ next to the Application Collection name to view all applications included in the Application Collection.



⊟		Application Collection	Publisher	Installed Count
□	☰	libvisual	CentOS	1
☑	☰	Microsoft Visual C++ Redistributable	Microsoft Corporation	1
☑	☰	Microsoft Visual C++ Additional Runtime	Microsoft Corporation	1
☑	☰	Microsoft Visual C++ Minimum Runtime	Microsoft Corporation	1

e. Click on **Save** when you are finished.

Click on **Clear** to clear all Application Collections added.



Application Rule Editor

Field: Display Name

Operator: Contain

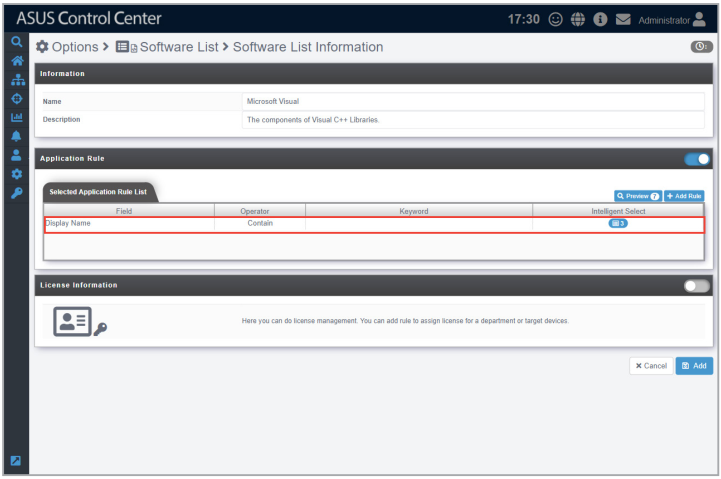
Keyword: Press the 'Enter' key to search...

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

Application Collection	Publisher
Microsoft Visual C++ Redistributable	Microsoft Corporation
Microsoft Visual C++ Additional Runtime	Microsoft Corporation
Microsoft Visual C++ Minimum Runtime	Microsoft Corporation

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.



Information

Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

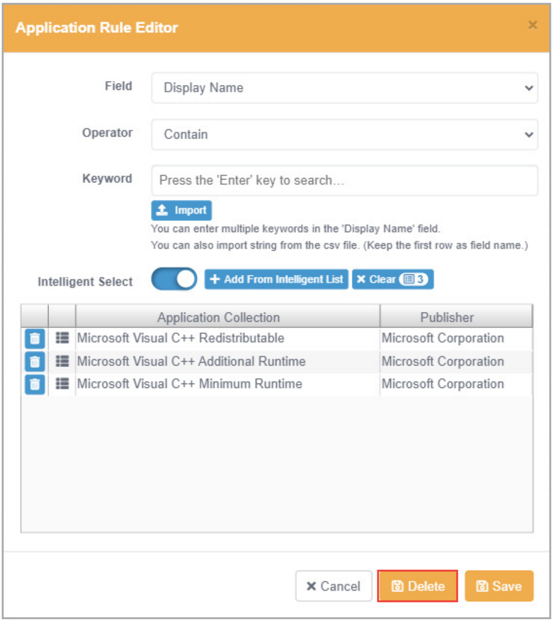
Application Rule

Selected Application Rule List

Field	Operator	Keyword	Intelligent Select
Display Name	Contain		3

License Information

Here you can do license management. You can add rule to assign license for a department or target devices.


Application Rule Editor

Field: Display Name

Operator: Contain

Keyword: Press the 'Enter' key to search...

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.)

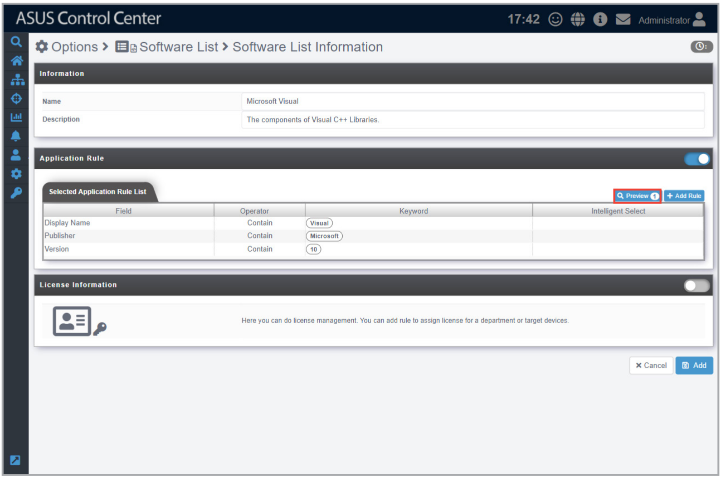
Intelligent Select

		Application Collection	Publisher
		Microsoft Visual C++ Redistributable	Microsoft Corporation
		Microsoft Visual C++ Additional Runtime	Microsoft Corporation
		Microsoft Visual C++ Minimum Runtime	Microsoft Corporation

6. Repeat step 3 to step 5 to add more Application Rules.

> 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.



ASUS Control Center
17:42
Administrator
Options > Software List > Software List Information

Information

Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

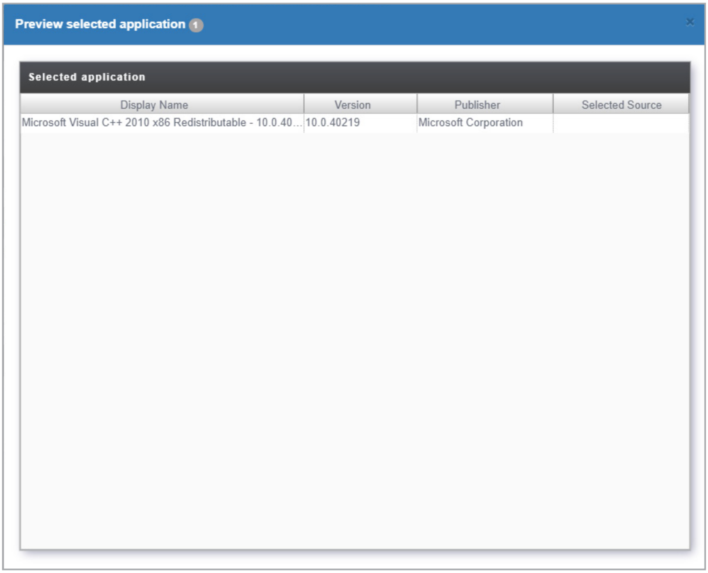
Application Rule

Selected Application Rule List
Preview 1
+ Add Rule

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

License Information

Here you can do license management. You can add rule to assign license for a department or target devices.



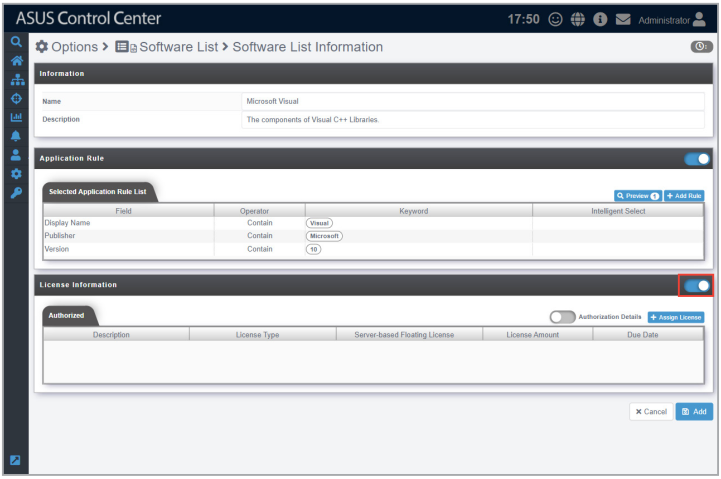
Preview selected application 1

Selected application

Display Name	Version	Publisher	Selected Source
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40...	10.0.40219	Microsoft Corporation	

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 — Preview 1 — + Add Rule

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

License Information

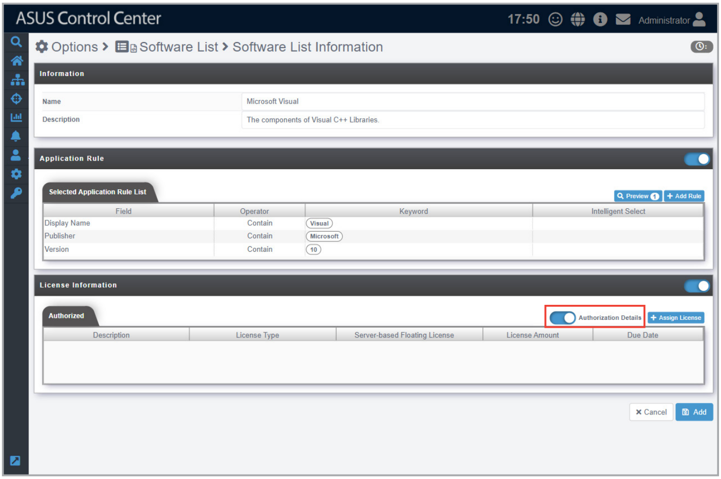
Authorized — Authorization Details — + Assign License

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.

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 — Preview 1 — + Add Rule

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

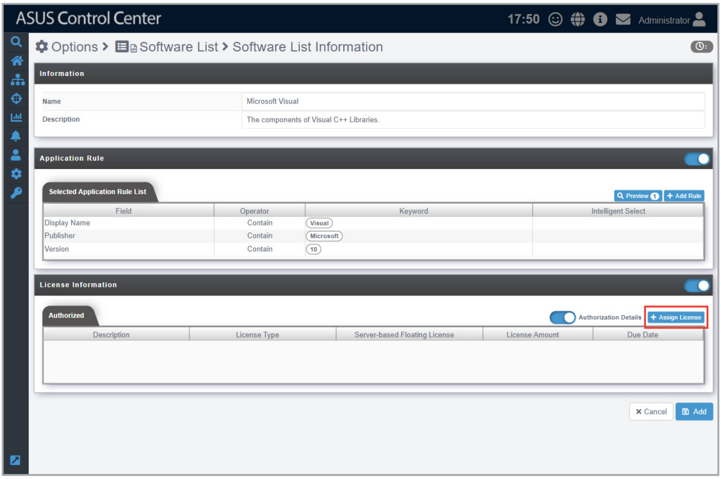
License Information

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 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

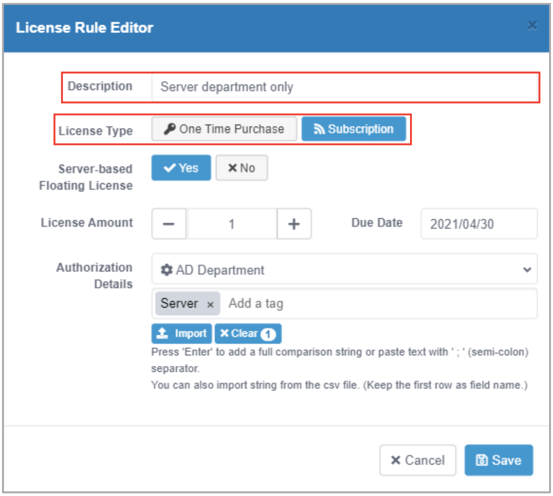
Authorized

Description	License Type	Server-based Floating License	License Amount	Due Date

11. Enter a **Description** for the License.

12. Select the **License Type**.

- **One Time Purchase**: Softwares that are a one time purchase and require no other subscription fees.
- **Subscription**: Softwares that require a periodic subscription fee.



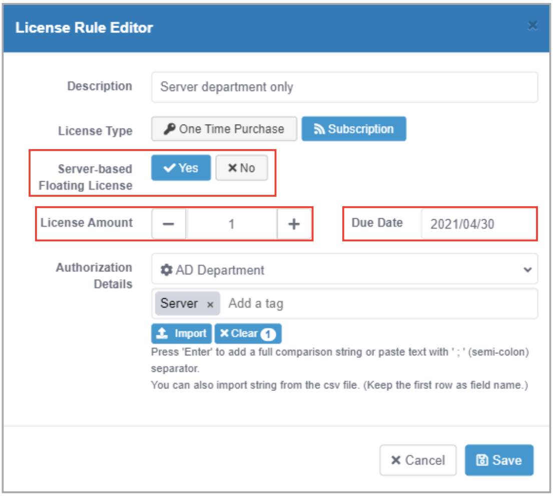
License Rule Editor

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 × 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.)

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 is 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**.

This option is only available when **Subscription** is selected as the **License Type**.



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 × Add a tag

Import | ✕ Clear 1

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

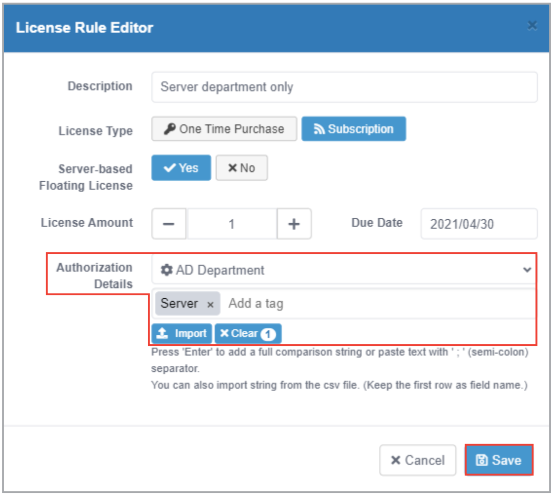
16. Select the Authorization Details from the drop down menu.

- 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.

- 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 (selected)

Server-based Floating License: Yes (selected) / No

License Amount: 1

Due Date: 2021/04/30

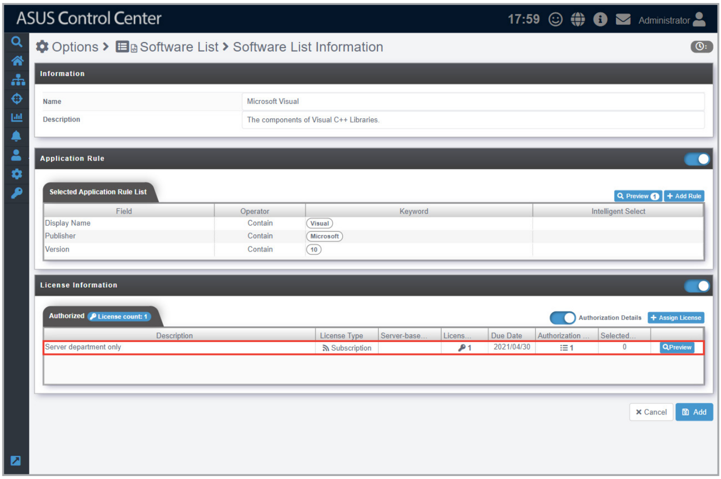
Authorization Details: AD Department

Server ×

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.



Information

Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Application Rule

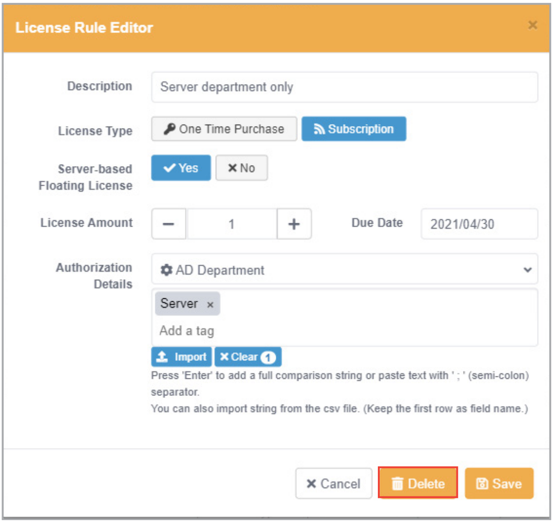
Selected Application Rule List

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

License Information

Authorized License count: 1

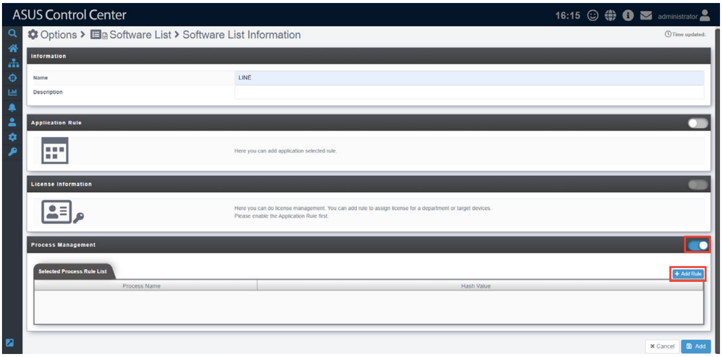
Description	License Type	Server-base...	Licens...	Due Date	Authorization ...	Selected...	
Server department only	Subscription		1	2021/04/30	1	0	Preview



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 × 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.)

20. (optional) Click on the slide button in the **Process Management** block, then click **Add Rule**.



ASUS Control Center

Options > Software List > Software List Information

Information

Name: LINE

Description:

Application Rule

Here you can add application selected rule.

License Information

Here you can do license management. You can add rule to assign license for a department or target devices.
Please enable the Application Rule first.

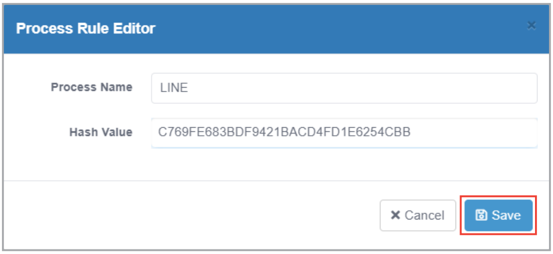
Process Management

Selected Process Rule List

Process Name	Hash Value

21. Enter the **Process Name** and **Hash Value** of the process, then click **Save**.

To get the hash value of a process, refer to **Application Usage Analysis** under the **Software Report** section of the **Report** chapter.

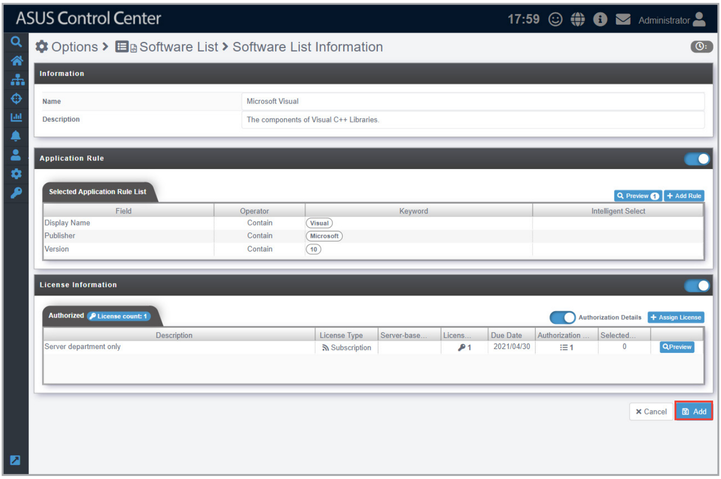


Process Rule Editor

Process Name: LINE

Hash Value: C769FE683BDF9421BACD4FD1E6254CBB

22. Click on **Add** once you have finished editing the software list.

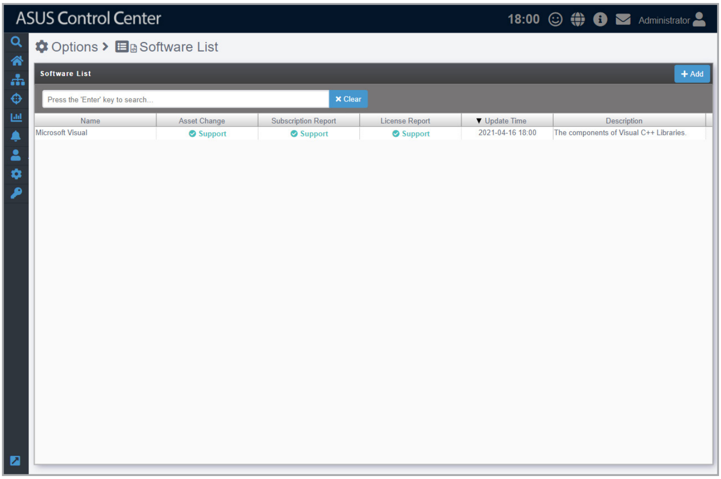


Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

Description	License Type	Server-base...	Licens...	Due Date	Authorization ...	Selected...	
Server department only	Subscription		1	2021/04/30	1	0	Preview

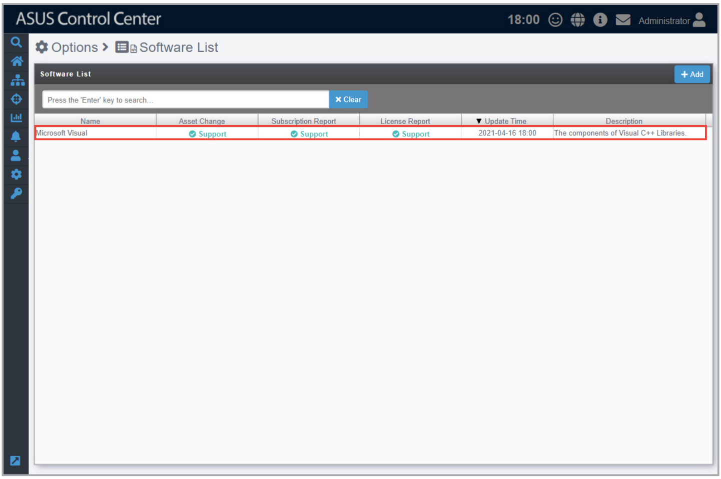
Your newly added software list should appear in the main Software List screen. For more information on applying the software list, please refer to the **Trust Software Asset** or **Focus Software Asset** sections.



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

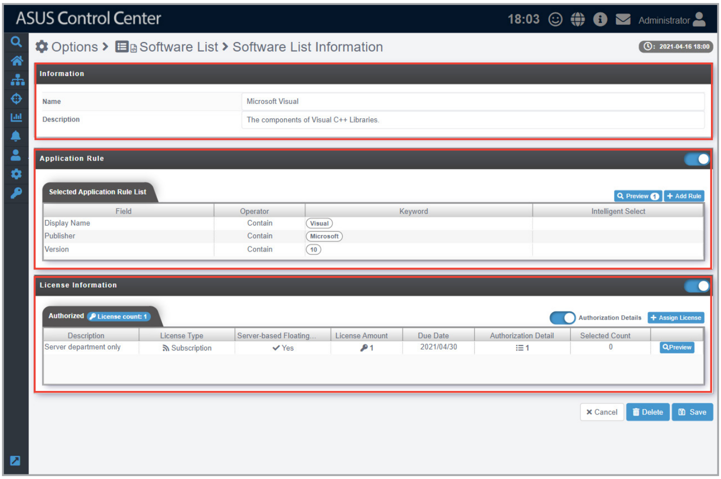
1. Click on the software list you would like to edit from the **Software List**.



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. 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.

You can see the date and time of the last time this software list was updated in the top right corner.



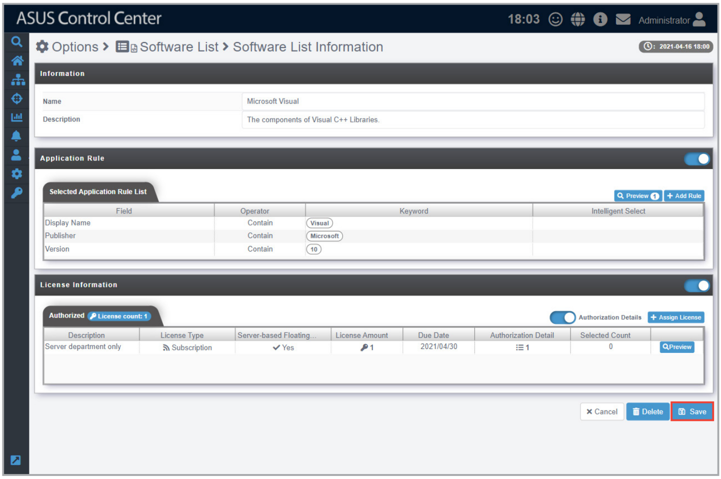
Information

Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

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	Preview

3. Click on **Save** once you are finished editing the software list.



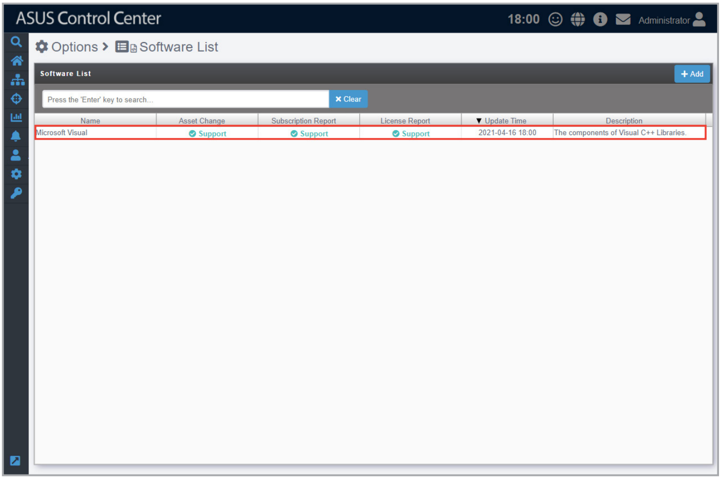
Name	Microsoft Visual
Description	The components of Visual C++ Libraries.

Field	Operator	Keyword	Intelligent Select
Display Name	Contain	Visual	
Publisher	Contain	Microsoft	
Version	Contain	10	

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	Preview

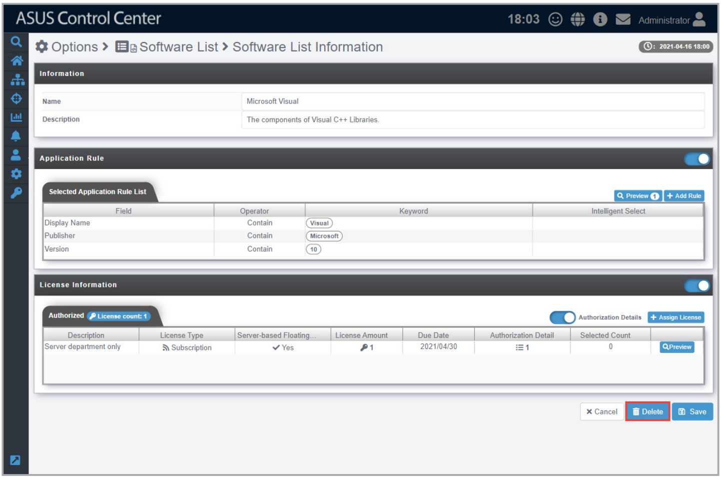
Deleting a software list

1. Click on the software list you would like to delete from the **Software List**.



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.



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 Floating...	License Amount	Due Date	Authorization Detail	Selected Count	
Server department only	Subscription	✓ Yes	1	2021/04/30	☰ 1	0	Preview

Chapter 9

This chapter describes the license settings.

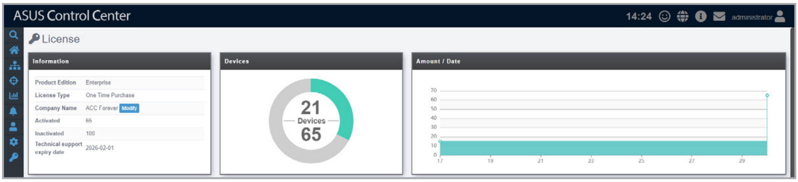
License

9.1 License Information

The **License** page displays license information, the number of licensed devices, the total number of licenses, and a time distribution graph of licensed devices.You can also upgrade from ASUS Control Center Classic or CSM edition to Enterprise edition. For more information on license keys, refer to https://asuscontrolcenter.asus.com.

To access **License**, click 🔑 in the left menu.

The upper number in the **Devices** block displays the number of activated devices and the bottom number displays the number of activated licenses.



ASUS Control Center

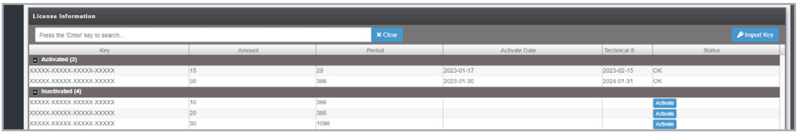
License

Information

Product Edition	Enterprise
License Type	One Time Purchase
Company Name	ACC Forever Modify
Activated	65
Inactivated	100
Technical support expiry date	2026-02-01

One Time Purchase licenses

For One Time Purchase licenses, the License Information list shows active and inactive licenses, and the activation date and technical support period for each license.



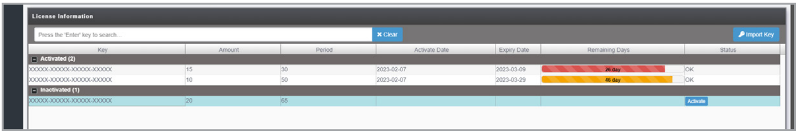
License Information

Press the 'Enter' key to search... ✕ Clear 🔑 Import Key

Key	Amount	Period	Activate Date	Technical S...	Status
⊟ Activated (2)					
XXXXX-XXXXX-XXXXX-XXXXX	15	29	2023-01-17	2023-02-15	OK
XXXXX-XXXXX-XXXXX-XXXXX	50	366	2023-01-30	2024-01-31	OK
⊟ Inactivated (4)					
XXXXX-XXXXX-XXXXX-XXXXX	10	366			Activate
XXXXX-XXXXX-XXXXX-XXXXX	20	366			Activate
XXXXX-XXXXX-XXXXX-XXXXX	30	1098			Activate

Subscription licenses

For Subscription licenses, the License Information list shows active and inactive licenses, and the activation date and expiry date for each license.



License Information

Press the 'Enter' key to search... ✕ Clear 🔑 Import Key

Key	Amount	Period	Activate Date	Expiry Date	Remaining Days	Status
⊟ Activated (2)						
XXXXX-XXXXX-XXXXX-XXXXX	15	30	2023-02-07	2023-03-09	26 day	OK
XXXXX-XXXXX-XXXXX-XXXXX	10	50	2023-02-07	2023-03-29	46 day	OK
⊟ Inactivated (1)						
XXXXX-XXXXX-XXXXX-XXXXX	20	65				Activate

Activating a License key

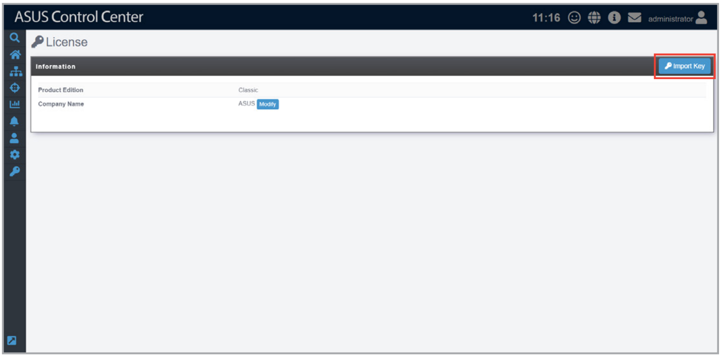
Click Activate next to an unused license key to activate a license.

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.

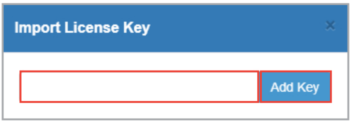
A working Internet connection is required when verifying the upgrade License key.

1. Click on **Import Key**.



Product Edition	Classic
Company Name	ASUS Modify

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.

System Requirements

Hardware Host Server Requirements

Virtual machine hypervisors		Oracle VirtualBox 5.1.x VMware ESXi 5.x
Virtual machine resources (3000 clients capability)	**vCPU (Cores)**	12 cores
	Memory (GB)	128 GB memory
	Disk (GB)	500 GB disk space
	Hypervisor recommended	VMware
Virtual machine resources (1000 clients capability)	**vCPU (Cores)**	12 cores
	Memory (GB)	64 GB memory
	Disk (GB)	200 GB disk space
	Hypervisor recommended	VMware
Virtual machine resources (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 (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 SMTP SNMP Connection among devices
Supported Internet browsers		Browsers with HTML5 support Google Chrome Firefox Apple Safari ASUS ZenUI browser

We do not recommend using Virtual Box as a hypervisor for client capabilites above 500 clients.

Managed Clients Requirements

Supported client OS	Windows 7 Windows 10 Windows 11 Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2022 RedHat 7.0~/8.0~/9.0~ CentOS 7.0~/8.0~ SUSE 12 SP3~/15~ Ubuntu 16.04~ Debian 9~ Rocky Linux 8.0~/9.0~ Scientific Linux 6.0~/7.0~
Requirement on Client Systems	Windows .NET Framework 4.8 Linux sysstat, smartmontools, ethtool, curl, ipmitool, OpenIPMI-libs, OpenIPMI-tools, pciutils, net-tools, ssh RHEL 6.0~8.5, CentOS 8~ (libnsl package installation required) SLES 15~ (insserv-compat installation required)

Service and Support

Visit our multi-language website at https://www.asus.com/support.