

v1.2



ASUS Control Center

User Guide

Copyright © 2020 ASUSTeK COMPUTER INC. All Rights Reserved.

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

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

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

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

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

Contents

About this guide	ix
------------------------	----

Chapter 1: Getting Started

1.1	Introduction to ASUS Control Center.....	1-2
1.1.1	How ASUS Control Center works	1-2
1.1.2	ASUS Control Center Licensing.....	1-3
1.2	Installation	1-5
1.2.1	Setting up the Hypervisor Environment	1-5
1.2.2	Importing the OVA file.....	1-7
1.3	Initialize settings	1-9
1.3.1	Initialize startup settings.....	1-9
1.3.2	Logging in to ASUS Control Center	1-12
1.4	ASUS Control Center layout	1-13
1.4.1	Banner	1-13
	<i>Logo.....</i>	<i>1-13</i>
	<i>Feedback.....</i>	<i>1-14</i>
	<i>Multiple Language</i>	<i>1-14</i>
	<i>About</i>	<i>1-14</i>
	<i>Mission Center.....</i>	<i>1-15</i>
	<i>Account Information.....</i>	<i>1-15</i>
1.4.2	Menu	1-16

Chapter 2: Monitor

2.1	System Overview	2-2
2.1.1	Status Dashboard	2-3
	<i>Connection overview</i>	<i>2-4</i>
	<i>Hardware Sensor overview</i>	<i>2-5</i>
	<i>Utilization overview.....</i>	<i>2-6</i>
	<i>Event Log overview</i>	<i>2-7</i>
2.1.2	Devices list.....	2-8
	<i>Setting power control (Action)</i>	<i>2-9</i>
	<i>Auto Refreshing the devices list (Auto Refresh).....</i>	<i>2-10</i>
	<i>Exporting devices list (Export).....</i>	<i>2-10</i>
2.1.3	Options.....	2-11
	<i>Hiding or displaying metadata fields.....</i>	<i>2-11</i>
	<i>Using the Row Groupings function</i>	<i>2-12</i>
	<i>Accessing remote desktop</i>	<i>2-13</i>

Contents

- 2.1.4 Search and Filter devices2-16
 - Filter devices using the Overview Circle*..... 2-16
 - Filter devices using the Search Bar*..... 2-17
 - Filter devices using the Advanced Event Log*..... 2-19
 - Filter devices using Column Headers*..... 2-20
- 2.2 Device Information2-21**
 - 2.2.1 Hardware Sensor2-23
 - 2.2.2 Utilization2-25
 - Editing the threshold values* 2-26
 - 2.2.3 Inventory2-27
 - 2.2.4 BMC2-28
 - Edit BMC using ASMB*..... 2-29
 - 2.2.5 Software2-30
 - Application*..... 2-31
 - Services (Windows only)* 2-33
 - Processes*..... 2-34
 - Environment Variables (Windows only)*..... 2-35
 - Software Market* 2-36
 - 2.2.6 Event Log2-37
 - Filtering the Event Log using the Advanced Search*..... 2-40
 - 2.2.7 BIOS2-43
 - BIOS Flash* 2-44
 - BIOS Setting*..... 2-49
 - DMI Info*..... 2-50
 - 2.2.8 Security2-51
 - Registry Editor (Windows only)* 2-52
 - USB Storage Device (Windows only)* 2-52
 - Watchdog* 2-53
 - 2.2.9 Configuration.....2-54
 - Agent Configuration*..... 2-55
 - Agent Uninstall Password*..... 2-56
- 2.3 VM Overview2-57**
 - Exporting VMware vSphere Hypervisors list* 2-58
- 2.4 Host Information2-59**
 - Exporting VM Information* 2-60
 - Setting Power Control*..... 2-61
 - Accessing remote desktop* 2-62

Contents

Chapter 3: Deployment

3.1	Agent Management	3-2
3.1.1	Deploy Agents.....	3-3
	<i>Adding a single device</i>	3-4
	<i>Adding multiple devices</i>	3-9
	<i>Exporting Deployment Management list</i>	3-11
	<i>Agent deployment conditions and settings</i>	3-12
3.1.2	Scan and Deploy.....	3-14
	<i>Scanning for managed devices and deploying agents</i>	3-15
3.1.3	Remove agents.....	3-20
	<i>Remove agents using ASUS Control Center</i>	3-20
	<i>Remove Windows Agent from local device</i>	3-22
	<i>Remove Linux Agent from local device</i>	3-25
3.1.4	Windows Agent.....	3-28
	<i>Install Windows agents manually</i>	3-28
3.1.5	Linux Agent.....	3-32
	<i>Install Linux agents manually</i>	3-32
3.1.6	Agent Deploy Report.....	3-36
3.2	Agentless Management	3-37
3.2.1	Add vSphere.....	3-38
	<i>Adding a single vSphere</i>	3-38
	<i>Adding multiple vSphere hypervisors</i>	3-41
	<i>Exporting VMware vSphere Host List</i>	3-42
3.2.2	Remove vSphere.....	3-43

Chapter 4: Centralized

4.1	Metadata Management	4-2
	<i>Adding metadata fields</i>	4-3
	<i>Editing metadata fields</i>	4-5
	<i>Deleting metadata fields</i>	4-6
	<i>Editing the metadata value of a single device</i>	4-7
	<i>Editing the metadata value of multiple devices</i>	4-8
	<i>Exporting the metadata value</i>	4-11
4.2	BIOS Flash Management	4-12
4.2.1	BIOS Cache.....	4-13
	<i>Adding a BIOS cap file to the BIOS Cache</i>	4-13
	<i>Removing BIOS cap files from BIOS Cache</i>	4-14

Contents

- 4.2.2 BIOS Flash Task 4-15
 - Manually uploading the BIOS cap file*..... 4-15
 - Selecting the BIOS cap file from the BIOS cache* 4-17
- 4.2.3 BIOS Flash Task Report 4-20
- 4.3 Security Management 4-21**
- 4.4 Software Dispatch 4-23**
 - 4.4.1 Software Pool..... 4-24
 - Adding software packages to the Software Pool*..... 4-24
 - Removing software packages from the Software Pool*..... 4-27
 - 4.4.2 Software Dispatch Task 4-28
 - Dispatching software packages to devices*..... 4-29
 - 4.4.3 Software Dispatch Task Report 4-31
- 4.5 Task Scheduler 4-32**
 - Task Scheduler Overview*..... 4-33
 - Adding a scheduled task* 4-35
 - Editing a scheduled task*..... 4-42
 - Deleting a scheduled task* 4-42
- 4.6 Power Control 4-43**

Chapter 5: Report

- 5.1 Software Report 5-2**
 - 5.1.1 Software Inventory 5-2
 - Refetch Application*..... 5-3
 - Filter newly installed applications* 5-3
 - Search for applications using keywords* 5-4
 - 5.1.2 Trust List 5-9
 - 5.1.3 Focus List..... 5-14
 - 5.1.4 Subscription Report 5-18
- 5.2 Task Report 5-29**
 - 5.2.1 Software Dispatch Report 5-30
 - 5.2.2 BIOS Flash Report..... 5-30
 - 5.2.3 Agent Update Report 5-31
 - 5.2.4 Agent Deploy Report..... 5-31

Chapter 6: Notification

- 6.1 SMTP Settings 6-2**
 - To set up the SMTP Server:*..... 6-3

Contents

6.2	Rule Management	6-6
	<i>Adding a new rule.....</i>	<i>6-7</i>
	<i>Deleting a notification rule</i>	<i>6-14</i>
6.3	Asset Changes	6-15
6.3.1	Software Asset.....	6-16
6.3.2	Hardware Asset	6-18

Chapter 7: Account Management

7.1	Role Privilege Management	7-2
	<i>Adding a new role.....</i>	<i>7-3</i>
	<i>Editing a role.....</i>	<i>7-6</i>
	<i>Deleting a role</i>	<i>7-8</i>
7.2	Accounts Management.....	7-10
	<i>Adding a new account</i>	<i>7-11</i>
	<i>Editing an account.....</i>	<i>7-14</i>
	<i>Deleting an account.....</i>	<i>7-15</i>

Chapter 8: Options

8.1	General Configuration	8-2
	<i>Adjusting items on the General configurations page</i>	<i>8-2</i>
8.2	Network Configuration	8-4
	<i>Adjusting the Network configurations</i>	<i>8-4</i>
8.3	Appearance Configuration	8-6
	<i>Setting a custom banner logo.....</i>	<i>8-7</i>
	<i>Resetting the banner logo</i>	<i>8-8</i>
8.4	Security Configuration	8-9
	<i>Setting a new Password.....</i>	<i>8-10</i>
	<i>Editing the Password.....</i>	<i>8-11</i>
	<i>Disabling the Password.....</i>	<i>8-11</i>
8.5	Backup & Restore	8-12
	<i>Setting the periodic backup</i>	<i>8-13</i>
	<i>Restoring the backup file.....</i>	<i>8-17</i>
8.6	Maintenance	8-19
	<i>Cofiguring the power option of Hypervisors.....</i>	<i>8-19</i>
	<i>Restarting the Services</i>	<i>8-20</i>

Contents

- 8.7 DBExpose Configuration.....8-21
 - To set the DBExpose account and password..... 8-21*
 - To edit the DBExpose account information 8-22*
 - To delete the DBExpose account information 8-23*
 - Using a third-party software to access ASUS Control Center . 8-24*
- 8.8 Sensor Threshold Configuration8-26
 - Adjusting the Disk S.M.A.R.T. status configurations 8-26*

Chapter 9: License

- 9.1 License Information9-2
 - Importing a License key..... 9-3*

Chapter 10: Update

- 10.1 Update10-2
 - 10.1.1 Update Task.....10-3
 - Updating Windows and Linux agents 10-4*
 - Updating ASUS Control Center main server 10-7*
 - 10.1.2 Agent Update Report10-8

Appendix

- System RequirementsA-2
 - Hardware Host Server Requirements.....A-2*
 - Managed Clients RequirementsA-3*
- ASUS contact informationA-4

About this guide

Audience

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

Contents

This guide contains the following parts:

Chapter 1: Getting Started

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

Chapter 2: Monitor

This chapter describes the various monitoring tools and options available.

Chapter 3: Deployment

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

Chapter 4: Centralized Management

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 and software related subscriptions.

Chapter 6: Notification

This chapter describes setting the notifications and SMTP Server

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 configuration options, and also backup and maintenance configurations.

Chapter 9: Options

This chapter describes the license settings.

Chapter 10: Update

This chapter describes the main system and agent update configurations.

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>+

Command

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

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

Reference

Visit the ASUS websites worldwide that provide updated information for all ASUS hardware and software products. Refer to the ASUS contact information for details.

Chapter 1

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

Getting Started

1.1 Introduction to ASUS Control Center

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

1.1.1 How ASUS Control Center works

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

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

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

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

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

1.1.2 ASUS Control Center Licensing

ASUS Control Center provides three license editions:

- **Classic edition** for assisting management on ASUS servers and workstations.
- **CSM edition** for ASUS Corporate Stable Model for enterprises, medium, or small businesses.
- **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	CSM	Enterprise
Banner	Mission Center	√	√	√
	System Overview	√	√	√
Monitor (Overview)	VM Overview	-	-	√
	Host Information	-	-	√
Monitor (one node)	Device Information	√	Partial functions unavailable	√
	Hardware Sensor	√	√	√
	Utilization	√	√	√
	Inventory	-	√	√
	Event Log	Partial functions unavailable	Partial functions unavailable	√
	Software	Partial functions unavailable	√	√
	BMC	√	-	√
	BIOS	Partial functions unavailable	√	√
	Security	Partial functions unavailable	√	√
	Configuration	Partial functions unavailable	Partial functions unavailable	√
	Deployment	Agent Management	√	√*
Agentless Management		-	-	√
Centralized	Metadata Management	√	√	√
	BIOS Flash Management	Partial functions unavailable	√	√
	Security Management	-	√	√
	Software Dispatch	Partial functions unavailable	√	√
	Task Scheduler	-	√	√
	Power Control	-	-	√
Report	Software Report	-	Partial functions unavailable	√
	Task Report	Partial functions unavailable	Partial functions unavailable	√

(continued on the next page)

Features		Classic	CSM	Enterprise
Notification	SMTP Settings	√	√	√
	Rule Management	√	√	√
	Asset Changes	-	-	√
Account	Role Privilege	-	√	√
	Accounts Management	-	√	√
Options	General Configuration	√	√	√
	Network Configuration	√	√	√
	Appearance Configuration	-	√	√
	Security Configuration	-	-	√
	Maintenance	√	√	√
	DBExpose Configuration	-	-	√
	Sensor Threshold	√	√	√
License	License	√	√	√
Update	Update	√	√	√

* 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

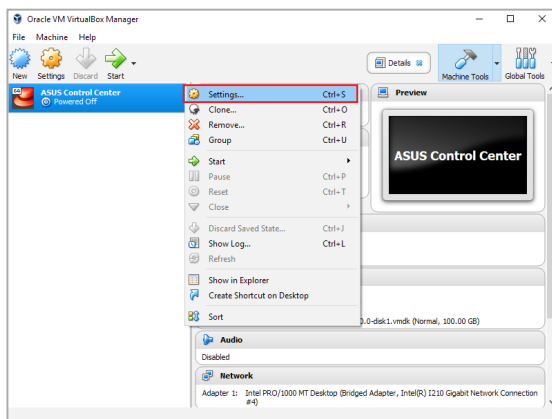
ASUS Control Center is a virtual appliance running on a virtual machine (VM), with all required services and settings pre-installed. The system requirements can be found in the **Appendix** section of this manual.

To install the ASUS Control Center on the Oracle VirtualBox, follow the steps below:

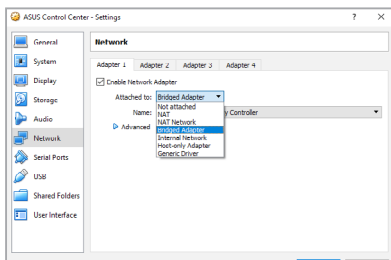
1.2.1 Setting up the Hypervisor Environment

A message may appear when starting up the VM for the first time, follow the steps below to set up the network settings:

1. Launch your VM, then right click on the OVA and select **Settings**.

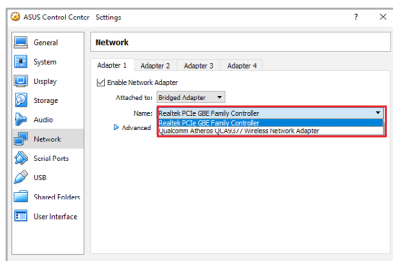


2. Select **Network** from the menu list on the left, then select **Bridged Adapter** in the **Attached to:** field.



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.



1.2.2 Importing the OVA file



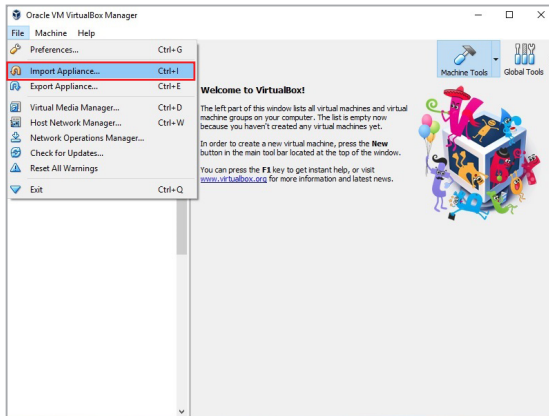
Oracle Virtualbox will be used as an example for Hypervisor related items.

1. Download **Oracle VirtualBox** and the **ASUS Control Center OVA** file.

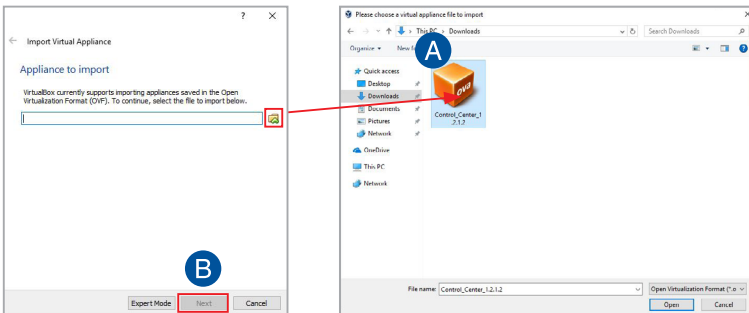


- Please refer to <http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html> to download **Oracle VirtualBox**.
- Please refer to <https://asuscontrolcenter.asus.com> to download the **ASUS Control Center OVA** file.

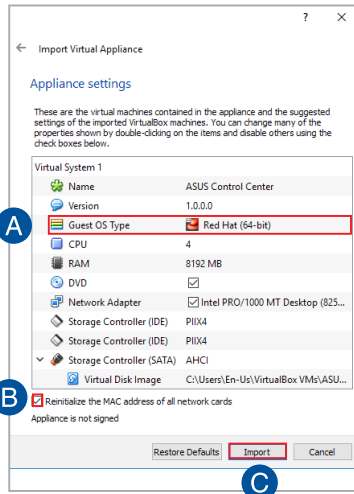
2. Install and launch **Oracle VirtualBox**, then select **File > Import Appliance...** to launch the **Import Virtual Appliance** wizard.



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



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



6. Wait for the appliance 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.



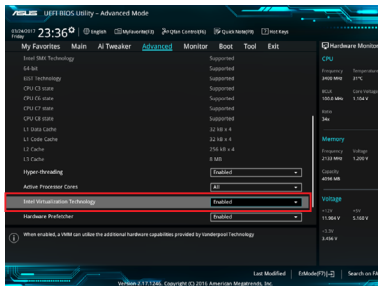
The minimum requirements for VM is as follows:

- 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**



- **Network Card:** Select the network connection you are currently using.

1.3 Initialize settings

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

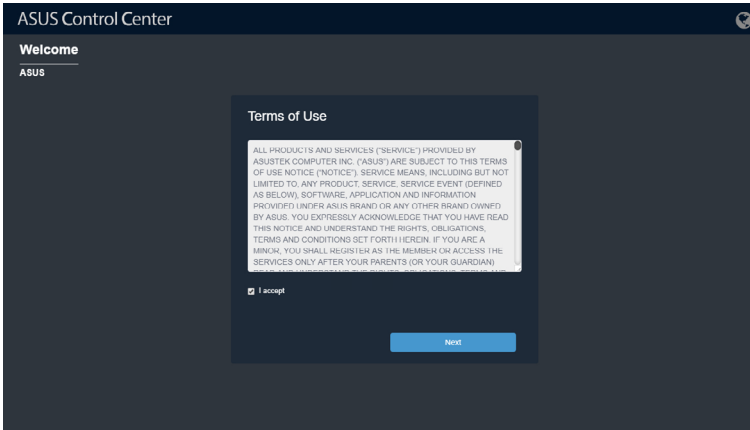
1.3.1 Initialize startup settings

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

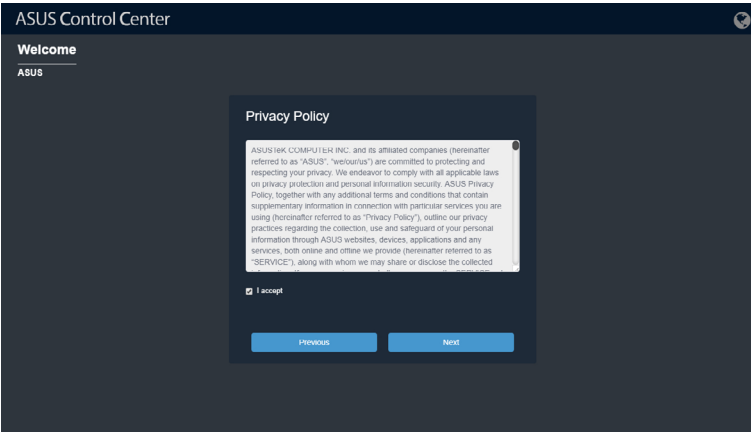


The information entered in this section is for reference only.

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



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



3. Select the **Product Edition**.

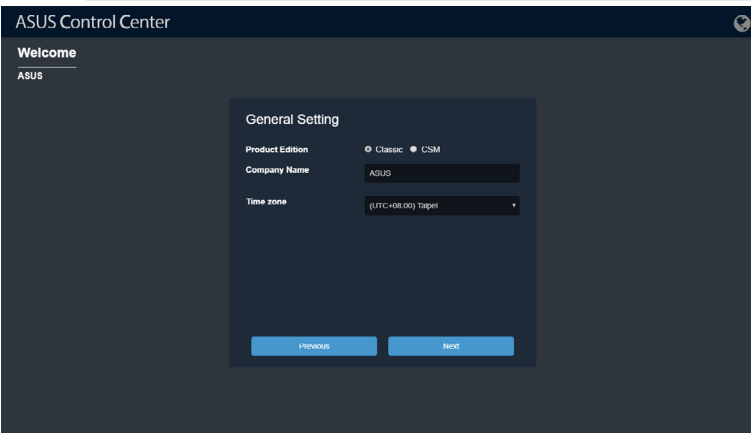


For more information on the CSM version, please visit <https://www.asus.com/microsite/csm/>.

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 Oracle Virtualbox installed.



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.

ASUS Control Center

Welcome
ASUS

Set up the Password

Account Administrator

Password *****

Confirm Password *****

Previous Next

6. 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.

ASUS Control Center

Welcome
ASUS

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

Previous Submit

1.3.2 Logging in to ASUS Control Center



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



To login 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

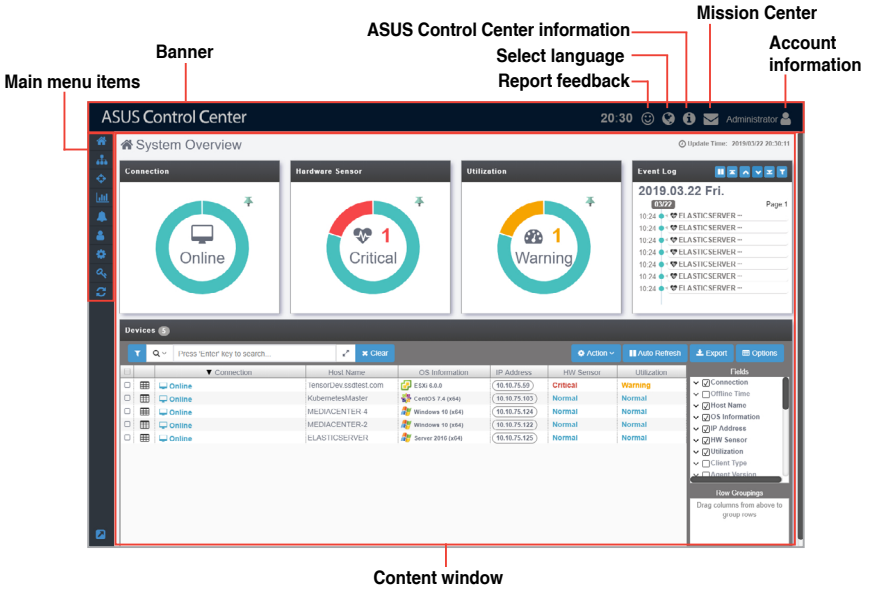


- The ACC in the URL is case sensitive, ensure to use all caps when entering ACC to the URL.
- The export files and import files functions are disabled when using the ACC through VM. For optimal experience, we recommend using an Internet browser installed on the host system to enter the main server URL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

2. Enter your **Account** and **Password**. Click **Login** to enter ASUS Control Center.

1.4 ASUS Control Center layout

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




1.4.1 Banner

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


Logo

You can customize the logo of your ASUS Control Center. For more details on customizing the logo for ASUS Control Center, please refer to **8.3 Appearance Configuration**.


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

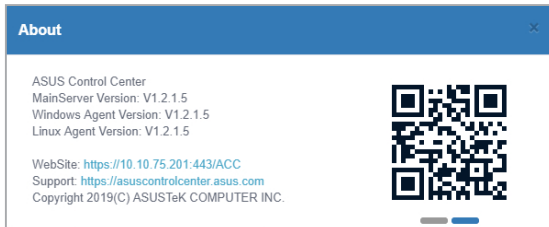
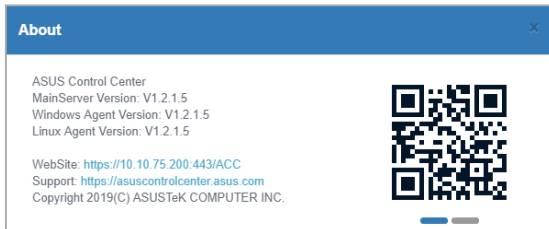
Click  in the top right corner of the banner, then select a language to change the language of ASUS Control Center. The languages currently supported are as follows: English, Traditional Chinese, Simplified Chinese, Japanese, Korean, German, Spanish, French, and Russian.

About


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

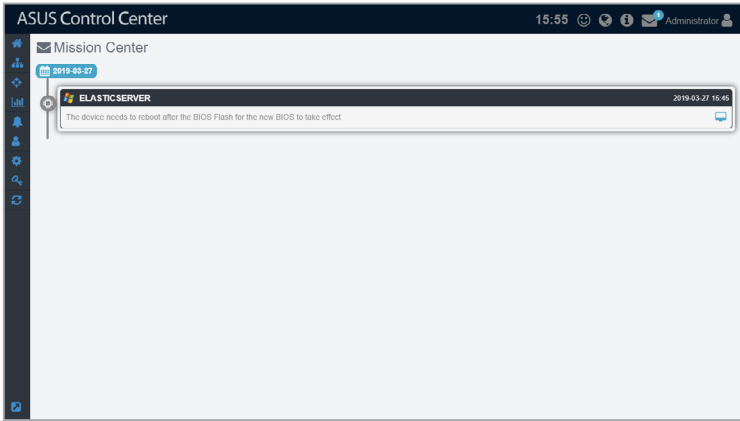


For more information on setting the network configurations for all network cards, please refer to **8.2 Network Configuration**.




Mission Center

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



Account Information

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



For more details on Accounts Management, please refer to **7.2 Accounts Management**.

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 set trust lists or focus lists for these software and receive notifications regarding new software installations.
	Task Report	View the reports for the task status and progress for Software Dispatch, BIOS Dispatch, Agent Update, and Agent Deploy.
Notification	SMTP Settings	Configure SMTP Server settings to send notifications for server alert events
	Rule Management	Setting notification rules for the administrator
	Asset Changes	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.

(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.
	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.
	Sensor Threshold Configuration	Centralized management of sensor threshold values for all managed devices.
	License	
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.

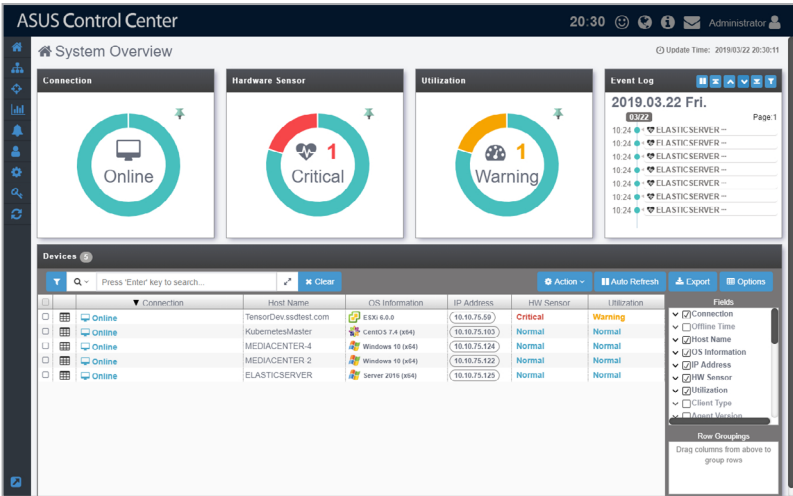
Chapter 2

This chapter describes the various monitoring tools and options available.

2.1 System Overview

The **System Overview** screen gives you a quick overall status check for all managed devices, giving you a basic overview of device status, or event log at a quick 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.



The screenshot displays the ASUS Control Center System Overview interface. At the top, the title bar shows 'ASUS Control Center', the time '20:30', and the user 'Administrator'. The main content area is divided into four panels: 'Connection' (Online), 'Hardware Sensor' (Critical), 'Utilization' (Warning), and 'Event Log' (2019.03.22 Fri.). Below these panels is a 'Devices' table with columns for Connection, Host Name, OS Information, IP Address, HW Sensor, and Utilization. A search bar and various action buttons are also visible.

Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
Online	TensorDevssdtest.com	EVI 6.0.0	10.10.75.59	Critical	Warning
Online	KubermetesMaster	CentOS 7.4 (x84)	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
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	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 or hardware sensor errors at a quick glance.

The screenshot displays the ASUS Control Center interface. At the top, it shows the title 'ASUS Control Center', the time '19:08', and the user 'Administrator'. The main area is titled 'System Overview' and contains four panels:

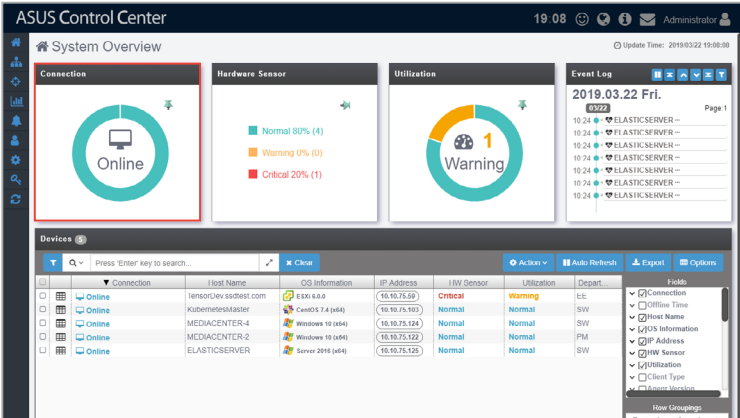
- Connection:** A circular gauge showing 'Online' status.
- Hardware Sensor:** A gauge showing 'Normal 80% (4)', 'Warning 0% (0)', and 'Critical 20% (1)'.
- Utilization:** A gauge showing 'Warning' status with a '1' icon.
- Event Log:** A list of events for '2019.03.22 Fri.' with a 'Page 1' indicator.

Below the overview panels is a 'Devices' section with a search bar and a table of managed devices:

Connection	Host Name	OS Information	IP Address	I/O Sensor	Utilization	Depart.	Fields
Online	sensorDev.ssdtest.com	EEX-6.0.0	10.10.75.59	Critical	Warning	ELC	Connection, Online Time, Host Name, OS Information, IP Address, I/O Sensor, Utilization, Client Type
Online	Kubethe968master	CentOS 7.4 (64)	10.10.75.103	Normal	Normal	SW	
Online	MEDACENTER-4	Windows 10 (64)	10.10.75.124	Normal	Normal	SW	
Online	MEDACENTER-2	Windows 10 (64)	10.10.75.122	Normal	Normal	PM	
Online	ELASTICSERVER	Server 2016 (64)	10.10.75.126	Normal	Normal	SW	

Connection overview

The Connection overview circle displays the connection and power statuses of managed devices in list or graph view. You can click on the ↕ / ↗ to toggle between list and graph view.





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

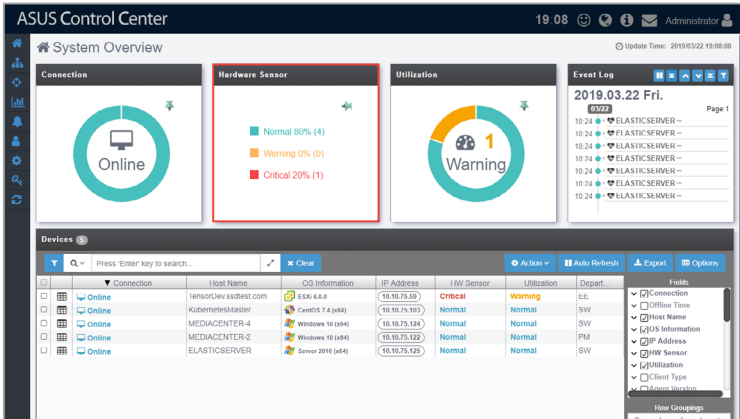
Connection Status	Green	Orange	Red
	Online	Maintain*	Offline



* 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. You can click on the  /  to toggle between list and graph view.

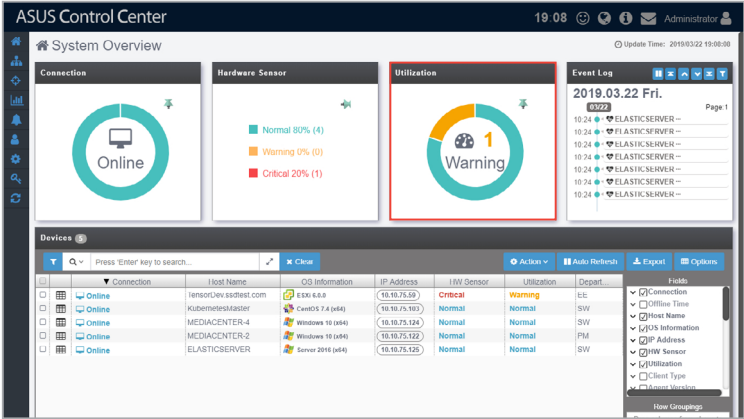


Please refer to the table below for the color status of the Hardware Sensor overview circle

	Green	Orange	Red
Hardware Sensor Status	Normal	Warning	Critical

Utilization overview

The Hardware Sensor overview circle displays an overview of the CPU, DIMM, Partition, and Network statuses of managed devices. You can click on the ↕ / ↕ to toggle between list and graph view.



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

	Green	Orange	Red
Utilization Status	Normal	Warning	Critical







Event Log overview

The **Event Log** displays the log events of ACC and also the Hardware Sensor and Utilization events of all managed devices in real time, keeping you updated on the different status changes of managed devices as they are happening. Clicking on an item on the list will display more details about that item.

The screenshot shows the ASUS Control Center interface. At the top, it displays 'System Overview' with three circular gauges: 'Connection' (Online), 'Hardware Sensor' (Critical), and 'Utilization' (Warning). Below these is a 'Devices' table with columns for Host Name, OS Information, IP Address, HW Sensor, and Utilization. The Event Log panel on the right shows a list of events for '2019.03.22 Fri.' with details like '10:24' and 'ELASTIC SERVER'.

Host Name	OS Information	IP Address	HW Sensor	Utilization
tensor1uv5sdtest.com	ESXi 6.8.0	10.10.75.99	Critical	Warning
KubernetesMaster	CentOS 7.4 (64)	10.10.75.103	Normal	Normal
MELIACENT1EN.4	Windows 10 (64)	10.10.75.124	Normal	Normal
MEDOCENTERS.2	Windows 10 (64)	10.10.75.123	Normal	Normal
ELASTICNODE1ENR	Server 2016 (64)	10.10.75.125	Normal	Normal

Event Log Quick Buttons

-  Pause the Advanced Event Log updates.
-  Jump to the top of the Advanced Event Log list.
-  Scroll up on the Advanced Event Log list.
-  Scroll down on the Advanced Event Log list.
-  Jump to the bottom of the Advanced Event Log list.
-  Filter managed devices in the **Devices** list using the **Advanced Event Log**. Please refer to **2.1.4 Search and Filter devices** section for more information on this function

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 **2.1.4 Search and Filter devices**.

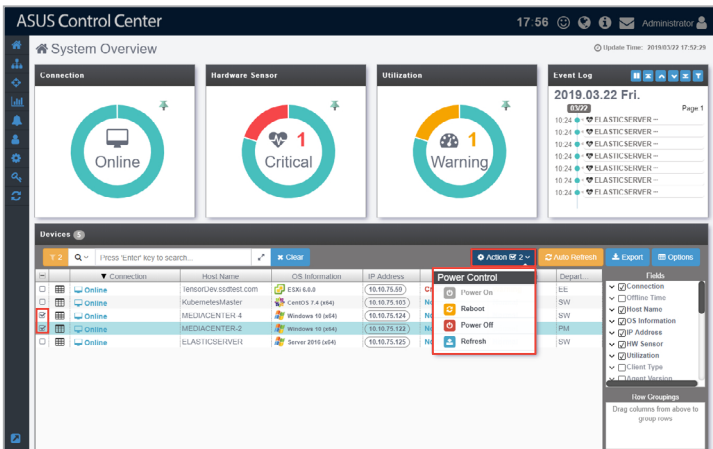
The screenshot shows the ASUS Control Center interface. At the top, there's a 'System Overview' section with three circular gauges: 'Connection' (Online), 'Hardware Sensor' (Critical), and 'Utilization' (Warning). To the right is an 'Event Log' for 2019.03.22 Fri. Below this is the 'Devices' list, which is a table with columns for Connection, Host Name, OS Information, IP Address, HW Sensor, and Utilization. A 'Fields' dropdown menu is open on the right side of the table, showing various metadata items that can be added to the table view.

Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization
Online	INFOFORV560951.com	ESXi 6.0.0	10.10.75.50	Critical	Warning
Online	Kubernetesblade1	CentOS 7.4.1810	10.10.75.55	Normal	Normal
Online	MILLIACN1514 4	Windows 10 19H1	10.10.75.124	Normal	Normal
Online	MEDIACENTER-2	Windows 10 19H1	10.10.75.122	Normal	Normal
Online	ELASTICSERVER	Server 2016 1606	10.10.75.125	Normal	Normal

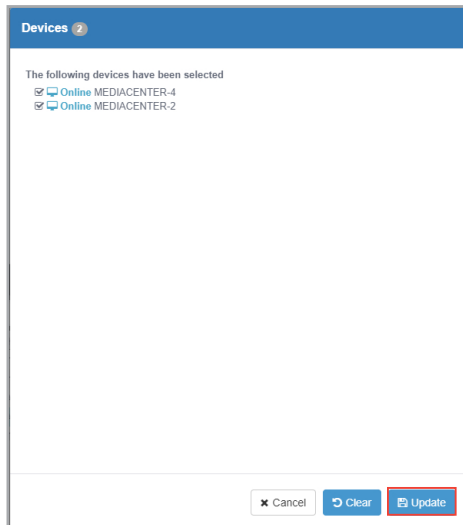
Setting power control (Action)

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

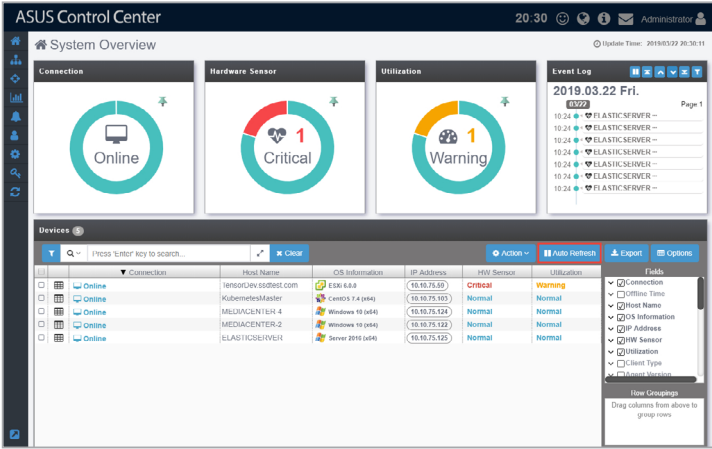


3. Confirm that the correct devices are selected, then click **Update**.



Auto Refreshing the devices list (Auto Refresh)

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

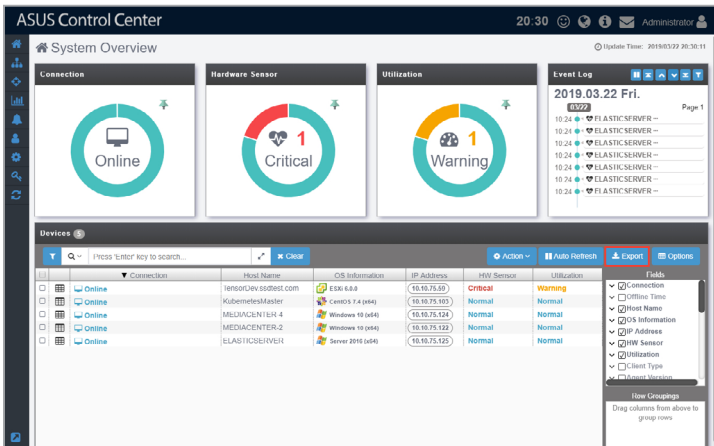


Exporting devices list (Export)

You can export the managed devices and metadata in the **Devices** list to a .csv file by clicking on **Export**.



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



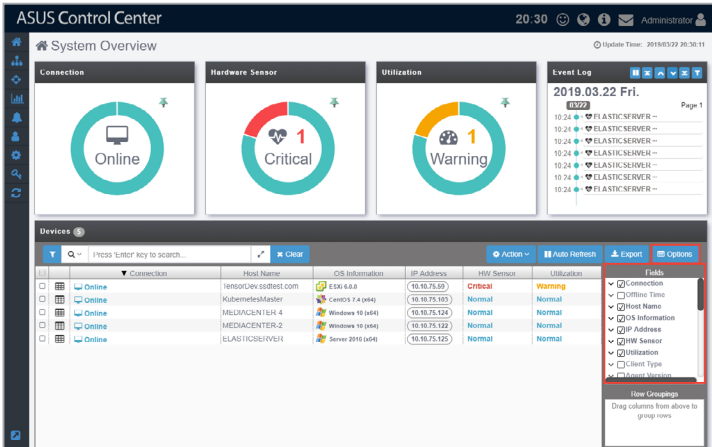
2.1.3 Options

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.

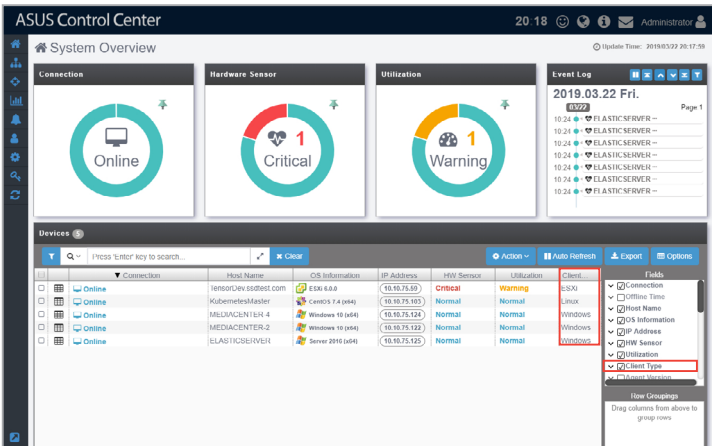
You can sort and group the managed devices in the **Devices** list according to a column criteria using the **Row Groupings** function.

Hiding or displaying metadata fields

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

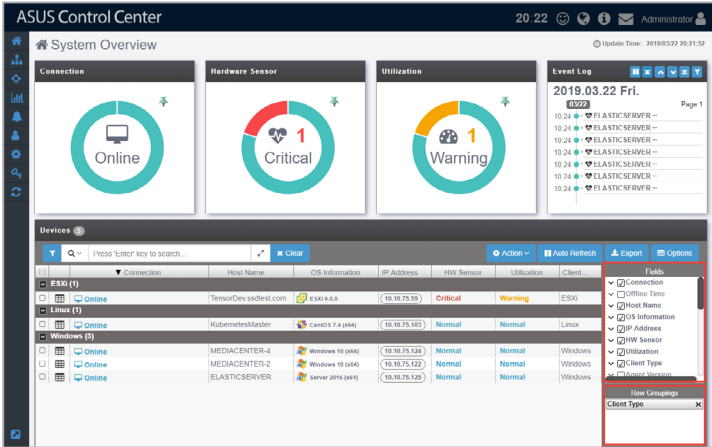


2. You can check the metadata field in the **Fields** window to hide or display the metadata. We check the **Client Type** field in the screenshot below.

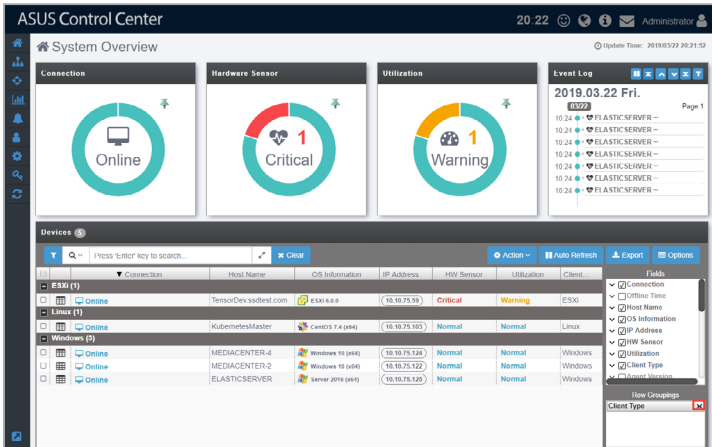


Using the Row Groupings function

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



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



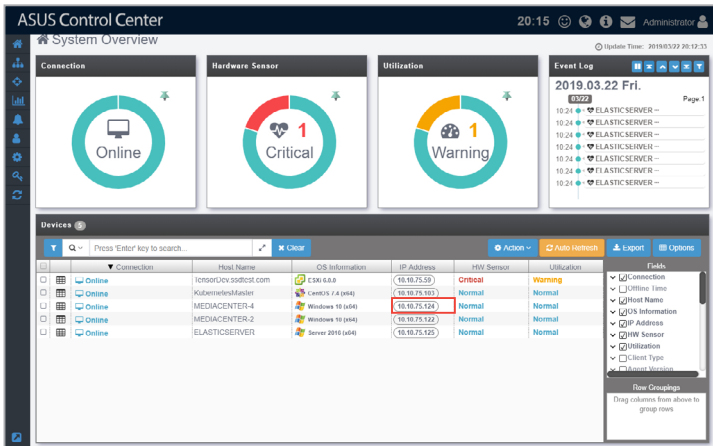
Accessing remote desktop

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

Device operating systems which support remote control:

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

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



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



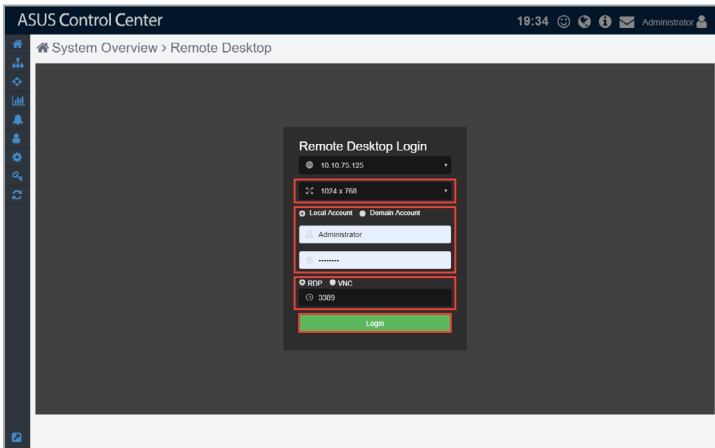
- **Local Account:** The agent's administrator privileges only allow you to manage the device the agent is installed on.
- **Domain Account:** The agent's administrator privileges allow you to manage all devices in the domain. The **Domain** field only appears if you selected **Domain Account**.

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



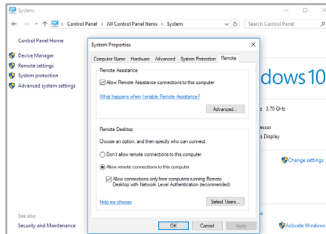
Linux and Windows® systems use different protocols, ensure the managed device is reachable through the selected protocol:

- **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.

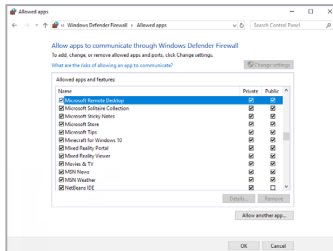




- Ensure the managed device you wish to remote control has a stable power supply and Internet connection.
- The managed device may be remote controlled if it is logged out or locked, but cannot be remote controlled if the managed device is powered off or in sleep mode. If the managed device is in sleep mode, please wake the device using the **Power Control (Wake-on-LAN)** function.
- 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 > Advanced System Settings > Remote**.



- Please ensure that the **Microsoft Remote Desktop** application is enabled in the **Windows Defender Firewall Allowed Apps** list. Search for **Control Panel** in the Windows Search Box, then navigate to **Windows Defender Firewall > Allowed Apps**.



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



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.

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.
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.

Connection	Hardware Sensor	Utilization	Event Log
Online	Critical	Warning	2019.03.22 Fri. 10:24 ELASTIC SERVER -- 10:24 ELASTIC SERVER -- 10:24 ELASTIC SERVER -- 10:24 ELASTIC SERVER -- 10:24 ELASTIC SERVER --

Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization	Depart.	Fields
Online	sensorview.ssd985.com	ESXi 6.6.0	10.10.75.50	Critical	Warning	EE	<input type="checkbox"/> Connection <input type="checkbox"/> Online Time <input type="checkbox"/> Host Name <input type="checkbox"/> OS Information <input checked="" type="checkbox"/> IP Address <input checked="" type="checkbox"/> HW Sensor <input type="checkbox"/> Utilization <input type="checkbox"/> Client Type <input type="checkbox"/> Health Status

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.

The screenshot shows the ASUS Control Center interface. At the top, there's a 'System Overview' section with three circular gauges: 'Connection' (Online), 'Hardware Sensor' (Normal), and 'Utilization' (Normal). To the right is an 'Event Log' for 2019.03.22 Fri. Below this is a 'Devices' section with a search bar containing 'SW Windows ELASTIC' and a 'Clear' button. A dropdown menu is open, showing 'Search with AND operator' (selected) and 'Search with OR operator'. Below the search bar is a table of devices:

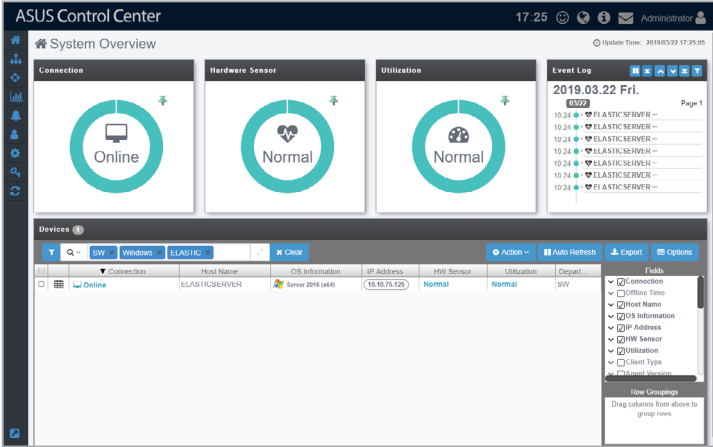
Host Name	OS Information	IP Address	HW Sensor	Utilization	Device
ELASTICSERVER	Server 2016 (x64)	10.10.75.125	Normal	Normal	SW

On the right side of the device list, there are 'Fields' and 'How Groups' options for filtering and grouping the data.

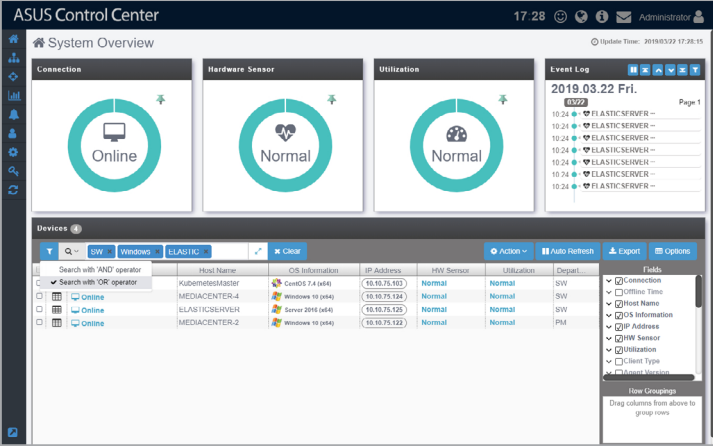
3. (optional) You may also click on to expand the search bar to view or edit your search criteria, or import a .csv file by clicking on **Import**. Click on **Save** once you are finished editing your search criteria.

The screenshot shows a dialog box titled 'Search with AND operator (3 Keywords)'. It has an 'Operator' section with 'AND' selected and 'OR' as an option. Below that is a 'Keywords' section with a text input field containing 'SW Windows ELASTIC'. Below the input field is a 'Keywords' label and a note: 'Press 'Enter' to add a keyword or paste text with ',' (semi-colon) separator. You can also import keywords from the csv file. (Keep place field name in the first line.)' At the bottom, there are three buttons: 'Import', 'Clear', and 'Save'.

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




- Report as a result of selecting the **Search with 'OR' operator** option.

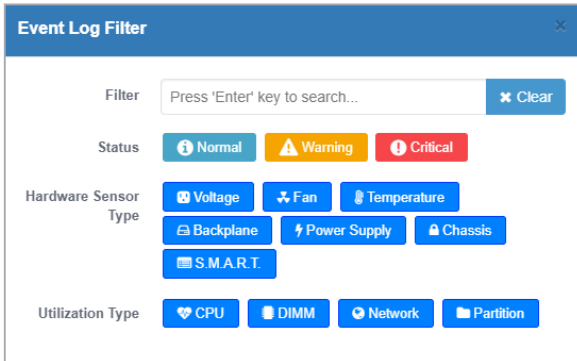


Filter devices using the Advanced Event Log



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

1. Click on  in the top right corner of the **Event Log** block.
2. Enter keywords, or select **Status**, **Hardware Sensor Type**, or **Utilization Type** to add to the filter criteria.




The image shows a screenshot of the 'Event Log Filter' dialog box. It has a blue header with the title 'Event Log Filter' and a close button (X) in the top right corner. Below the header, there are four filter categories, each with a set of buttons:

- Filter:** A search input field with the placeholder text 'Press 'Enter' key to search...' and a 'Clear' button to its right.
- Status:** Three buttons: 'Normal' (blue with an 'i' icon), 'Warning' (yellow with a triangle icon), and 'Critical' (red with a lightning bolt icon).
- Hardware Sensor Type:** Seven buttons: 'Voltage' (blue with a battery icon), 'Fan' (blue with a fan icon), 'Temperature' (blue with a thermometer icon), 'Backplane' (blue with a server rack icon), 'Power Supply' (blue with a lightning bolt icon), 'Chassis' (blue with a server rack icon), and 'S.M.A.R.T.' (blue with a hard drive icon).
- Utilization Type:** Four buttons: 'CPU' (blue with a heart icon), 'DIMM' (blue with a memory stick icon), 'Network' (blue with a globe icon), and 'Partition' (blue with a folder icon).

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  .

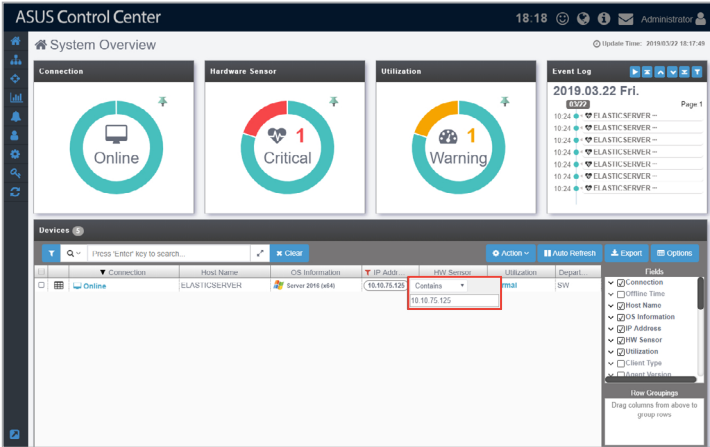


Some column headers may not support the filter function.

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.



The screenshot shows the ASUS Control Center interface. The top navigation bar includes the title 'ASUS Control Center', the time '18:18', and the user 'Administrator'. Below the navigation bar is the 'System Overview' section with four widgets: 'Connection' (Online), 'Hardware Sensor' (Critical), 'Utilization' (Warning), and 'Event Log' (2019.03.22 Fri.). The main area is the 'Devices' table, which has a search bar and a 'Clear' button. The table columns are Connection, Host Name, OS Information, IP Addr, HW Sensor, Utilization, and Depart. A filter is applied to the 'IP Addr' column with the rule 'Contains' and the value '10.10.75.125'. The table shows one device with IP '10.10.75.125' and department 'SW'. A 'Fields' panel on the right allows for selecting additional metadata columns.


Connection	Host Name	OS Information	IP Addr	HW Sensor	Utilization	Depart.
Online	ELASTICSERVER	Server 2014 (x64)	10.10.75.125	Contains	10.10.75.125	SW

2.2 Device Information



The screenshot may vary between agent and agentless devices, for more details on viewing agentless device details, refer to **2.3 Host Information**.

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**.

ASUS Control Center 16:00 Administrator

System Overview > 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

Hardware Sensor, BMC, BIOS, Utilization, Software, Security, Inventory, Event Log, Configuration

The **Device Information** screen will display a photo slide of the device, which you may scroll through by clicking on the tabs below the device photo. The **OS Information**, **BIOS Version**, **Agent Version**, **Model Name**, **IP Address**, **Timezone**, and **Up Time** of the device will also be displayed to the right of the device photo.



- Device photos are only available for ASUS Server, Work Station, and CSM products.
- 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 **2.1.4 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 **2.1.3 Options**.

Device Statuses and Quick Buttons



Connection status:

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



Message status:

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



The Message status is only available on BMC enabled devices.



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 is 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 **2.1.3 Devices list** 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.



Refresh:

This item will refresh 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.








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.

ASUS Control Center 14:38 Administrator

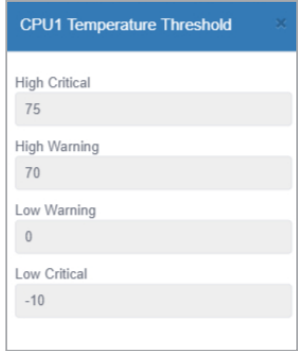
System Overview > ELASTICSERVER > Hardware Sensor Update Time: 2019-03-26 14:37:48

- Voltage**
- Temperature**
 - CPU1 Temperature: Normal, 47 °C
 - CPU2 Temperature: Normal, 47 °C
 - PSU1 Over Temp: Normal, Transition to OK
- Fan**
 - FRONT_FAN1: Normal, 1100 rpm
 - FRONT_FAN2: Normal, 3500 rpm
 - FRONT_FAN3: Normal, 1200 rpm
 - PSU1 Slow FAN1: Normal, Transition to OK
 - PSU1 Slow FAN2: Normal, Transition to OK
- Backplane**
- Power Supply**
 - PMPower: Normal, 60 Watt
 - PSU1 AC Lost: Normal, Presence Detected
 - PSU1 PWR Detect: Normal, Presence Detected
- S.M.A.R.T.**

Quick Buttons

-  Click to switch the layout view.
-  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.



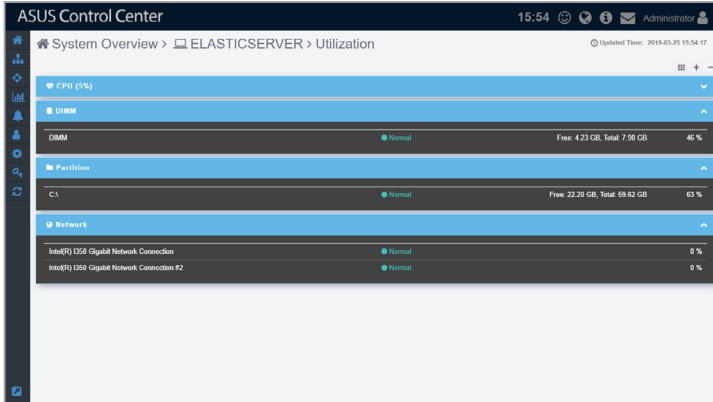
High Critical	If the sensor value is equal to or exceeds this value the sensor status will be Critical . For the above example, if the sensor value is 75 or higher, the sensor status will be Critical .
High Warning	If the sensor value is equal to or exceeds this value, and below the High Critical value 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 .

2.2.2 Utilization






This item allows you to view 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.



Quick Buttons

-  Click to switch the layout view.
-  Click to expand all blocks.
-  Click to minimize all blocks.
-  Click to expand this block.
-  Click to minimize this block.

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**.



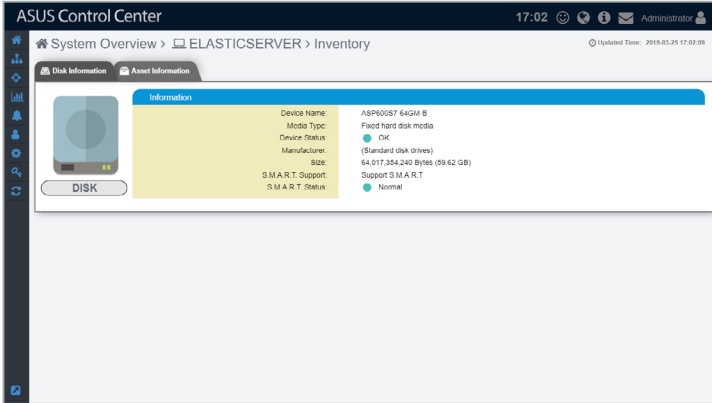
The threshold options for each item may vary.

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

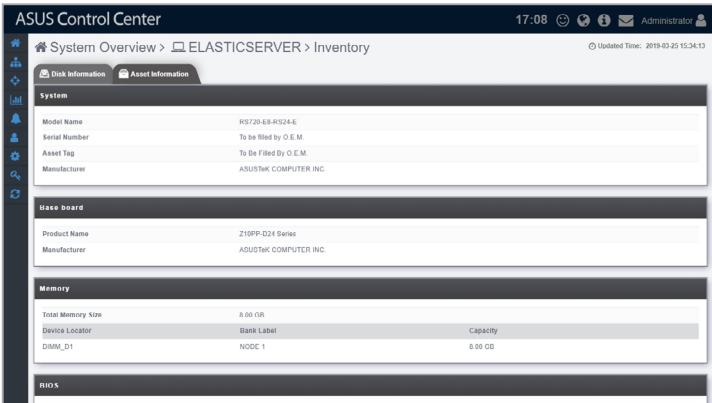
Memory Utilization Threshold			
High Critical	-	95	+
High Warning	-	90	+
Save			

2.2.3 Inventory

This item displays more details about your managed device and disk. Click on **Disk Information** for more details on disks installed on the managed device, such as CD ROM drives, hard disk drives, and USB drives.



Click on **Asset Information** for the **System**, **Base Board**, **Memory**, **BIOS**, **Processor**, and **Network Adapter** details on the managed device.



2.2.4 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.

The screenshot shows the ASUS Control Center interface for a device named ELASTICSERVER. The main section is titled 'BMC' and contains the following information:

BMC Model Name	ASMB00-01VM
Version	1.14
SEL Number	9
Card Type	Onboard
Flash Type	Aspeed 2100

Below the BMC section, there are two tabs: 'Shared LAN' and 'DM_LAN'. The 'Shared LAN' tab is active and shows the following network configuration:

IP Address	10.10.75.104
IP Source	DHCP
MAC Address	2C:56:DC:88: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

Shared LAN	DM_LAN1
IP Address	10.10.75.104
IP Source	DHCP
MAC Address	2C:56:DC:0B:DA:3E
Subnet Mask	255.255.255.0
Default Gateway	10.10.75.1

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

Shared LAN	DM_LAN1
IP Address	0.0.0.0
IP Source	DHCP
MAC Address	2C:56:DC:0B:DA:3D
Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0

2. Login ASMB.


ASMB8 IKVM

ASMB8 v1.0.0.0

Username:

Password: [Forgot Password?](#)

Required Browser Settings

1. Allow popups from this site
2. Allow file download from this site (Help by )
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.

2.2.5 Software

This item displays details on the software and applications with the **Application**, **Services**, **Processes**, and **Environment Variables** 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
ACC Windows Agent	1.2.1.4.1	ASUS	2019-03-26
Teams Machine Wide Installer	1.2.0.3961	Microsoft Corporation	2019-03-12
Google Update Helper	1.3.33.23	Google Inc.	2018-12-20
Office 16 Click-to-Run Extensibility Component	16.0.11328.20158	Microsoft Corporation	2019-03-20
Office 16 Click-to-Run Localization Component	16.0.11328.20158	Microsoft Corporation	2019-03-20
Adobe Acrobat Reader DC	19.016.20698	Adobe Systems Incorporated	2019-03-11
Realtek High Definition Audio Driver	6.0.1.7926	Realtek Semiconductor Corp.	2019-03-05
HeavyLoad V3.4 (64 bit)	3.4	JAM Software	2019-03-22
Microsoft Office 365 管理控制台 - zh-tw	16.0.11328.20158	Microsoft Corporation	2019-03-12
Google Chrome	73.0.3683.86	Google, Inc.	2018-11-05
7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	2019-03-26
Office 16 Click-to-Run Licensing Component	16.0.11328.20158	Microsoft Corporation	2019-03-20
Office 16 Click-to-Run Extensibility Component 64-bit Registration	16.0.11328.20158	Microsoft Corporation	2019-03-20

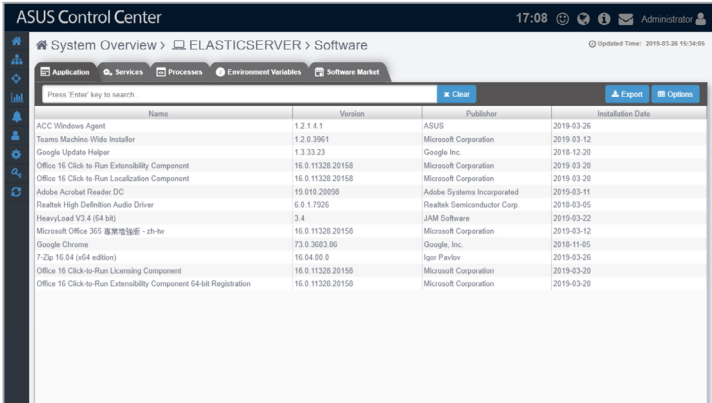
For Linux system:

Name	Version	Publisher	Installation Date
libwrap	0.3.0	CentOS	2018-01-02
satyr	0.13	CentOS	2017-07-31
gpg-pubkey	362c6465	(none)	2017-07-31
webkitgtk-plugin-process-gtk2	2.16.7	CentOS	2018-01-02
atomic-registry	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
libcurl	2.4.2	CentOS	2018-01-02
boom3dscan	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
sc-utils	20130529	CentOS	2018-01-02
pciutils	10.23	CentOS	2018-01-02
org.freedesktop.Type1	7.5	CentOS	2017-07-31
automake	1.13.4	CentOS	2017-08-01
webkitgtk3	2.4.11	CentOS	2018-01-02
lib7265-firmware	22.0.7.0	CentOS	2018-01-02
cryptsetup-luks	1.7.4	CentOS	2018-01-02
bcqtp-tools	1.0.17	CentOS	2017-07-31
libreport-devel	0.9.9	CentOS	2017-08-01

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®.

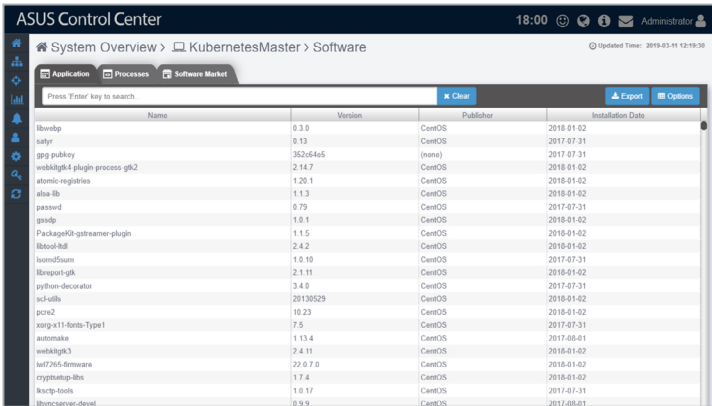
For Windows® system:



The screenshot shows the ASUS Control Center interface for a Windows system. The breadcrumb navigation is 'System Overview > ELASTICSERVER > Software'. The 'Application' tab is selected. A search bar contains the text 'Press Enter key to search'. Below the search bar is a table listing installed applications with columns for Name, Version, Publisher, and Installation Date.

Name	Version	Publisher	Installation Date
ACC Windows Agent	1.2.1.4.1	ASUS	2019-03-26
Teams Machine Wide Installer	1.2.0.3961	Microsoft Corporation	2019-03-12
Google Update Helper	1.3.33.23	Google Inc.	2018-12-20
Office 16 Click-to-Run Extensibility Component	16.0.11328.20150	Microsoft Corporation	2019-03-20
Office 16 Click-to-Run Localization Component	16.0.11328.20150	Microsoft Corporation	2019-03-20
Adobe Acrobat Reader DC	19.019.20090	Adobe Systems Incorporated	2019-03-11
Realtek High Definition Audio Driver	6.0.1.7526	Realtek Semiconductor Corp.	2019-03-05
HeavyLoad V3.4 (64 bit)	3.4	JAM Software	2019-03-22
Microsoft Office 365 繁體中文 - zh-tw	16.0.11328.20150	Microsoft Corporation	2019-03-12
Google Chrome	73.0.3603.90	Google, Inc.	2018-11-05
7-Zip 16.04 (x64 edition)	16.04.00.0	Igor Pavlov	2019-03-26
Office 16 Click-to-Run Extensibility Component	16.0.11328.20150	Microsoft Corporation	2019-03-20
Office 16 Click-to-Run Extensibility Component 64-bit Registration	16.0.11328.20150	Microsoft Corporation	2019-03-20

For Linux system:



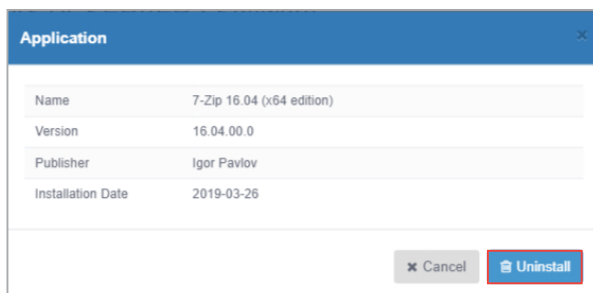
The screenshot shows the ASUS Control Center interface for a Linux system. The breadcrumb navigation is 'System Overview > KubernetesMaster > Software'. The 'Software Market' tab is selected. A search bar contains the text 'Press Enter key to search'. Below the search bar is a table listing installed applications with columns for Name, Version, Publisher, and Installation Date.

Name	Version	Publisher	Installation Date
libwvloop	0.3.0	CentOS	2018-01-02
rsync	0.13	CentOS	2017-07-31
gpg pubkey	352c6465	(none)	2017-07-31
wobblygk4 plugin process gk2	2.14.7	CentOS	2018-01-02
atomic-registry	1.20.1	CentOS	2018-01-02
alsa-lib	1.1.3	CentOS	2018-01-02
passwd	0.79	CentOS	2017-07-31
gnupg	16.1	CentOS	2018-01-02
PackageKit-gstreamer-plugin	1.1.5	CentOS	2018-01-02
libtool-ltd	2.4.2	CentOS	2018-01-02
lua52sum	1.0.10	CentOS	2017-07-31
librepo-gtk	2.1.11	CentOS	2018-01-02
python-decorator	3.4.0	CentOS	2017-07-31
rsync	2013029	CentOS	2018-01-02
pcsc2	10.23	CentOS	2018-01-02
xorg-x11-fonts-Type1	7.5	CentOS	2017-07-31
automake	1.13.4	CentOS	2017-08-01
wobblygk3	2.4.11	CentOS	2018-01-02
rsync-ssh-key	20.0.17.0	CentOS	2018-01-02
cryptsetup-libs	1.7.4	CentOS	2018-01-02
rsync-tools	1.0.17	CentOS	2017-07-31
libunc-sscanf-devel	0.9.8	CentOS	2017-08-01

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

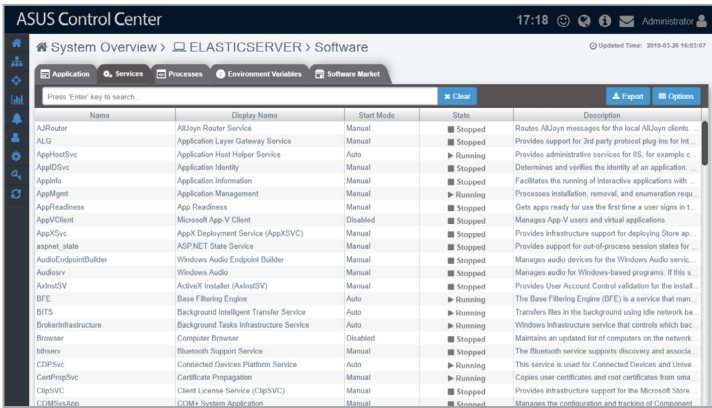


- Uninstalling applications using the **Application** tab is disabled on Linux systems.
- The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.



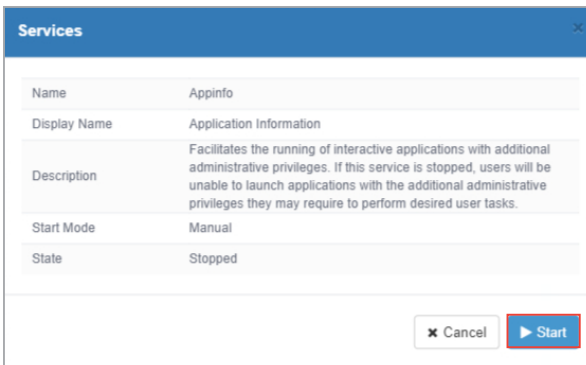
Services (Windows only)

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
ALRouter	ALJyn Router Service	Manual	■ Stopped	Routes ALJyn messages for the local ALJyn clients.
ALG	Application Layer Gateway Service	Manual	■ Stopped	Provides support for 3rd party protocol plug-ins for Int...
AppHostSvc	Application Host Helper Service	Auto	▶ Running	Provides administrative services for IIS, for example c...
AppIDSvc	Application Identity	Manual	■ Stopped	Determines and verifies the identity of an applicatio...
Appinfo	Application Information	Manual	■ Stopped	Facilitates the running of interactive applications with...
AppMgmt	Application Management	Manual	▶ Running	Processes installation, removal, and enumeration requ...
AppReadiness	App Readiness	Manual	■ Stopped	Gets apps ready for use the first time a user signs in t...
AppXClient	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 ap...
asnet_state	ASP.NET State Service	Manual	■ Stopped	Provides support for out-of-process session states for...
AudioEndpointBuilder	Windows Audio Endpoint Builder	Manual	■ Stopped	Manages audio devices for the Windows Audio servic...
AudioSvc	Windows Audio	Manual	■ Stopped	Manages audio for Windows-based programs. If this s...
ActiveSV	ActiveX Installer (ActiveSV)	Manual	■ Stopped	Provides User Account Control validation for the instal...
BFE	Base Filtering Engine	Auto	▶ Running	The Base Filtering Engine (BFE) is a service that man...
BITS	Background Intelligent Transfer Service	Auto	▶ Running	Transfers files in the background using idle network ba...
BrokerInfrastructure	Background Tasks Infrastructure Service	Auto	▶ Running	Windows infrastructure services that controls which bac...
Browser	Computer Browser	Disabled	■ Stopped	Maintains an updated list of computers on the network...
btssrv	Bluetooth Support Service	Manual	■ Stopped	The Bluetooth service supports discovery and associa...
CDPSvc	Connected Devices Platform Service	Auto	▶ Running	This service is used for Connected Devices and Drive...
CertPropSvc	Certificate Propagation	Manual	▶ Running	Copies user certificates and root certificates from sma...
ClpSvc	Client License Service (ClpSvc)	Manual	■ Stopped	Provides infrastructure support for the Microsoft Store...
COMSysApp	COM+ System Application	Manual	■ Stopped	Manages the configuration and tracking of Component...

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**.



Services	
Name	Appinfo
Display Name	Application Information
Description	Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks.
Start Mode	Manual
State	Stopped

✖ Cancel **▶ Start**

Processes

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

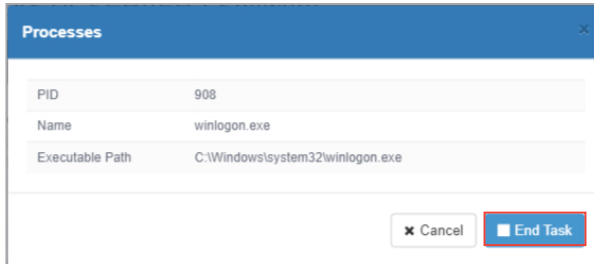
For Windows® system:

PID	Name	Executable Path
0	System Idle Process	
4	System	
628	smss.exe	
748	csrss.exe	
816	wininit.exe	
824	csrss.exe	
908	winlogon.exe	C:\Windows\system32\winlogon.exe
936	services.exe	
952	lsass.exe	C:\Windows\system32\lsass.exe
106	svchost.exe	C:\Windows\system32\svchost.exe
680	svchost.exe	C:\Windows\system32\svchost.exe
1036	svchost.exe	C:\Windows\system32\svchost.exe
1064	LogonUI.exe	C:\Windows\system32\LogonUI.exe
1072	dmn.exe	C:\Windows\system32\dmn.exe
1084	svchost.exe	C:\Windows\system32\svchost.exe
1112	svchost.exe	C:\Windows\system32\svchost.exe
1256	svchost.exe	C:\Windows\system32\svchost.exe
1292	svchost.exe	C:\Windows\system32\svchost.exe
1300	svchost.exe	C:\Windows\system32\svchost.exe
1476	svchost.exe	C:\Windows\system32\svchost.exe
1488	svchost.exe	C:\Windows\system32\svchost.exe
2708	csrss.exe	C:\Windows\system32\csrss.exe

For Linux system:

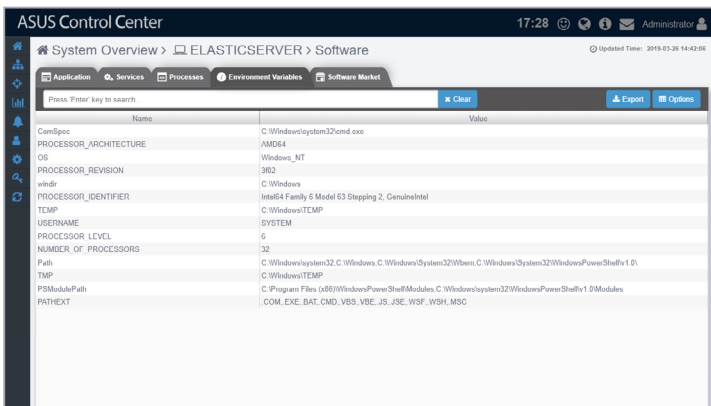
PID	Name	Executable Path
1	/usr/sbin/systemd/systemd	
2	[kthreadd]	
3	[ksoftirqd]	
5	[kworker/0:0H]	
8	[migration/0]	
9	[rcu_bh]	
10	[rcu_sched]	
11	[watchdog/0]	
12	[watchdog/1]	
13	[migration/1]	
14	[ksoftirqd/1]	
16	[kworker/1:0H]	
17	[watchdog/2]	
18	[migration/2]	
19	[ksoftirqd/2]	
21	[kworker/2:0H]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

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



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.



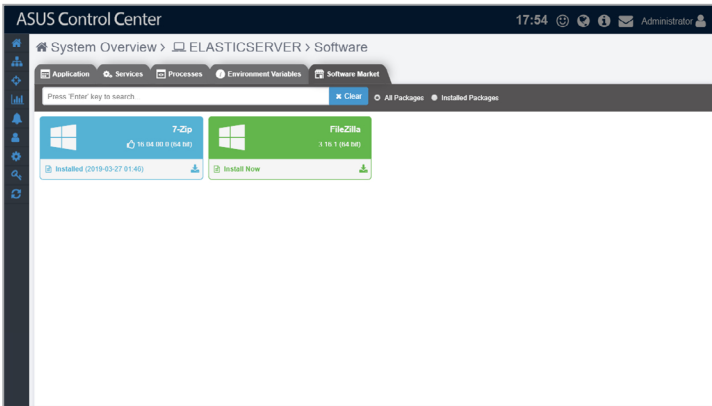
Software Market

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.

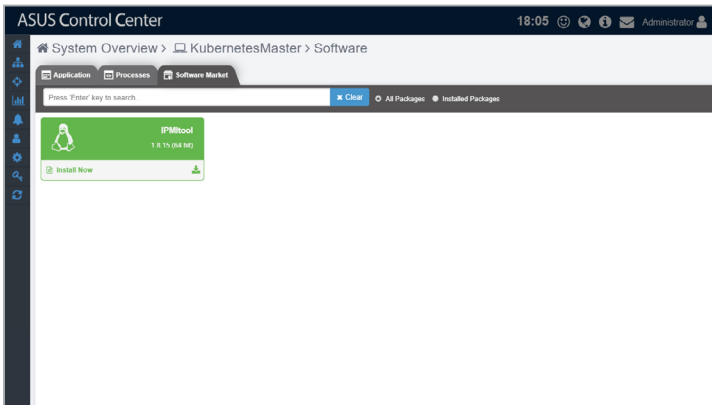


Refer to **4.4.1 Software Pool** for more information on adding and removing software packages from the software pool.

For Windows® system:



For Linux system:



2.2.6 Event Log

This item displays the event logs for the **ASUS Control Center**, **Application**, **System**, and **Security**. 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**.
- Linux systems only support the **ASUS Control Center** tab.

For Windows® system:

Level Type	Date & Time	Message
Normal	2019-03-16 10:31:28	Software dispatch task done.
Normal	2019-03-11 11:56:06	Software dispatch task done.
Normal	2019-03-11 11:56:43	CPU Core ID: 27 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 26 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 25 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 24 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 23 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 22 Utilization: 1 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 21 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 20 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 19 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 17 Utilization: 3 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 16 Utilization: 1 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 16 Utilization: 0 % Status: Critical -> Normal

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 04:46:55	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 04:39:36	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: 60 % Status: Warning -> Normal
Warning	2019-10-24 04:34:26	CPU Core ID: 1 Utilization: 91 % Status: Normal -> Warning
Normal	2019-10-24 04:30:54	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 04:30:50	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

ASUS Control Center tab

ASUS Control Center System Overview > ELASTICSERVER > Event Log

Updated Time: 2019-03-29 18:30:30

Normal: 50, Warning: 30, Critical: 47

Level Type	Date & Time	Message
Normal	2019-03-18 10:31:28	Software dispatch task done.
Normal	2019-03-11 12:16:06	Software dispatch task done.
Normal	2019-03-11 11:56:43	CPU Core ID: 27 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 26 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 25 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 24 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 23 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 22 Utilization: 1 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 21 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 20 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 19 Utilization: 0 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 18 Utilization: 3 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 17 Utilization: 1 % Status: Critical -> Normal
Normal	2019-03-11 11:56:43	CPU Core ID: 16 Utilization: 5 % Status: Critical -> Normal

Application tab (Windows only)

ASUS Control Center System Overview > ELASTICSERVER > Event Log

Updated Time: 2019-03-29 18:30:33

Normal: 943, Warning: 4, Critical: 53

Level Type	Date & Time	Source	Message
Normal	2019-03-20 10:43:48	Software Protection Platform Se...	SLUI.exe was launched with the following command-line parameters: /ui010-3167/164...
Normal	2019-03-20 10:48:53	Software Protection Platform Se...	The Software Protection service has completed licensing status check Application IDs...
Normal	2019-03-20 10:48:52	Software Protection Platform Se...	Initialization status for service objects C:\Windows\system32\upppwmsvc.dll, mott.spwv...
Normal	2019-03-20 15:48:52	Software Protection Platform Se...	The Software Protection service is starting. Parameters: /trigger:timer;sessionid=0
Normal	2019-03-20 14:50:31	Desktop Window Manager	The Desktop Window Manager has registered the session port.
Normal	2019-03-20 14:46:59	Desktop Window Manager	The Desktop Window Manager has registered the session port.
Normal	2019-03-20 11:28:52	Software Protection Platform Se...	Successfully scheduled Software Protection service for re-start at 2019-03-20T07:48...
Normal	2019-03-20 11:08:22	MailInstaller	Windows installer reconfigured the product. Product Name: ACC Windows Agent. Pro...
Normal	2019-03-20 11:08:22	MailInstaller	Windows installer reconfigured the product. Product Name: Google Update Helper. Pr...
Normal	2019-03-20 11:08:22	MailInstaller	Windows installer reconfigured the product. Product Name: 7-Zip 16.01 (x64 edition)...
Normal	2019-03-20 11:08:22	MailInstaller	Windows installer reconfigured the product. Product Name: Plo2016 MUI Installer. Pro...
Normal	2019-03-20 11:08:21	MailInstaller	Windows installer reconfigured the product. Product Name: Google Chrome. Product...
Normal	2019-03-20 11:08:21	MailInstaller	Windows installer reconfigured the product. Product Name: Adobe Acrobat Reader D...
Normal	2019-03-20 11:08:21	MailInstaller	Windows installer reconfigured the product. Product Name: Teams Machine Wide Ins...

System tab (Windows only)

ASUS Control Center | 18:33 | Administrator

System Overview > ELASTICSERVER > Event Log | Updated Time: 2019-03-20 15:34:02

ASUS Control Center | Application | System | Security

996 Normal | **2** Warning | **2** Critical

Logs (996)

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

Level/Type	Date & Time	Source	Message
Normal	2019-03-20 14:34:06	Service Control Manager	The Function Discovery Provider Host service entered the stopped state.
Normal	2019-03-20 14:32:07	Service Control Manager	The Device Association Service service entered the stopped state.
Normal	2019-03-20 14:31:24	Service Control Manager	The Device Setup Manager service entered the stopped state.
Normal	2019-03-20 14:30:35	Service Control Manager	The Device Association Service service entered the running state.
Normal	2019-03-20 14:30:35	Service Control Manager	The Device Setup Manager service entered the running state.
Normal	2019-03-20 14:30:31	Service Control Manager	The Smart Card Device Enumeration Service service entered the running state.
Normal	2019-03-20 14:30:20	Service Control Manager	The Smart Card Device Enumeration Service service entered the stopped state.
Normal	2019-03-20 14:30:01	Service Control Manager	The Device Association Service service entered the stopped state.
Normal	2019-03-20 14:30:30	Service Control Manager	The Device Association Service service entered the running state.
Normal	2019-03-20 14:17:51	Service Control Manager	The Device Association Service service entered the stopped state.
Normal	2019-03-20 14:46:59	Service Control Manager	The Device Setup Manager service entered the stopped state.
Normal	2019-03-20 14:46:19	Service Control Manager	The Device Association Service service entered the running state.
Normal	2019-03-20 14:46:16	Service Control Manager	The Function Discovery Provider Host service entered the running state.
Normal	2019-03-20 14:46:11	Microsoft Windows Kernel Gen...	The description for Event ID '16' in Source 'Microsoft Windows Kernel Generat...

Security tab (Windows only)

ASUS Control Center | 18:34 | Administrator

System Overview > ELASTICSERVER > Event Log | Updated Time: 2019-03-20 15:29:03

ASUS Control Center | Application | System | Security

1,000 Security audit is successful. | **0** Security audit failed.

Logs (1000)

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

Level/Type	Date & Time	Message
Security audit is successful.	2019-03-20 15:29:28	Special privileges assigned to new logon Subject: Security ID: S-1-5-18 Account Name: SY...
Security audit is successful.	2019-03-20 15:28:28	An account was successfully logged on Subject: Security ID: S-1-5-18 Account Name: ELA...
Security audit is successful.	2019-03-20 15:17:41	Special privileges assigned to new logon Subject: Security ID: S-1-5-18 Account Name: SY...
Security audit is successful.	2019-03-20 15:57:41	An account was successfully logged on Subject: Security ID: S-1-5-18 Account Name: ELA...
Security audit is successful.	2019-03-20 14:52:06	A user's local group membership was enumerated Subject: Security ID: S-1-5-21-2208400...
Security audit is successful.	2019-03-20 14:50:35	A user's local group membership was enumerated Subject: Security ID: S-1-5-21-2208400...
Security audit is successful.	2019-03-20 14:50:32	An account was logged off Subject: Security ID: S-1-5-90-0-3 Account Name: DVM-3 Acco...
Security audit is successful.	2019-03-20 14:50:32	An account was logged off Subject: Security ID: S-1-5-21-229840001-2305067423-66910...
Security audit is successful.	2019-03-20 14:50:31	Special privileges assigned to new logon Subject: Security ID: S-1-5-21-229840001-23993...
Security audit is successful.	2019-03-20 14:50:31	An account was successfully logged on Subject: Security ID: S-1-5-18 Account Name: ELA...
Security audit is successful.	2019-03-20 14:50:31	A logon was attempted using explicit credentials Subject: Security ID: S-1-5-18 Account Na...
Security audit is successful.	2019-03-20 14:50:31	The computer attempted to validate the credentials for an account Authentication Package...
Security audit is successful.	2019-03-20 14:50:31	A user's local group membership was enumerated Subject: Security ID: S-1-5-18 Account ...

Filtering the Event Log using the 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

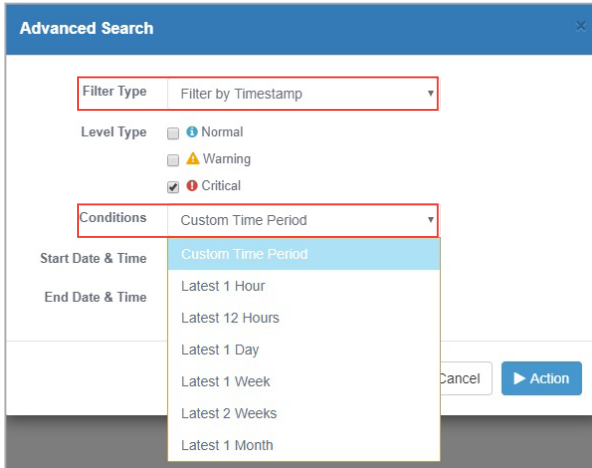
Filter Type Filter by total records

Level Type Normal
 Warning
 Critical

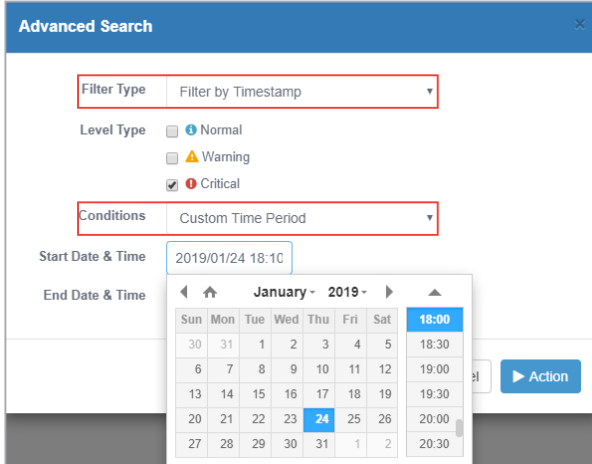
Conditions Latest 100 Records

Cancel Action

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



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



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	2019-05-11 11:26:41	CPU Core ID: 27 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 28 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 29 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 24 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 23 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 22 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 21 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 20 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 19 Utilization: 94 % Status: Normal -> Warning
Warning	2019-05-11 11:26:41	CPU Core ID: 18 Utilization: 94 % Status: Normal -> Warning

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

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

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.

ASUS Control Center

System Overview > MEDIACENTER-2 > BIOS

16:12 Administrator

BIOS Flash BIOS Settings DMI Info

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	06/06/2017

BIOS Flash Information

BIOS Flash Type: Manually Upload BIOS File

Upload BIOS

Drop BIOS File Here
or Click Upload BIOS File

Upload BIOS File

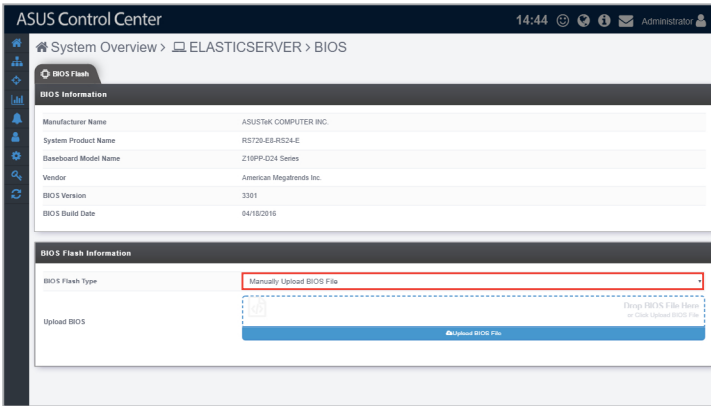
BIOS Flash

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.

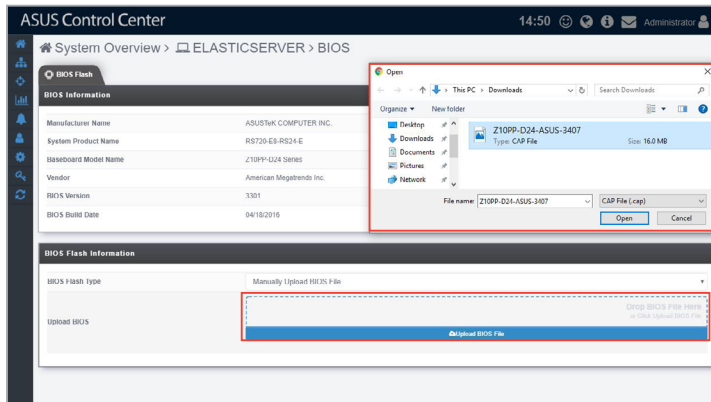
1. You can upload or select your BIOS cap file using the following methods:
 - **Manually uploading BIOS cap file**
 - a. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.



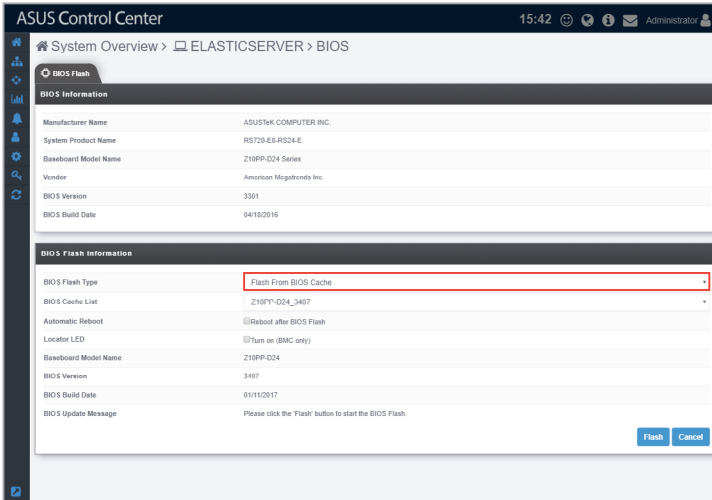
- b. Click on **Upload BIOS File** to select a BIOS cap file, or drag the BIOS cap file into the dotted square.



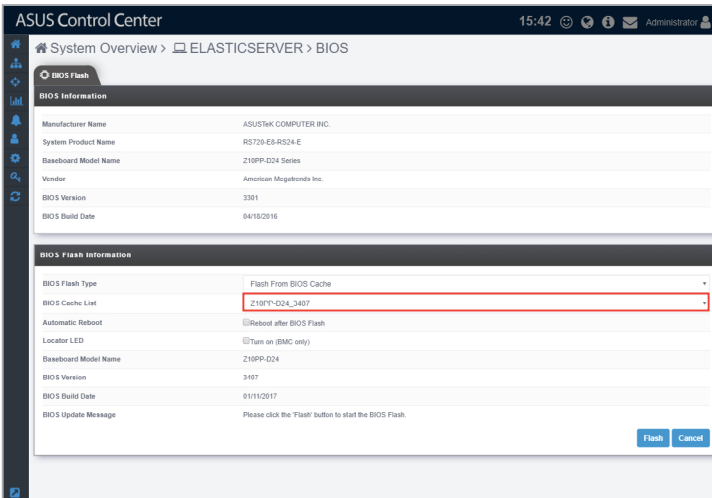
The uploaded BIOS cap file will automatically be added to the **BIOS Cache**.



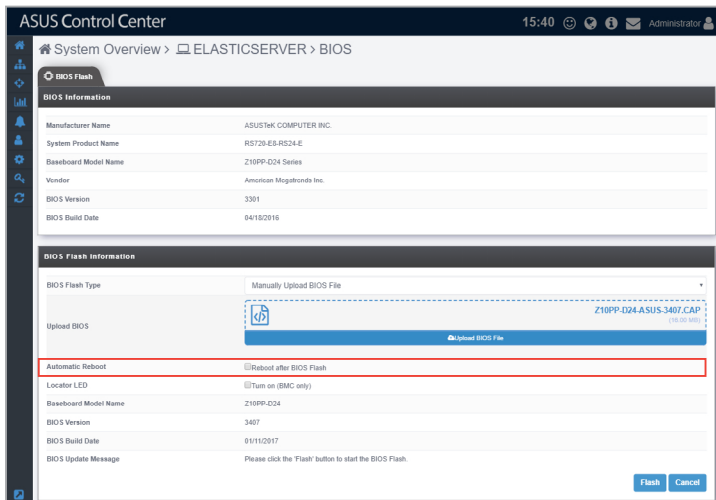
- **Selecting BIOS cap file from the BIOS Cache**
 - a. Select **Flash From BIOS Cache** in the **BIOS Flash Type** field.



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



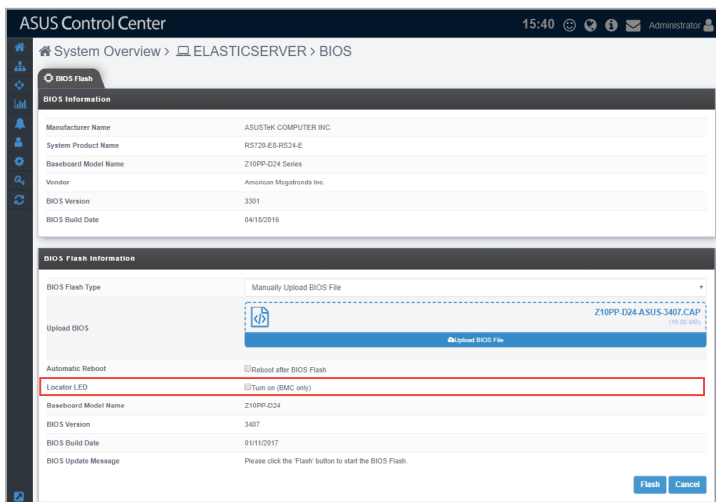
- (optional) You may check the **Reboot after BIOS Flash** checkbox in the **Automatic Reboot** field to automatically reboot the device after BIOS has been flashed.



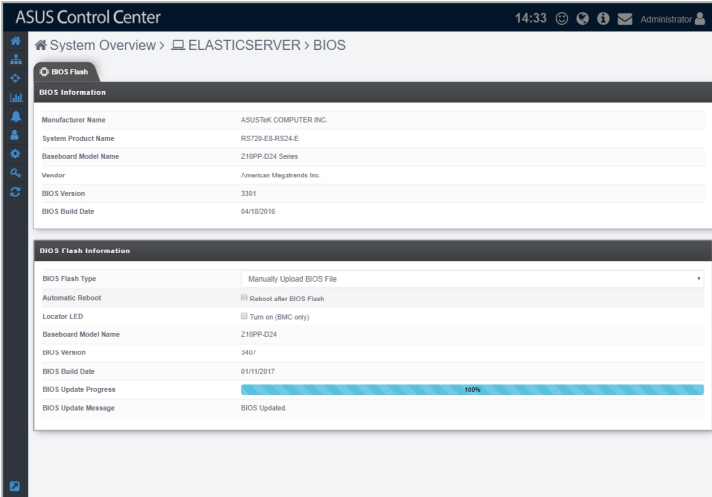
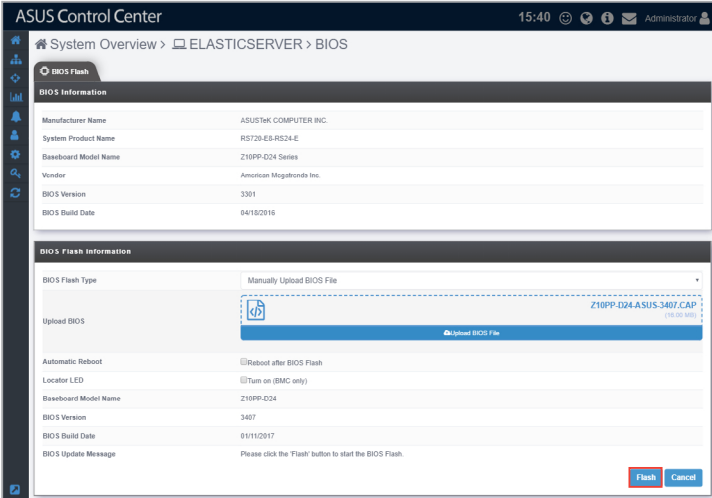
- (optional) You may check the **Turn On(BMC only)** checkbox in the **Locator LED** field to turn on the Locator LED once BIOS Flash is completed.



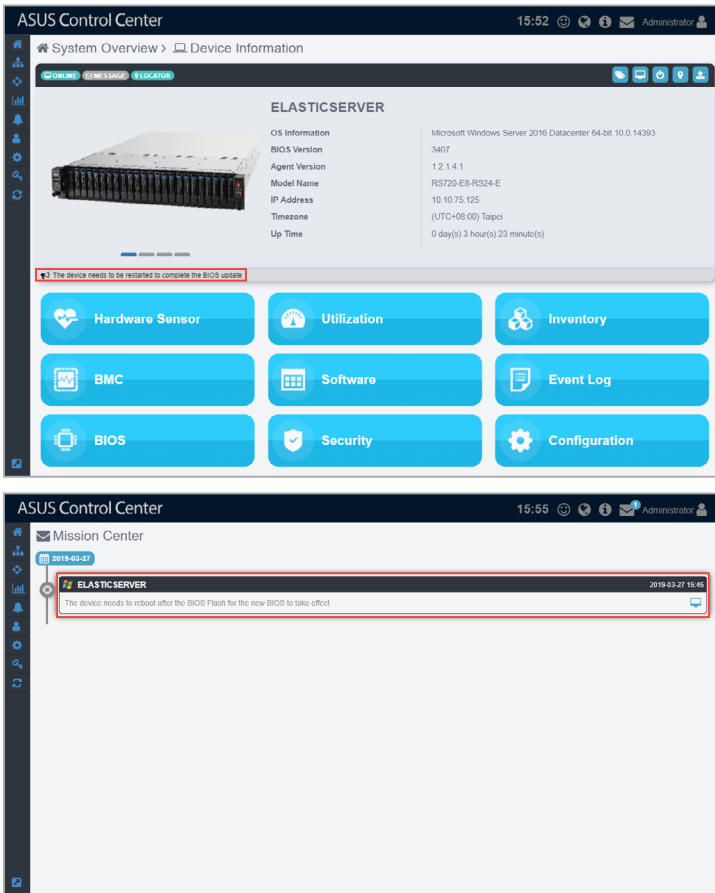
BMC is required for this option to work properly.



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



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



- Reboot the device to complete the BIOS flash.

BIOS Setting



The **BIOS Setting** tab is only available on specific ASUS CSM products. For more information on ASUS CSM products that support ASUS Control Center, please refer to <https://www.asus.com/Microsite/csm>.

The **BIOS Setting** tab allows you to view and adjust the **BIOS Advanced**, **Boot**, **Monitor** 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.

ASUS Control Center 16:16 Administrator

System Overview > MEDIACENTER-2 > BIOS

BIOS Flash BIOS Setting OMI Info

Press 'Enter' key to search. Clear Save

Advanced

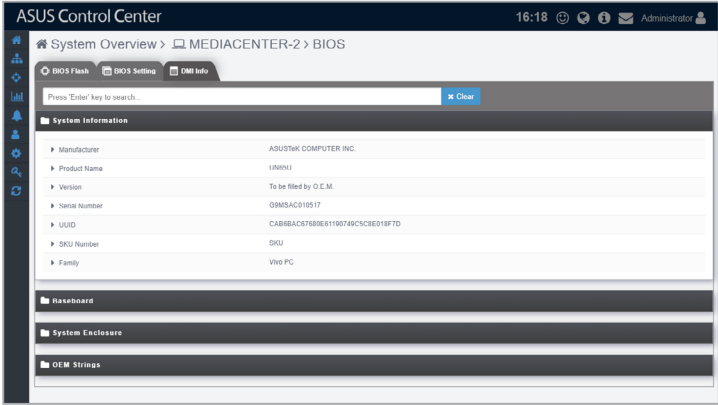
Monitor

boot

- 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 BIOS 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.
- Dev 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 on 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 Table** tab allows you to view details on certain items such as manufacturer name and hardware component information of the device without a hardware controller.



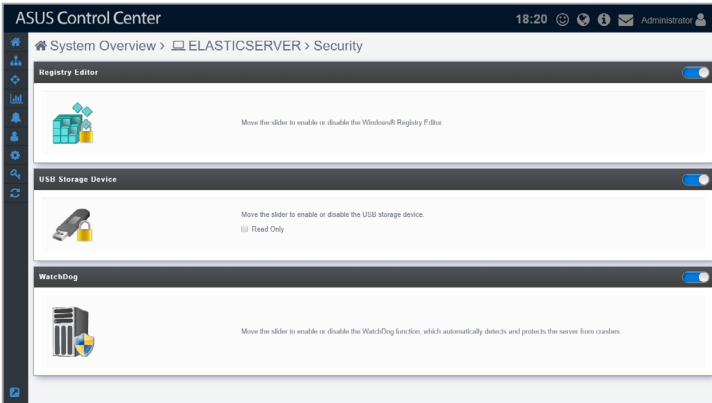
2.2.8 Security

This item allows you to set permissions on the device for the **Registry Editor**, **USB Storage Device**, and **Watchdog**. For more details on setting permissions for the device, refer to **3.3.3 Setting the device security**.

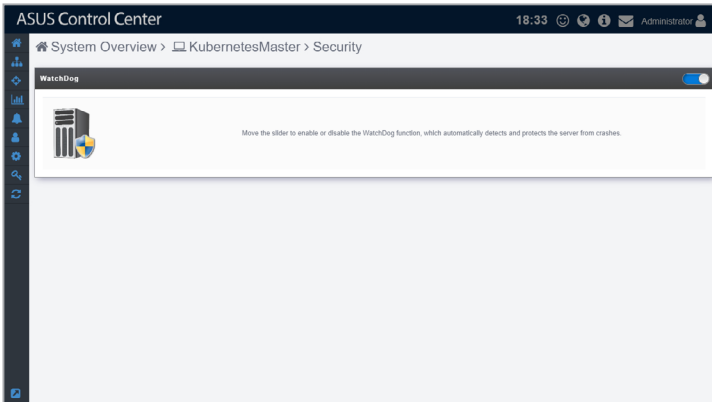


Linux systems only supports **Watchdog**.

For Windows® system:

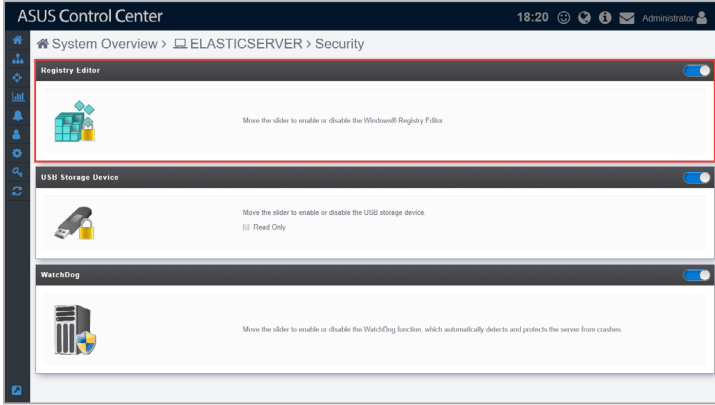


For Linux system:



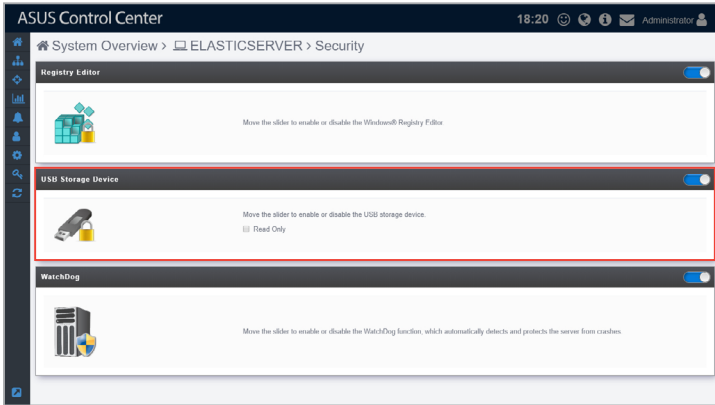
Registry Editor (Windows only)

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



USB Storage Device (Windows only)

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

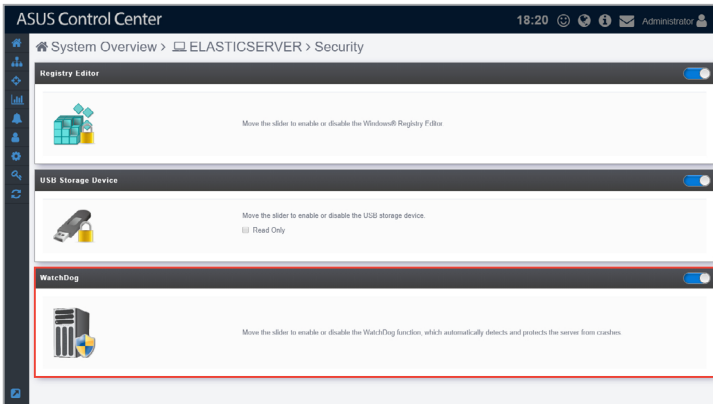


Watchdog

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

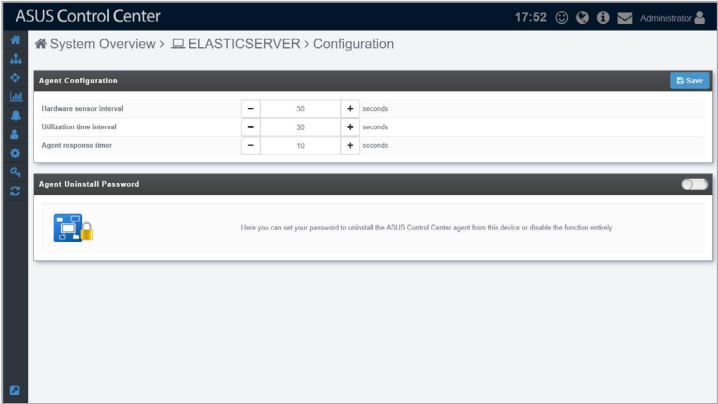


Auto Restart needs to be disabled on Windows® Server 2016 or later versions for **Watchdog** to successfully reboot the device when required. To disable **Auto Restart**, search for **Control Center** in the Windows Search Box, then navigate to **System > Advanced System Settings > Startup and Recovery**.



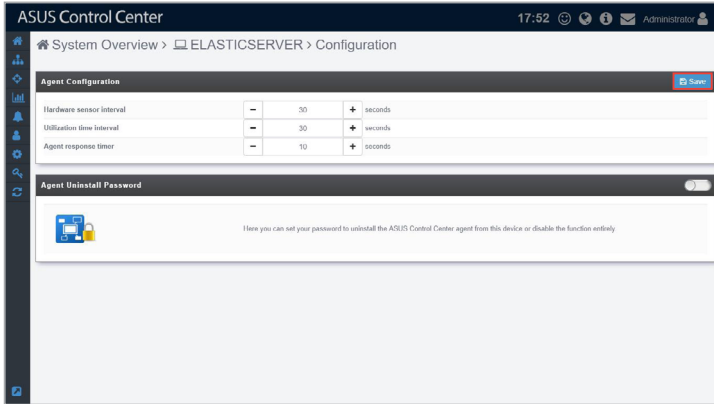
2.2.9 Configuration

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



Agent Configuration

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

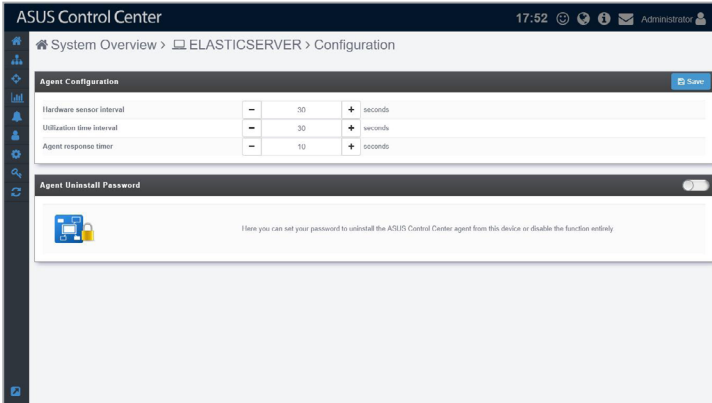


Hardware sensor interval	<p>Interval in seconds at which the hardware sensor information is sent to the ASUS Control Center server.</p> <p>The default is set to 30 seconds, which means that every 30 seconds the agent will report items such as fan disconnected back to the ACC server, and the ACC server will update this fan status within 30 seconds of receiving this report from the agent.</p>
Utilization time interval	<p>Interval in seconds at which the utilization information is sent to the ASUS Control Center server.</p> <p>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.</p>
Agent response timer	<p>Interval in seconds at which the agent will query the ASUS Control Center server for task updates.</p> <p>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.</p>

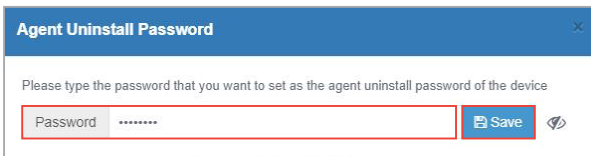
Agent Uninstall Password

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

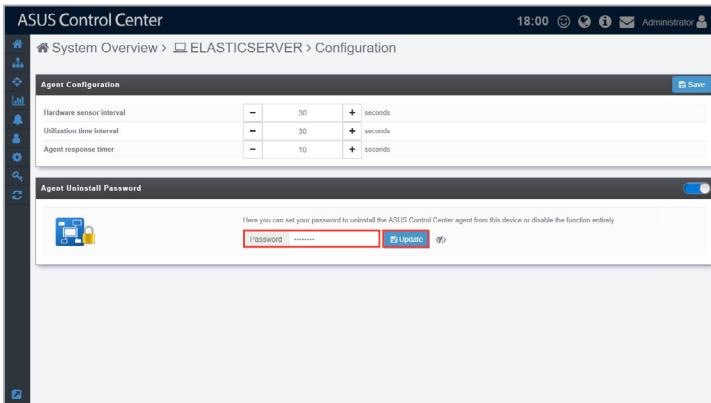
1. If **Agent Uninstall Password** is not enabled, click on the slider to enable it.



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



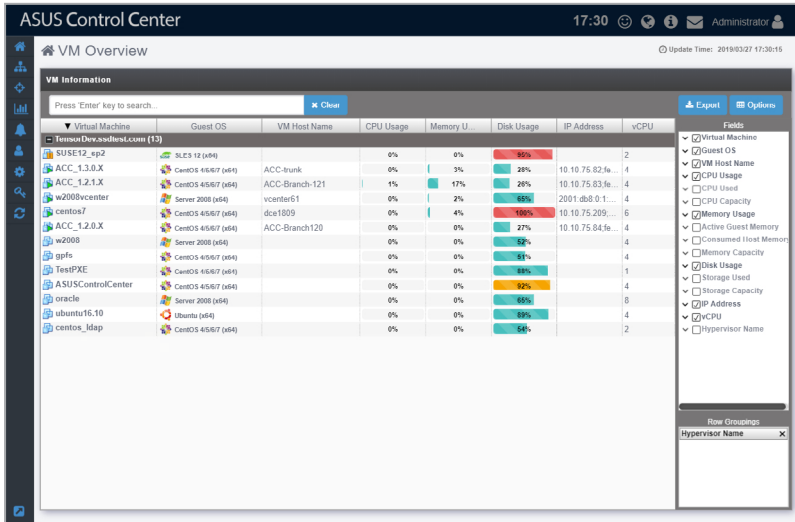
3. (optional) You can edit the password by entering a new password into the **Password** field, then clicking on **Update**.



2.3 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.



Virtual Machine	Guest OS	VM Host Name	CPU Usage	Memory U.	Disk Usage	IP Address	vCPU
SUSE12_4p2	SLES 12 (x64)	ACC-brunk	0%	0%	26%		2
ACC_1.2.0.X	CentOS 4.5/67 (x64)	ACC-Branch-121	0%	3%	28%	10.10.75.82.9...	4
ACC_1.2.1.X	CentOS 4.5/67 (x64)	ACC-Branch-121	1%	17%	26%	10.10.75.83.9...	4
w2008vcenter	Server 2008 (x64)	vcenter01	0%	2%	63%	2001.d8.0.1...	4
centos7	CentOS 4.5/67 (x64)	dce1809	0%	4%	16%	10.10.75.209...	6
ACC_1.2.0.X	CentOS 4.5/67 (x64)	ACC-Branch120	0%	0%	27%	10.10.75.84.9...	4
w2008	Server 2008 (x64)		0%	0%	52%		4
gppfs	CentOS 4.5/67 (x64)		0%	0%	51%		4
TestPXE	CentOS 4.5/67 (x64)		0%	0%	88%		1
ASUSControlCenter	CentOS 4.5/67 (x64)		0%	0%	92%		4
oracle	Server 2008 (x64)		0%	0%	65%		8
ubuntu16.10	Ubuntu (x64)		0%	0%	69%		4
centos_ldap	CentOS 4.5/67 (x64)		0%	0%	54%		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 **2.1.4 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 **2.1.3 Options**.
- 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.

The screenshot shows the 'ASUS Control Center' interface with the 'VM Overview' section. The 'VM Information' block contains a table with the following columns: Virtual Machine, Guest OS, VM Host Name, CPU Usage, Memory U., Disk Usage, IP-Address, and vCPU. The table lists 13 virtual machines, including 'SUSE12_302', 'ACC_1.3.0.X', 'ACC_1.2.1.X', 'wP00livercenter', 'centos7', 'ACC_1.7.0.X', 'wP00l', 'ggfs', 'TSHPXF', 'ASUSControlCenter', 'oracle', 'ubuntu16.10', and 'centos_3tag'. Each row shows the corresponding values for these columns, with usage percentages color-coded (green for low, yellow for medium, red for high).

Virtual Machine	Guest OS	VM Host Name	CPU Usage	Memory U.	Disk Usage	IP-Address	vCPU
SUSE12_302	SLES 12 (x64)		0%	0%	100%		2
ACC_1.3.0.X	CentOS 6.867 (x64)	ACC-Branch	0%	3%	20%	10.10.75.82	4
ACC_1.2.1.X	CentOS 6.867 (x64)	ACC-Branch-121	1%	17%	20%	10.10.75.83	4
wP00livercenter	Server 2008 (x64)	vcantor61	0%	2%	16%	2001-d8-0-1...	4
centos7	CentOS 6.867 (x64)	doc1809	0%	4%	100%	10.10.75.209	6
ACC_1.7.0.X	CentOS 6.867 (x64)	ACC-Branch120	0%	0%	27%	10.10.75.84	4
wP00l	Server 2008 (x64)		0%	0%	8%		4
ggfs	CentOS 6.867 (x64)		0%	0%	3%		4
TSHPXF	CentOS 6.867 (x64)		0%	0%	10%		1
ASUSControlCenter	CentOS 6.867 (x64)		0%	0%	14%		4
oracle	Server 2008 (x64)		0%	0%	5%		8
ubuntu16.10	Ubuntu (x64)		0%	0%	6%		4
centos_3tag	CentOS 6.867 (x64)		0%	0%	14%		2

On the right side of the 'VM Information' block, there are 'Export' and 'Options' buttons. The 'Options' dropdown menu is open, showing a list of metadata items with checkboxes, including 'Virtual Machine', 'Guest OS', 'VM Host Name', 'CPU Usage', 'CPU Usage', 'CPU Capacity', 'Memory Usage', 'Active Guest Memory', 'Consumed Host Memory', 'Memory Capacity', 'Disk Usage', 'Storage Used', 'Storage Capacity', 'IP-Address', and 'vCPU'. The 'Hypervisor Name' option is currently unchecked.

2.4 Host Information



- The screenshot may vary between agent and agentless devices, for more details on viewing details on devices with agents, refer to **2.2 Device 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 **2.1.4 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 **2.1.3 Options**.

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.

The screenshot displays the 'Host Information' page in the ASUS Control Center. The top section shows system metrics: CPU 1% (140 MHz / 720 CPU X 2100 MHz), MEMORY 94% (68.17 GB / 65.95 GB), DISK 43% (1094.83 GB / 2708.91 GB), and a Hardware Sensor status. Below this is a 'VM Information' table with columns for Virtual Machine, Guest OS, VM Host Name, CPU Use, Memory Usage, Click User, IP Address, and vCPU. The table lists several VMs, including 'w2000vcenter', 'ACC_1.2.0.X', 'ACC_1.2.1.X', 'ACC_1.3.0.X', 'vcenter1', 'ACC-Branch120', 'ACC-Branch-121', 'ACC-trunk', 'dca1009', 'w2003', 'TestIPXF', 'C8809_3dap', and 'gplk'.

Virtual Machine	Guest OS	VM Host Name	CPU Use	Memory Usage	Click User	IP Address	vCPU
w2000vcenter	Server 2008 (x64)	vcenter1	0%	0%	30%	2007-08-01 1:45:40	4
ACC_1.2.0.X	CentOS 4.6-07 (x64)	ACC-Branch120	1%	1%	27%	10.10.75.84.9680.2	4
ACC_1.2.1.X	CentOS 4.6-07 (x64)	ACC-Branch-121	1%	13%	36%	10.10.75.83.9680.2	4
ACC_1.3.0.X	CentOS 4.6-07 (x64)	ACC-trunk	0%	0%	2%	10.10.75.82.9680.2	4
vcenter1	Server 2008 (x64)	dca1009	0%	0%	100%	10.10.75.209.172.1	6
w2003	Server 2008 (x64)		0%	0%	4%		4
TestIPXF	CentOS 4.6-07 (x64)		0%	0%	34%		1
C8809_3dap	CentOS 4.6-07 (x64)		0%	0%	1%		2
gplk	CentOS 4.6-07 (x64)		0%	0%	4%		4

Device Statuses and Quick Buttons



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



Metadata Editor: This item allows you to edit the metadata of the hypervisor by double clicking in the **Value** field.



VMware ESXi: This item allows you to link to the vSphere Web Client management interface.



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

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.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes the time 17:46 and the user Administrator. The main content area is titled "VM Overview > Host Information".

Host Information Panel:

- Hypervisor Type:** VMware ESXi 6.0.0 build-2805209
- Host Name:** TensorDev.ssdtest.com
- Manufacturer:** ASUS/IEK COMPUTER INC.
- Model Name:** Z59P-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

System Metrics:

- CPU 1%:** 448 MHz / 20 CPUs x 2159 MHz
- MEMORY 94%:** 69.17 GB / 63.35 GB
- DISK 43%:** 1194.83 GB / 2796.54 GB
- HARDWARE SENSOR:** Critical

VM Information Table:

Virtual Machine	Guest OS	VM Host Name	CPU Use	Memory Usage	Disk Use	IP Address	vCPU
w2000vcenter	Server 2008 (x64)	vcenter01	0%	0%	36%	2001.0b.0.1.484b...	4
ACC_12.0.X	CentOS 6.6-0.07 (x64)	ACC-branch-120	0%	1%	2%	10.10.75.55.6400-2...	4
ACC_12.1.X	CentOS 6.6-0.07 (x64)	ACC-branch-121	1%	13%	26%	10.10.75.81.6400-2...	4
ACC_13.0.X	CentOS 6.6-0.07 (x64)	ACC-branch	0%	2%	28%	10.10.75.82.6400-2...	4
centos7	CentOS 6.6-0.07 (x64)	dca1809	0%	0%	96%	10.10.75.209.172.1...	6
ORACLE	Server 2008 (x64)		0%	0%	84%		8
w2008	Server 2008 (x64)		0%	0%	52%		4
TEMPXE	CentOS 6.6-0.07 (x64)		0%	0%	38%		1
centos_mdap	CentOS 6.6-0.07 (x64)		0%	0%	54%		2
gpfs	CentOS 6.6-0.07 (x64)		0%	0%	81%		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.

The screenshot displays the ASUS Control Center interface. At the top, it shows 'ASUS Control Center' and the time '17:55'. The main area is divided into 'VM Overview' and 'Host Information'. The 'Host Information' section shows details for the hypervisor (VMware ESXi 6.0.0), host name (TensorDev.ssdtest.com), manufacturer (ASUSTeK COMPUTER INC.), model name (Z9PP-D24 Series), processor type (Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.20GHz), and other hardware specifications. Below this, the 'VM Information' table lists several virtual machines with columns for Name, Guest OS, VM Host Name, CPU Use, and Memory Usage. A 'Power Control' dropdown menu is open over the table, showing options: Power Off, Reboot, and Suspend. The 'Power Off' option is highlighted in red.


Virtual Machine	Guest OS	VM Host Name	CPU Use	Memory Usage	Power Control	Reboot	vCPU
w2000vcenter	Server 2008 (x64)	vcenter11	0%	1%	Power Off	0:1:45:0	4
ACC_1.2.6.X	CentOS 4.6.0-7 (x64)	ACC-Branch-120	0%	14%	Power Off	0:4:58:0	4
ACC_1.2.1.X	CentOS 4.6.0-7 (x64)	ACC-Branch-121	1%	14%	Power Off	0:3:58:0	4
ACC_1.3.0.X	CentOS 4.6.0-7 (x64)	ACC-trunk	0%	3%	Power Off	0:2:58:0	4
CentOS7	CentOS 4.6.0-7 (x64)	dce1009	0%	0%	Power Off	10:10:19:209:172:1	6
Ubuntu16.10	Ubuntu (x64)		0%	0%	Power Off	0:2:58:0	4
Oracle	Server 2008 (x64)		0%	0%	Power Off	0:2:58:0	8
w2000	Server 2008 (x64)		0%	0%	Power Off	0:2:58:0	4
ASUSMC_center	CentOS 4.6.0-7 (x64)		0%	0%	Power Off	0:2:58:0	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 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.



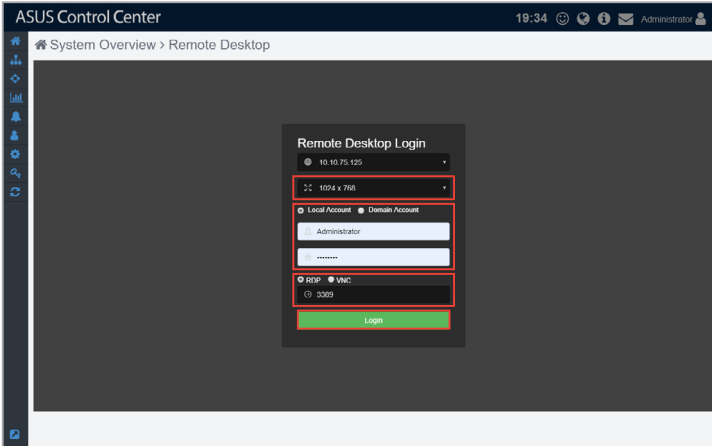
- **Local Account:** The agent's administrator privileges only allow you to manage the device the agent is installed on.
 - **Domain Account:** The agent's administrator privileges allow you to manage all devices in the domain. The **Domain** field only appears if you selected **Domain Account**.
-

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



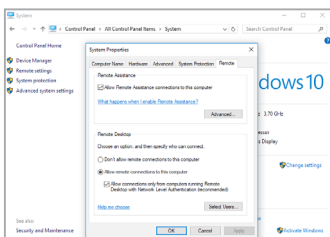
Linux and Windows® systems use different protocols, ensure the device is reachable through the selected protocol:

- **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.

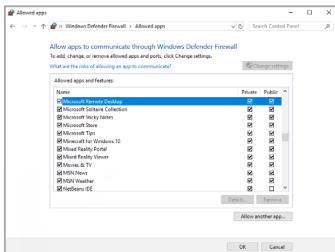




- Ensure the device you wish to remote control has a stable power supply and Internet connection.
- The device may be remote controlled if it is logged out or locked, but cannot be remote controlled if the device is powered off or in sleep mode. If the device is in sleep mode, please wake the device using the Wake-on-LAN function.
- 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 > Advanced System Settings > Remote**.



- Please ensure that the **Microsoft Remote Desktop** application is enabled in the **Windows Defender Firewall Allowed Apps** list. Search for **Control Panel** in the Windows Search Box, then navigate to **Windows Defender Firewall > Allowed Apps**.



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



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.

Chapter 3

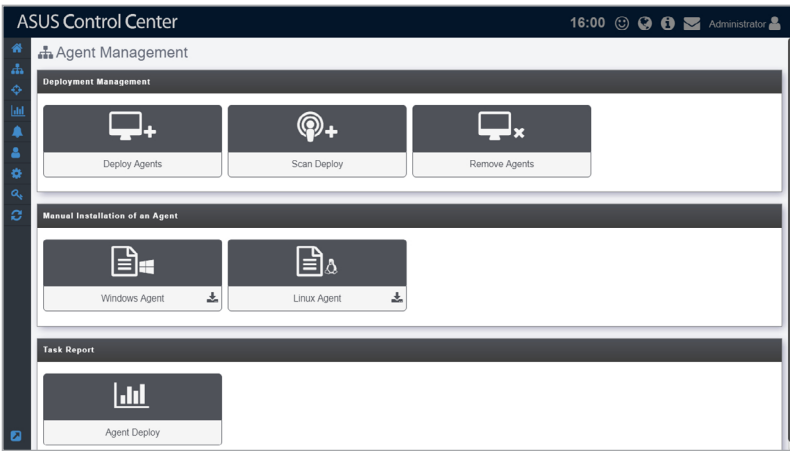
This chapter describes how to deploy ASUS Control Center agents and remove agents through Microsoft® Active Directory or manually. You may also add and manage agentless VMware.

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 **2.1.4 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 **2.1.3 Options**.

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.



You may exchange 500 sets of CSM License Keys for 1 set of Server License Key to enable the automatic Windows Agent deployment function (**Deploy Agents**). Please contact your local ASUS Sales representative and/or TPM for more information.

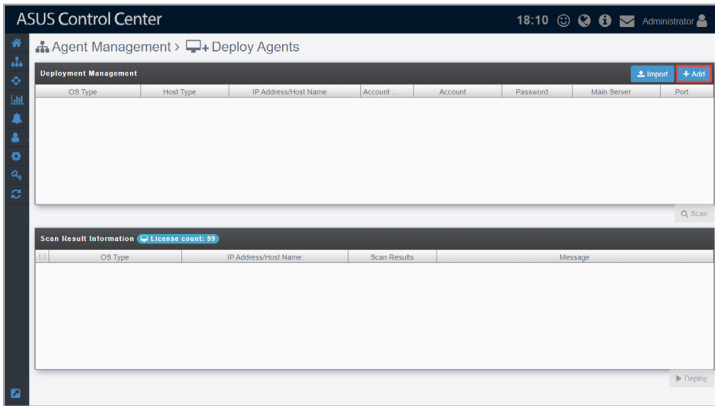
The screenshot displays the 'ASUS Control Center' interface, specifically the 'Agent Management > Deploy Agents' section. The top part of the interface features a table for adding agents with columns for OS Type, Host Type, IP Address/Host Name, Account, Account, Password, Main Server, and Port. Below this is a 'Scan Result Information' section with a 'License count: 99' indicator. This section contains a table with columns for IP, OS Type, IP Address/Host Name, Scan Results, and Message.

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

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

Adding a single device

1. Click on **Add**.



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

The 'Add Target Host' dialog box is shown with a green header. It contains the following fields and options:

- Main Server**: 10.10.75.123
- Port**: 8080
- OS Type**: Windows (dropdown menu)
- Host Type**: IP Address Host Name
- IP Address/Host Name**: 10.10.75.125
- Account Type**: Local Account Domain Account
- Account**: Administrator
- Password**: [Redacted]

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

3. Select the **OS Type** of the device you wish to add from the **OS Type** drop down menu, 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:

The screenshot shows the 'Add Target Host' dialog box with the following fields and options:

- Main Server:** 10.10.75.123
- Port:** 8080
- OS Type:** Windows (selected in the dropdown menu)
- Host Type:** IP Address (selected with a radio button), Host Name
- Host Type Input:** 10.10.75.125
- Account Type:** Local Account (selected with a radio button), Domain Account
- Account:** Administrator
- Password:** [Redacted with dots]
- Buttons:** Cancel, Save

Selecting Linux system:

The screenshot shows the 'Add Target Host' dialog box with the following fields and options:

- Main Server:** 10.10.75.123
- Port:** 8080
- OS Type:** Linux (selected in the dropdown menu)
- Host Type:** IP Address (selected with a radio button), Host Name
- Host Type Input:** 10.10.75.103
- Account:** root
- Password:** [Redacted with dots]
- Buttons:** Cancel, Save

4. Select the **Account Type**.



- **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 allows you to manage all devices in the domain.

Selecting Local Account:

The screenshot shows the 'Add Target Host' dialog box with the following fields and settings:

- Main Server: 10.10.75.123
- Port: 8080
- OS Type: Windows
- Host Type: IP Address (selected), Host Name
- Host Name: 10.10.75.125
- Account Type: Local Account (selected and highlighted with a red box), Domain Account
- Account: Administrator
- Password: [Redacted]

Buttons: Cancel, Save

Selecting Domain Account:

The screenshot shows the 'Add Target Host' dialog box with the following fields and settings:

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

Buttons: Cancel, Save



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 of the device, then click on **Save**.

Add Target Host

Main Server: 10.10.75.123 Port: 8080

OS Type: Windows

Host Type: IP Address Host Name

10.10.75.125

Account Type: Local Account Domain Account

Account: Administrator

Password:

Cancel Save

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

ASUS Control Center 19:11 Administrator

Agent Management > Deploy Agents

Deployment Management Import Export Add

OS Type	Host Type	IP Address/Host Name	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

Scan Result Information License Used: 98

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

Deploy

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



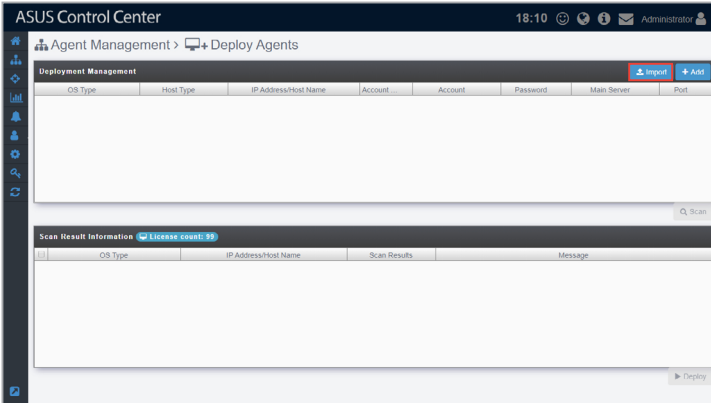
Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.

The screenshot shows the ASUS Control Center interface. The top navigation bar includes the title "ASUS Control Center", the time "19:33", and the user "Administrator". The main content area is divided into two sections:

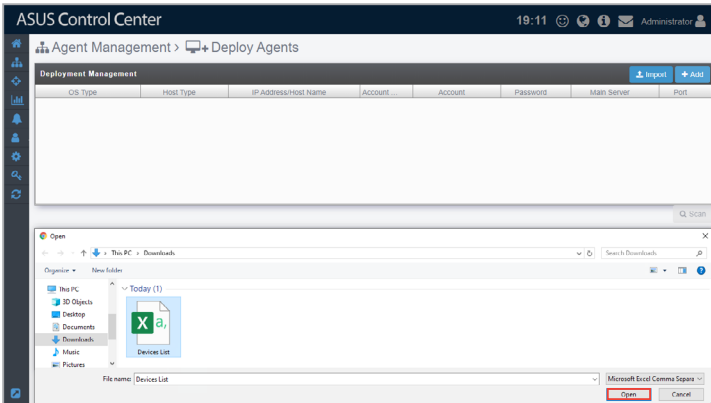
- Deployment Management:** A table with columns: OS Type, Host Type, IP Address/Host Name, Account, Account, Password, Main Server, and Port. It lists two entries: Windows (IP: 10.10.75.125, Account: local/Administrator, Port: 8080) and Linux (IP: 10.10.75.103, Account: local/root, Port: 3088). Buttons for "Import", "Export", and "Add" are visible.
- Scan Result Information:** A table with columns: OS Type, IP Address/Host Name, Scan Results, and Message. It shows two entries: Windows (IP: 10.10.75.125, Scan Results: Support, Message: OK) and Linux (IP: 10.10.75.103, Scan Results: Not Support, Message: Scan Successful, Please check your BMC is installed, it cannot monitor hardware). A "Support (2)" filter is active. A "Deploy All" button is at the bottom right.

Adding multiple devices

1. Click on **Import**.



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



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



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

The screenshot shows the ASUS Control Center interface with the 'Agent Management' section open. A table lists devices with columns for OS Type, Host Type, IP Address/Host Name, Account, Password, Main Server, and Port. An Excel spreadsheet is overlaid on the interface, showing a table with columns: relationNum, osType, targetType, target, adminPort, accountType, domain, account, password, mainServerIp, and mainServerPort. The spreadsheet contains two rows of data for Windows and Linux OS types.

- 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.

The screenshot shows the ASUS Control Center interface with the 'Scan Result Information' section open. A table displays the results of the scan, including OS Type, IP Address/Host Name, Scan Results, and Message. The results show that Windows is supported and Linux is not supported due to missing BMC.

OS Type	IP Address/Host Name	Scan Results	Message
Windows	10.10.75.125	Support	OK
Linux	10.10.75.103	Not Support	Scan Successful, 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.

ASUS Control Center 18:16 Administrator

Agent Management > Deploy Agents

Deployment Management Import Export Add

OS Type	Host Type	IP Address/Host Name	Account	Account	Password	Main Server	Port
Windows	ip	10.10.75.125	local	Administrator	****	10.10.75.125	9080
Linux	ip	10.10.76.103	local	root	****	10.10.76.123	9080

Scan Result Information License count: 99

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

Deploy

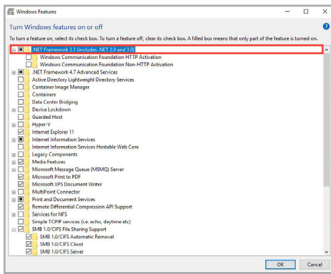
Agent deployment conditions and settings

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.

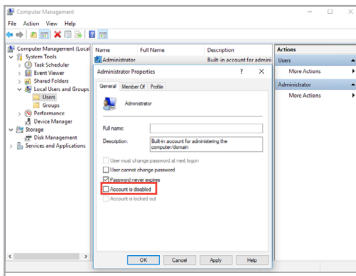


The examples used in this section are all based on Windows® 10.

- Ensure the device has sufficient power and a steady connection to prevent packet loss when deploying the agent.
- Windows® Home or lower versions of Windows® are not supported by ASUS Control Center.
- For Windows® 8 and above, or Windows® Server 2012 and above, ensure that .Net Framework 3.5 is enabled by searching for **Control Panel** in the Windows Search Box, then navigating to **Programs > Programs and Features > Turn Windows features on or off**, then check the **.NET Framework 3.5** checkbox to enable it.

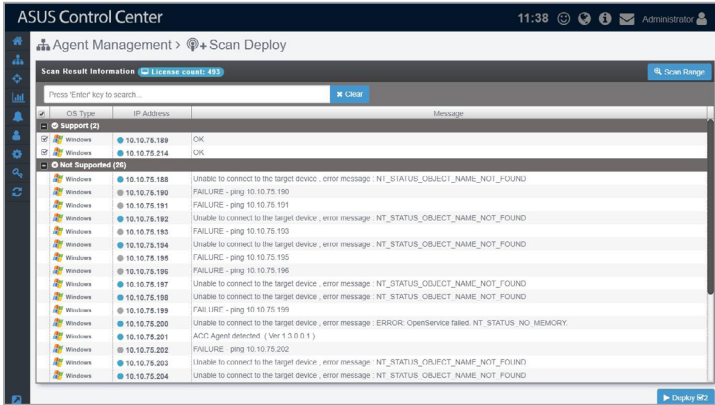


- The Administrator account of the client is enabled and has a password set. (Windows disables the Administrator account by default, to enable the account search for **Computer Management** in the Windows Search Box, then navigating to **System Tools > Local Users and Groups > Users > Administrator**, right click and select **Properties**, then uncheck the **Account is disabled** field, and click **OK**)



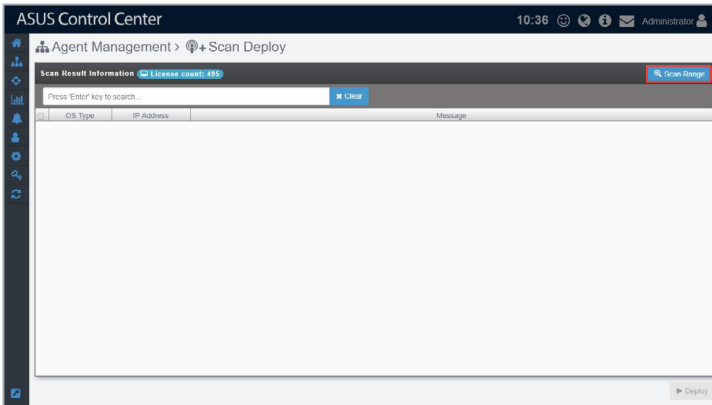
3.1.2 Scan and Deploy

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.

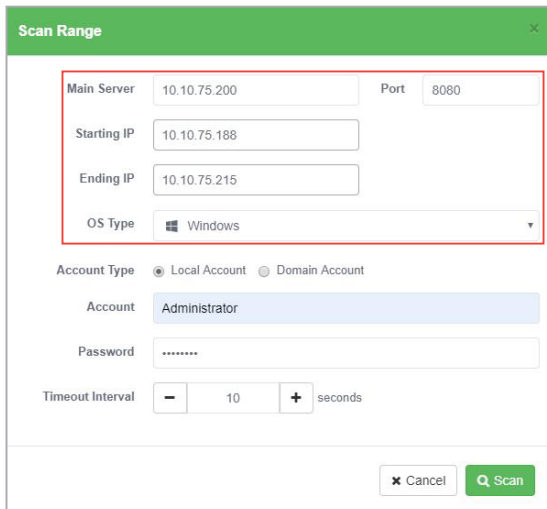


Scanning for managed devices and deploying agents

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



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

The "Scan Range" pop-up window has a green header with a close button. It contains several input fields: "Main Server" (10.10.75.200), "Port" (8080), "Starting IP" (10.10.75.188), "Ending IP" (10.10.75.215), and "OS Type" (Windows). Below these are "Account Type" (Local Account selected), "Account" (Administrator), "Password" (masked), and "Timeout Interval" (10 seconds). At the bottom are "Cancel" and "Scan" buttons.

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



The account and password entered should be for an account that has administrator privileges on managed devices. For more information on activating the administrator account on managed devices, please refer to **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

Account Type: Local Account Domain Account

Account: Administrator

Password:

Timeout Interval: - 10 + seconds

Cancel Scan

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

The image shows a 'Scan Range' configuration dialog box with a green header and a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Main Server:** Text input field containing '10.10.75.200'.
- Port:** Text input field containing '8080'.
- Starting IP:** Text input field containing '10.10.75.188'.
- Ending IP:** Text input field containing '10.10.75.215'.
- OS Type:** Dropdown menu with 'Windows' selected.
- Account Type:** Radio buttons for 'Local Account' and 'Domain Account', with 'Domain Account' selected.
- Domain:** Text input field containing 'ssctest.com', highlighted with a red rectangular border.
- Account:** Text input field containing 'Administrator'.
- Password:** Password input field with masked characters '.....'.
- Timeout Interval:** Control with minus and plus buttons, a numeric input field containing '10', and the text 'seconds'.

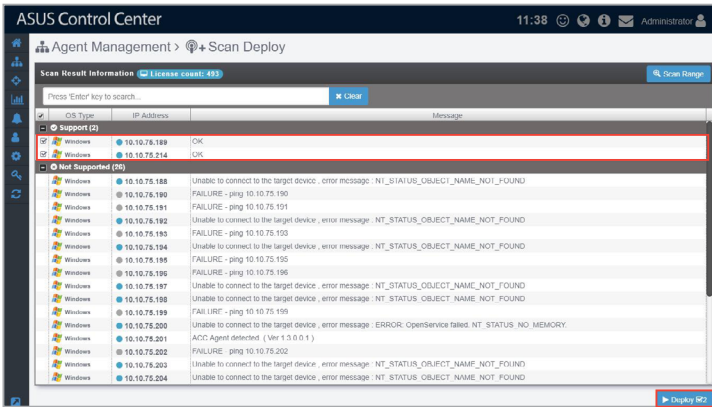
At the bottom right of the dialog, there are two buttons: 'Cancel' (with an X icon) and 'Scan' (with a magnifying glass icon).

- 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**.

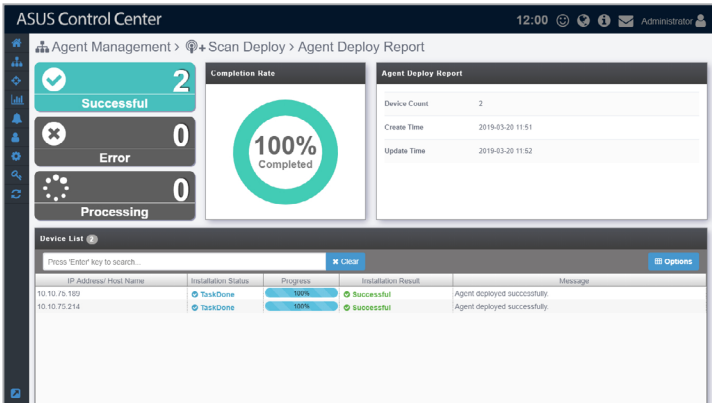
- The scan results will display which devices you can deploy agents to and also the devices which cannot be deployed as well as the reasons they cannot be deployed to, for more information on agent deployment conditions, please refer to **3.1.1 Deploy Agents** section.

OS Type	IP Address	Message
Windows	10.10.75.188	OK
Windows	10.10.75.194	OK
Not Supported (20)		
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

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

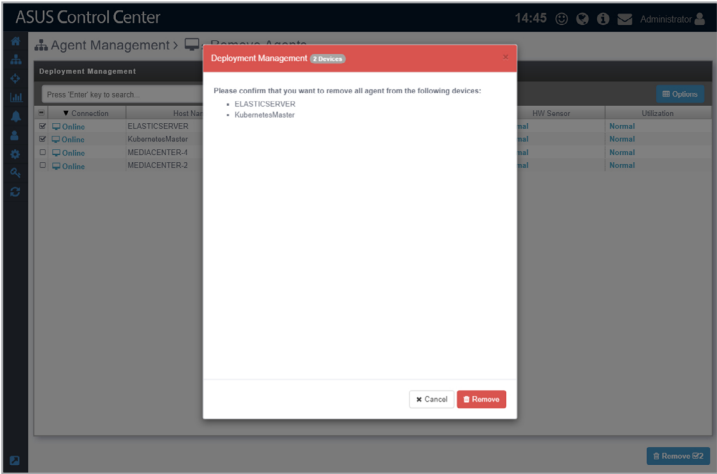


- Once the agents deployment has finished, a **Agent Deploy Report** will appear, detailing the deploy status of each selected device. This will help you check if all agents have been successfully deployed.



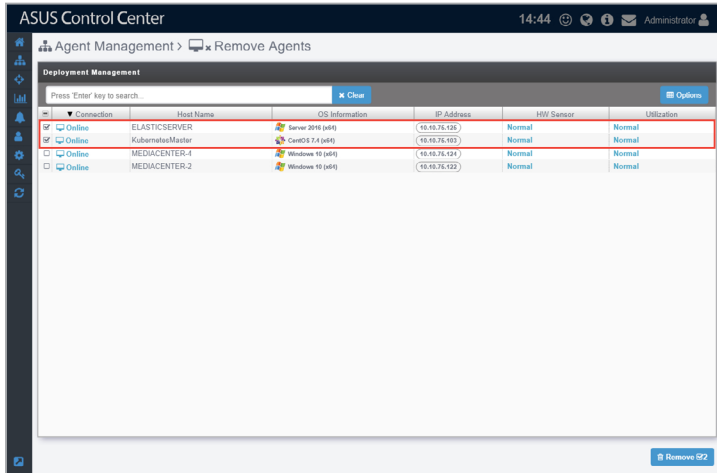
3.1.3 Remove agents

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



Remove agents using ASUS Control Center

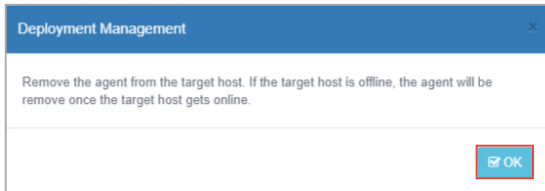
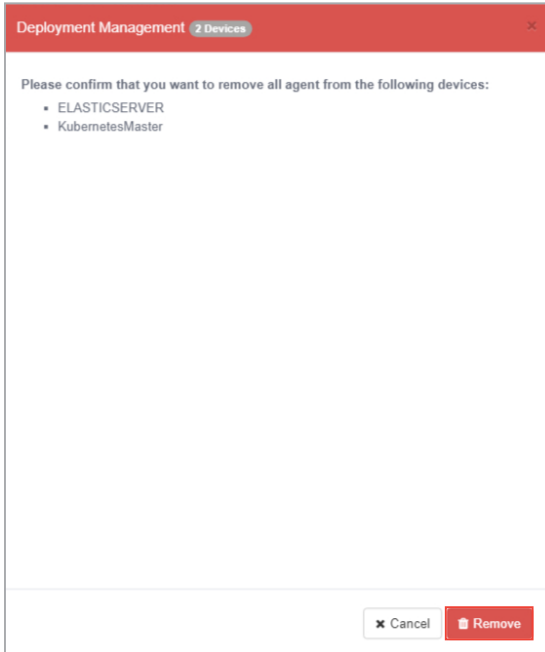
1. Check the devices you wish to remove agents from on the list.



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



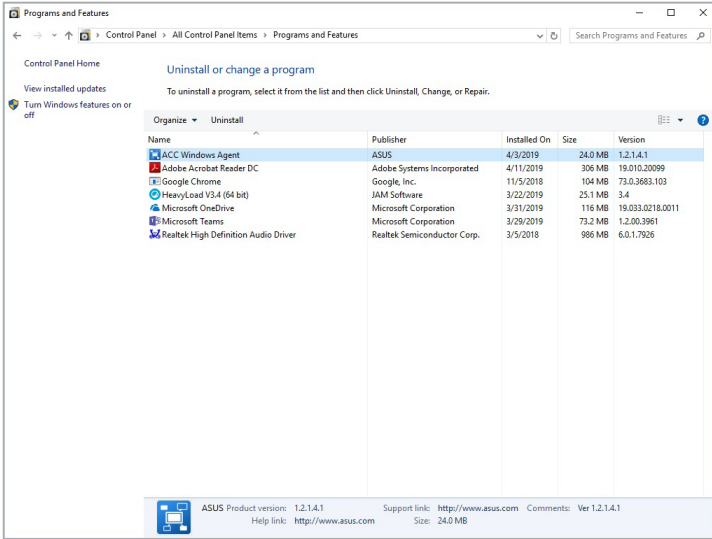
If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.



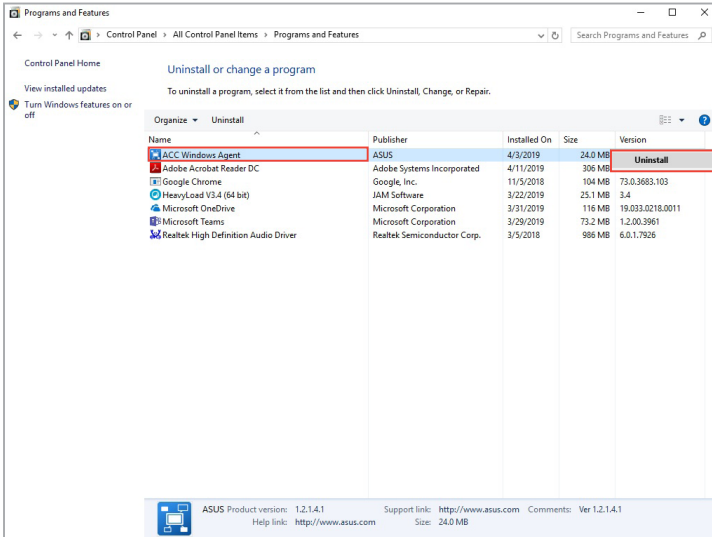
Remove Windows Agent from local device

You may choose to remove Agents from Windows systems manually.

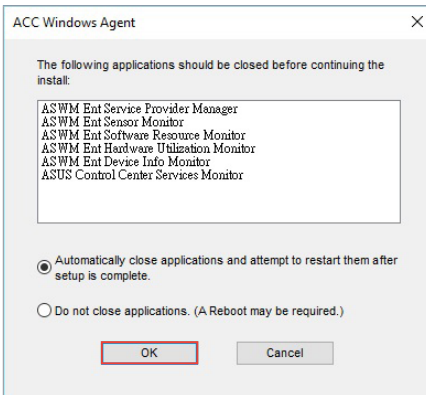
1. To remove the Windows Agent manually on a managed device, click on **Control Panel > Programs and Features**.



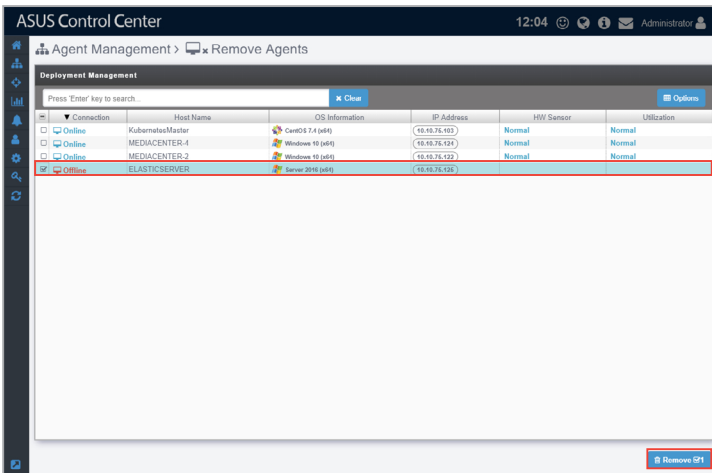
2. Select and uninstall **ACC Windows Agent** from the list of programs.



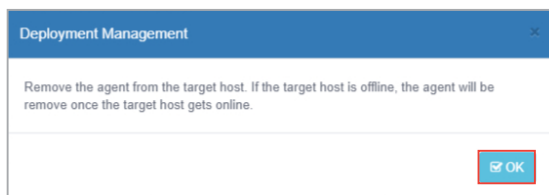
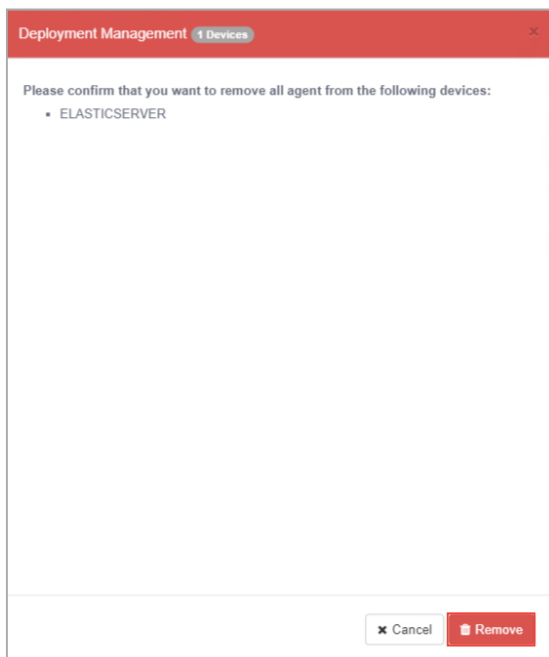
3. Ensure the applications shown in the pop-up window are closed, or you can check the **Automatically close applications and attempt to restart them after setup is complete** checkbox, then click **OK** to continue with the uninstallation process.



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



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

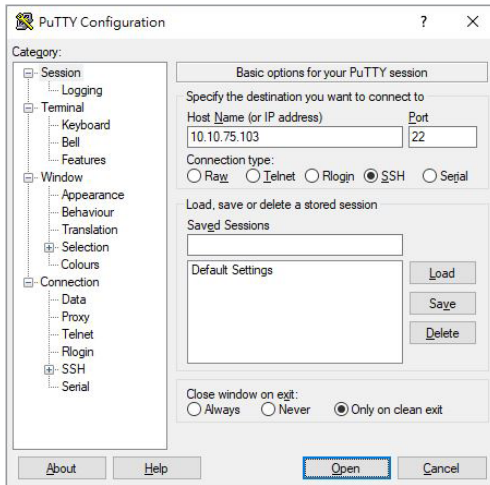


Remove Linux Agent from local device

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

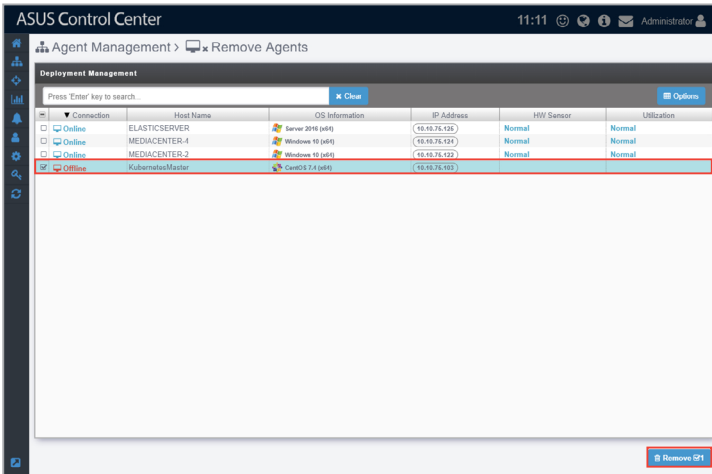
1. (optional) If you are using a Windows OS, you may use a third-party SSH or telnet client such as PuTTY to connect to the managed Linux device.

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

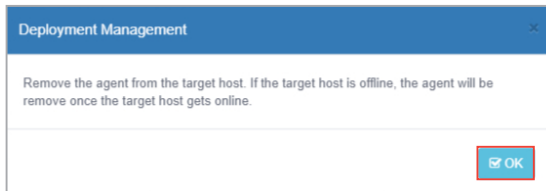
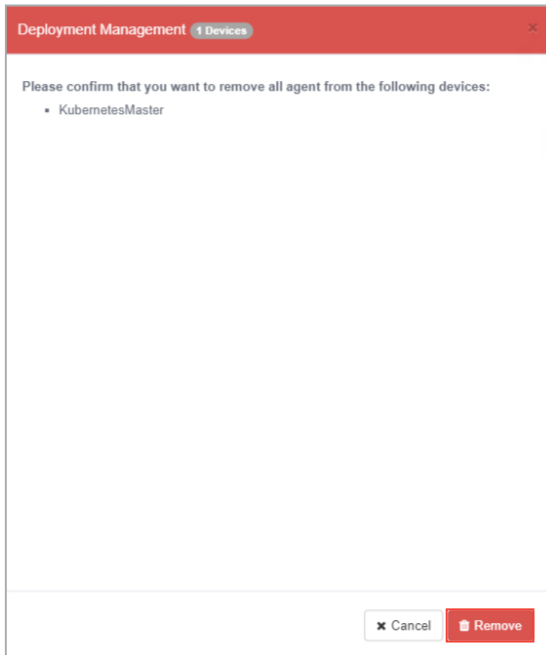


2. Enter the root account and password of the client Linux device.
3. Once you've logged in, execute `/root/uninstall.sh` to remove the Linux Agent from the managed device.
4. Once the Linux Agent is removed on the managed device, please navigate to the **Remove Agents** menu of your ASUS Control Center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

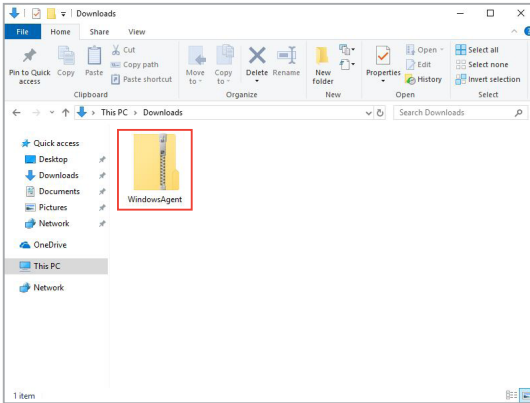
- 5. Select the managed device which you manually removed the agent from, the connection status for that managed device should be **Offline**, then click on **Remove** to remove the managed device from ASUS Control Center.



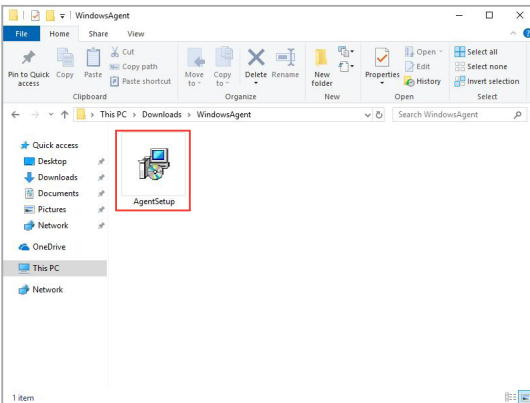
- A pop-up window should appear, displaying the devices you wish to remove agents from. After confirming the correct devices are selected, click on **Remove**, then click on **OK**.



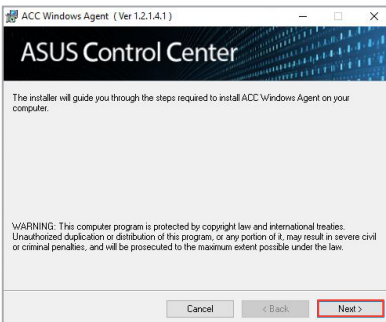
3. Unzip the ZIP file containing the installation files.



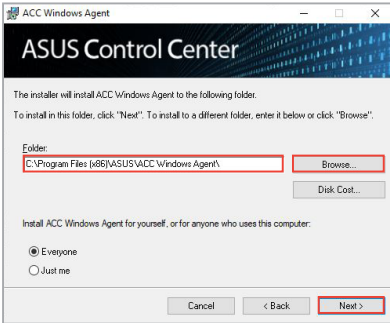
4. Click on the **AgentSetup.msi** file to launch the installation.



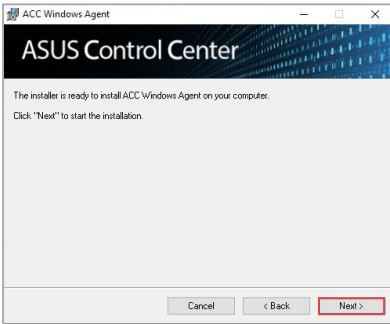
5. Click on **Next** to begin the installation.



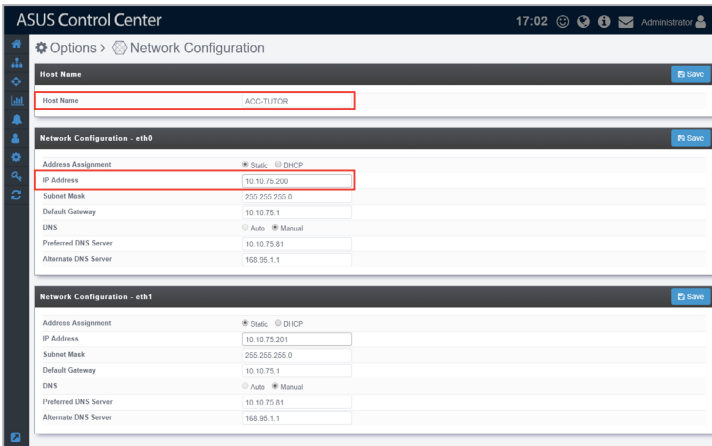
6. Browse and select a folder to install the agent, then click **Next**.



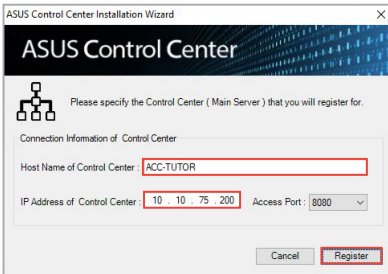
7. Click on **Next** again to continue the installation.



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



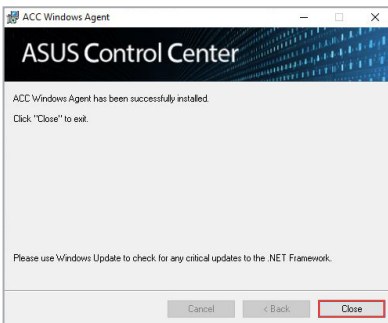
9. Enter the **Host Name** and **IP Address** from the previous step into the Windows® Agent Installer, then click **Register**.



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.




3.1.5 Linux Agent

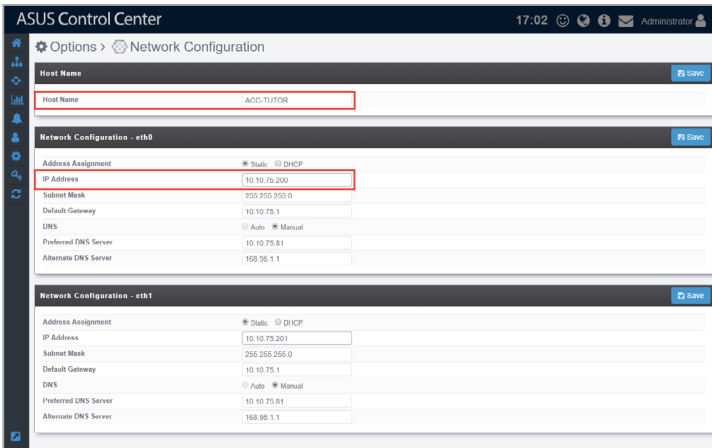


This function is only available on the Classic and Enterprise edition.

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

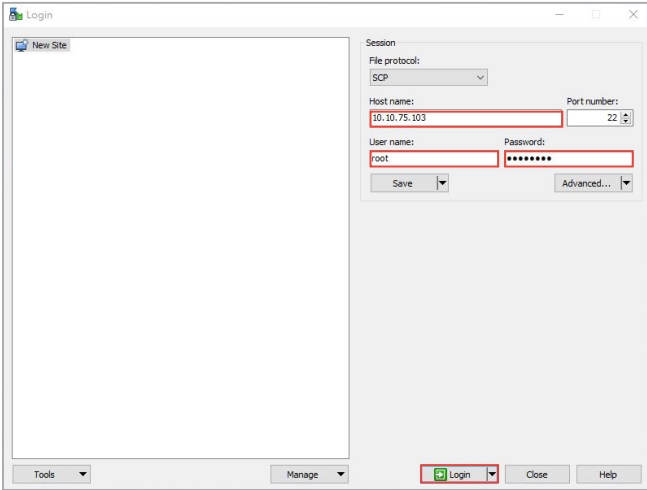
Install Linux agents manually

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



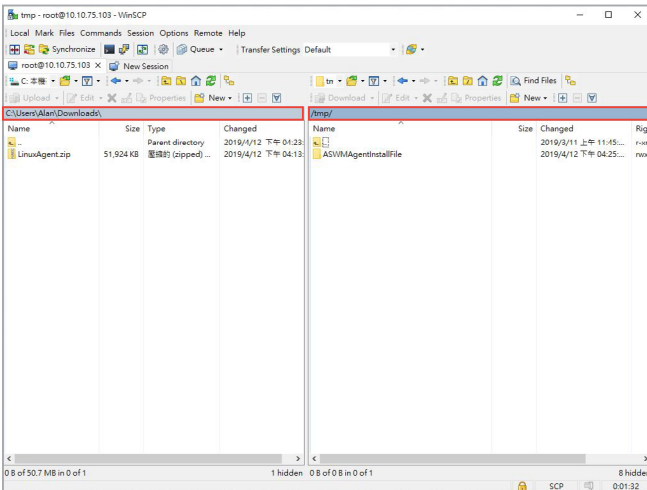
4. To copy the Linux Agent .tar file to the Linux device you wish to install the agent on, use a third-party file transfer program such as WinSCP, which is seen in the below example.

Enter the IP, account, and password of the device, then click on **Login**.



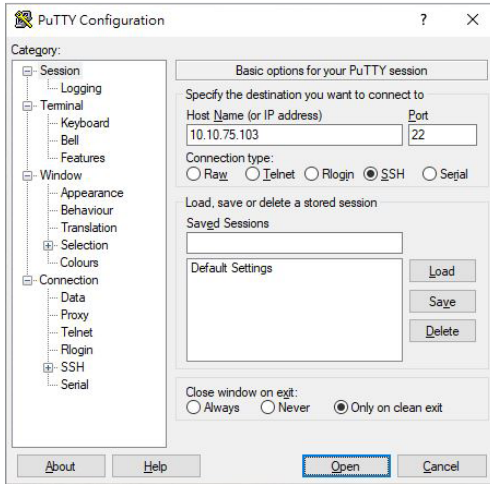
4. On the left window, navigate to the folder where the Linux Agent .tar file is located. On the right window, navigate to the destination you wish to save the Linux Agent installation file.

For this example we use tmp as our destination folder on the right window.

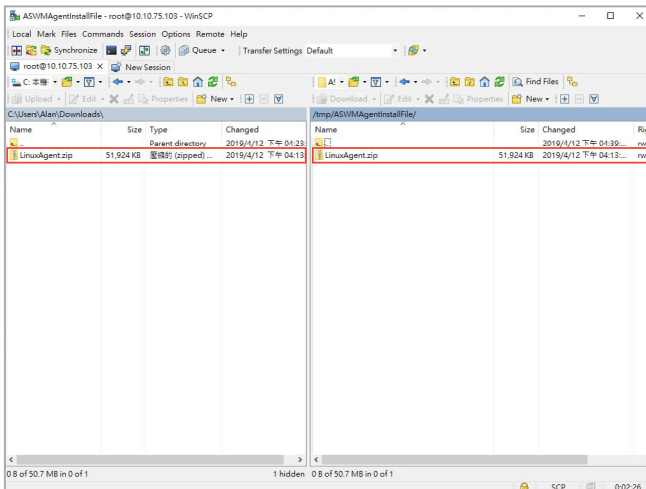


5. Log into the Linux device using a third-party SSH or telnet client such as PuTTY.

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



6. Enter the root account and password of the client Linux device.
7. Once you've logged in, execute `mkdir -p /tmp/ASWMAgentInstallFile` to create a folder named ASWMAgentInstallFile under tmp.
8. On WinSCP, copy and paste the **LinuxAgent** zip file from the left window to the newly created ASWMAgentInstallFile folder in the right window.



9. Decompress the LinuxAgent zip file, you should see a .tar file named **ASWMLinuxAgent-64bits.tar.gz**, then decompress the **ASWMLinuxAgent-64bits.tar.gz** file.

10. 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:8080
```

- For SLES

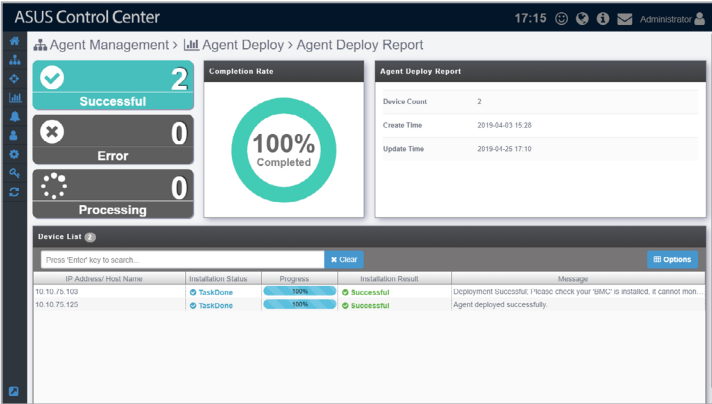
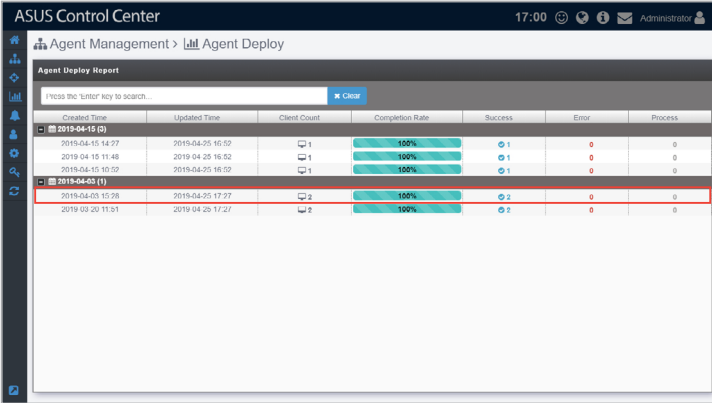
```
Execute /tmp/ASWMAgentInstallFile/Silentinstall_SLES.sh  
XXXX.XXX.XXX.XXX:8080
```



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

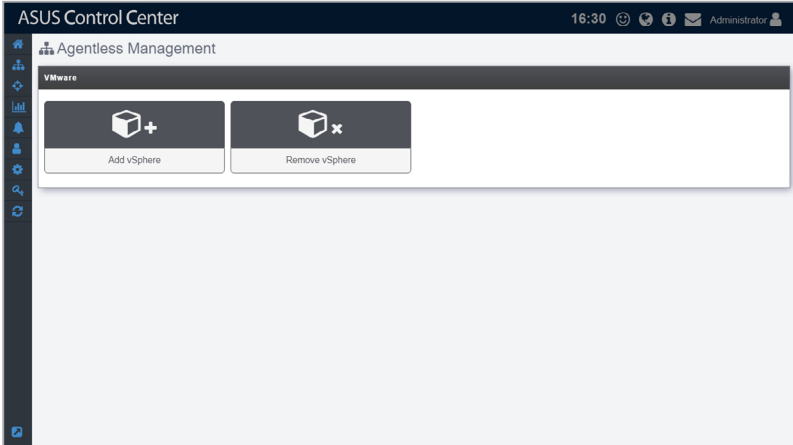
The Agent Deploy Report will display information of each time you deploy agent(s) onto managed devices. Each item showed on the **Agent Deploy Report** represents a single batch of deployment; clicking on each item will allow you to view information on the devices you deployed agents to in that batch.



3.2 Agentless Management

The **Agentless Management** screen allows you to add vSphere 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.



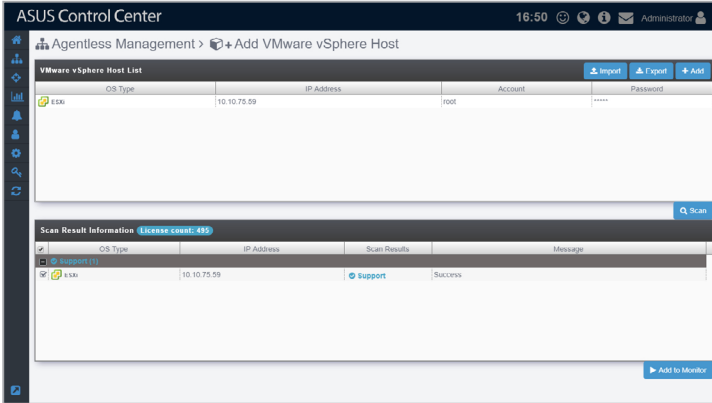
- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to **2.1.4 Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to **2.1.3 Options**.

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.

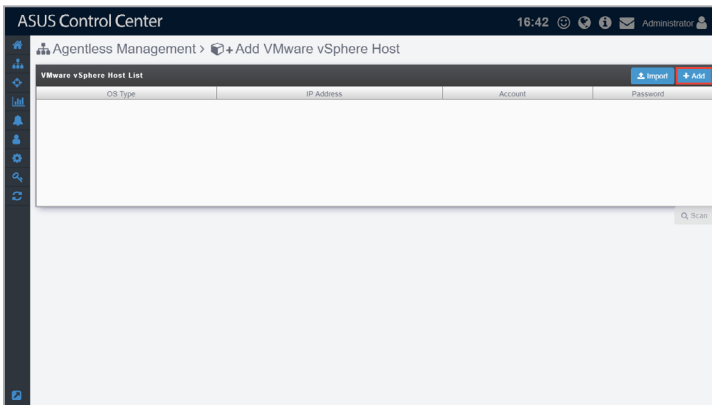


Ensure to register the License keys before adding the vSphere you wish to manage to ASUS Control Center. For more information on registering license keys, please refer to **Chapter 9 License**.

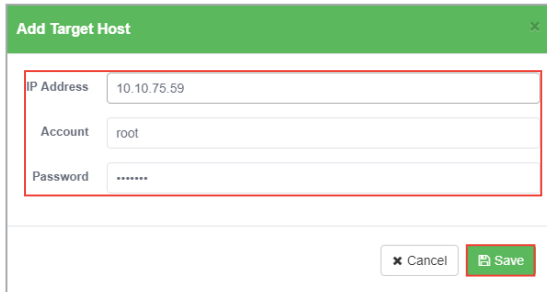


Adding a single vSphere

1. Click on **Add**.



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



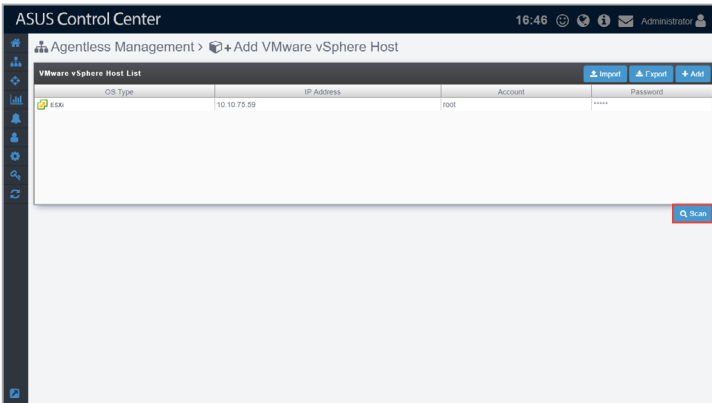
IP Address 10.10.75.59

Account root

Password

Cancel Save

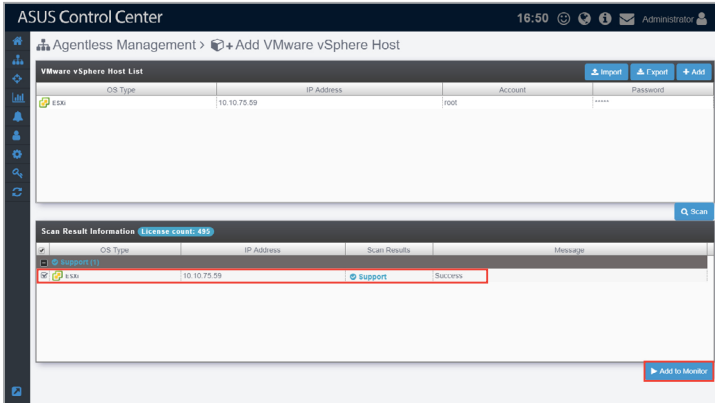
3. Repeat steps 1 and 2 to add additional vSpheres to be scanned, or refer to the **To add multiple vSpheres** section to import a list of vSpheres.
4. Once you have added all the vSpheres you wish to scan, click on **Scan**.



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.

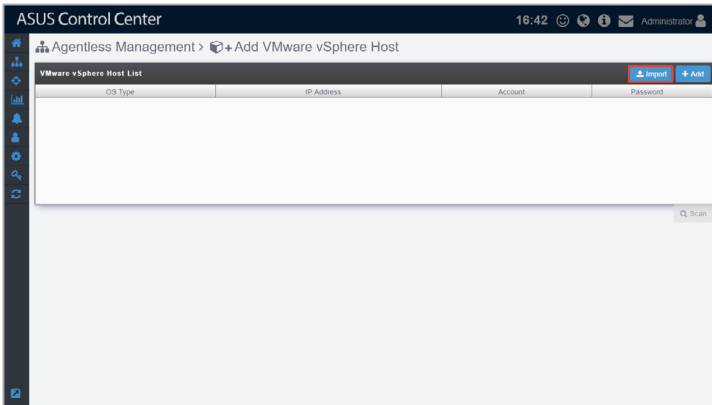


- Unavailable vSpheres will be listed as **Not Support**. You may click on the vSpheres to view details on why it is unavailable.
- vSpheres added may take a few minutes before they are displayed in the overview.



Adding multiple vSphere hypervisors

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.

The screenshot shows the ASUS Control Center interface. At the top, it says "ASUS Control Center" and "Agentless Management > + Add VMware vSphere Host". Below this is a table titled "VMware vSphere Host List" with columns for OS Type, IP Address, Account, and Password. A single entry is visible: OS Type: ESX, IP Address: 10.10.75.59, Account: root, Password: *****. To the right of the table are buttons for "Import", "Export", and "Add". Below the table is a "Scan Result Information" section with a "License count: 455" and a "Scan" button. It contains a table with columns for OS Type, IP Address, Scan Results, and Message. A single entry is visible: OS Type: ESX, IP Address: 10.10.75.59, Scan Results: support, Message: Success. A red box highlights the "support" and "Success" cells. At the bottom right of the scan results section is a button labeled "Add to Monitor".

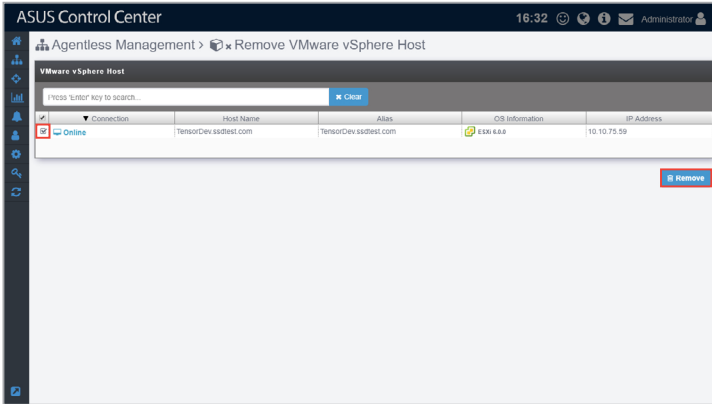
Exporting VMware vSphere Host List

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.

This screenshot is identical to the one above, showing the same interface and data. The only difference is that the "Export" button in the top right corner of the "VMware vSphere Host List" section is highlighted with a red box.

3.2.2 Remove vSphere

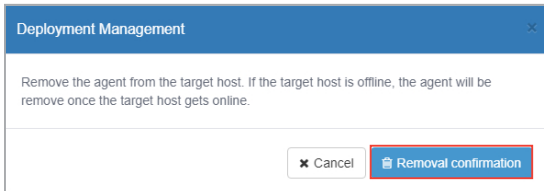
1. Check the vSphere(s) you wish to remove, then click **Remove**.



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



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



Chapter 4

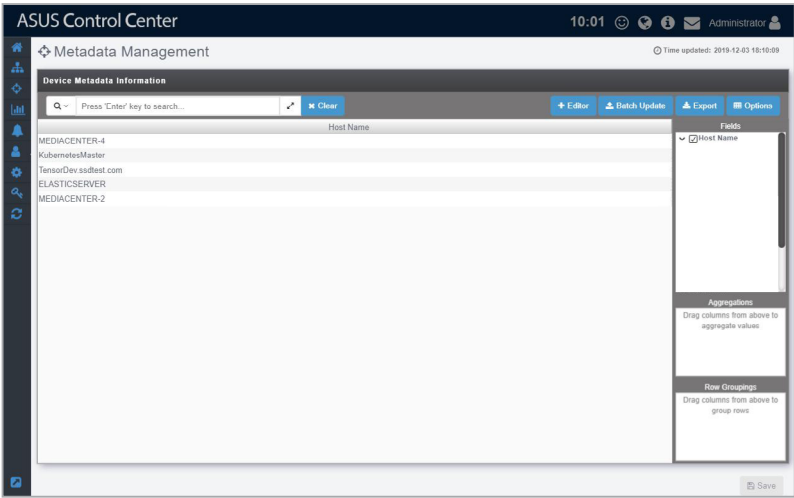
This chapter describes centralized management of metadata, BIOS flash, security, software, tasks, and power control of ASUS Control Center managed devices.

Centralized

4.1 Metadata Management

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

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

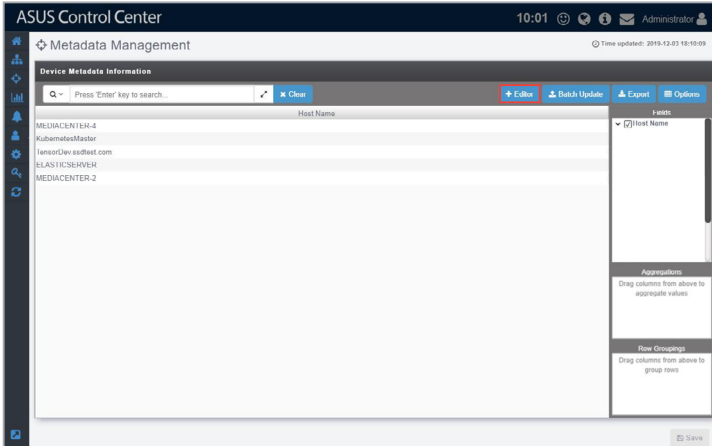


- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to **2.1.4 Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to **2.1.3 Options**.

Adding metadata fields

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

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



2. Enter the Field Name of the new metadata column, 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	Field Type	Default Value
	Department	String	SW
	Extension	Number	29631
	Production date	Date	2018-01-01

- (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.

Metadata Editor

Field Name:

Field Type: --Please Select--

+ Add

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

Save

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

Metadata Editor

Update

Field Name: Done.

Field Type: --Please Select--

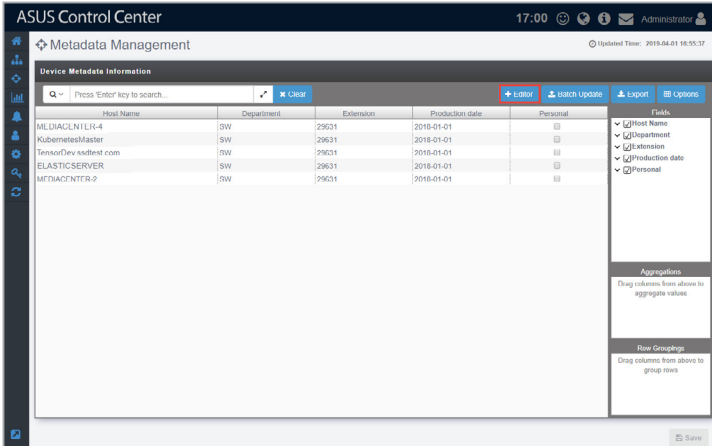
+ Add

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

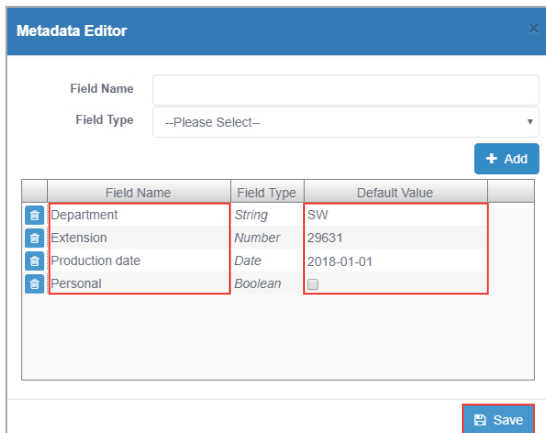
Save

Editing metadata fields

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

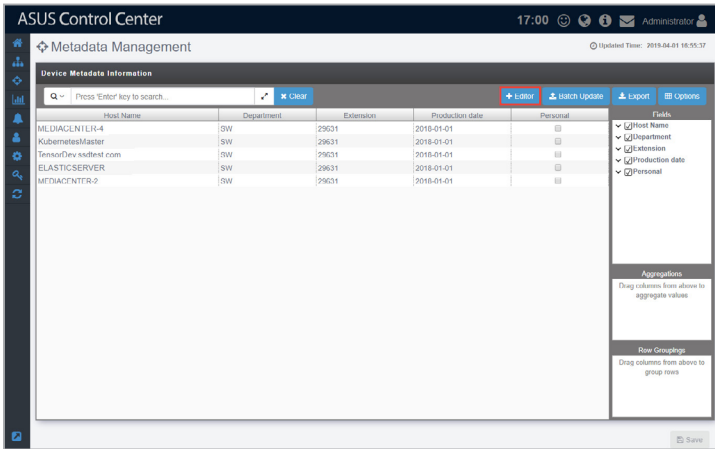



2. You can edit the **Field Name** and **Default Value** of existing metadata fields. When you are finished editing, click on **Save** to save the changes made.

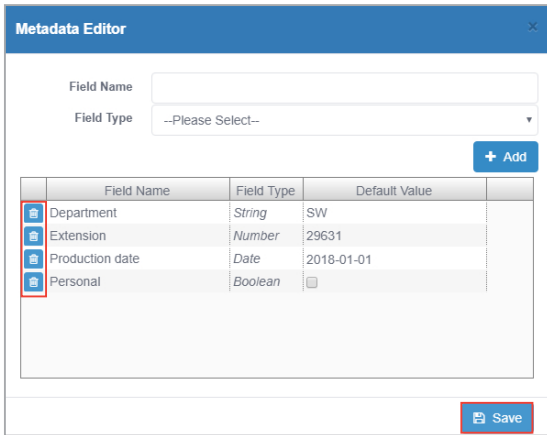


Deleting metadata fields

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



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



Editing the metadata value of a single device

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



- 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.

ASUS Control Center 11:15 Administrator

Metadata Management Time updated: 2018-12-01 18:10:09

Device Metadata Information

Press 'Enter' key to search. Clear Edit Batch Update Export Options

Host Name	Department	Extension	Production date	Personal	Flags
MS-URACE-N1E-K-4	ISW	29633	2018-01-01		
KubermakesMaster	ISW	29633	2018-01-01		
lanesoftDev.confnet.com	ISW	29176	2018-01-01		
ELASTICSEARCH	ISW	29633	2018-01-01		
ELASTICSEARCH-2	ISW	29633	2018-01-01		

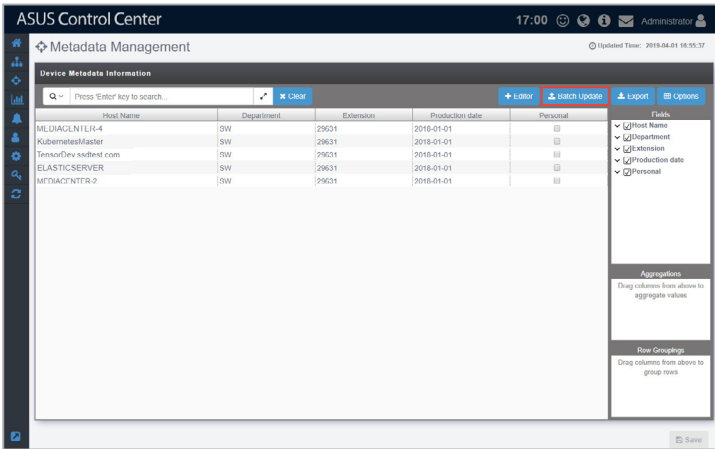
Aggregation: Drag columns from above to aggregate values

Row Groupings: Drag columns from above to group rows

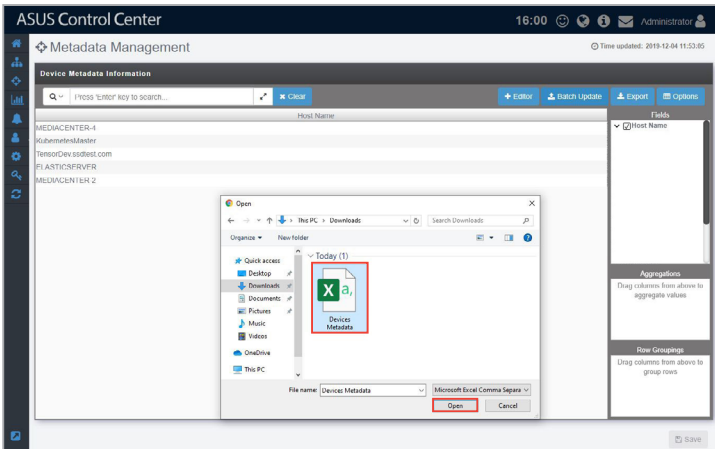
Save

Editing the metadata value of multiple devices

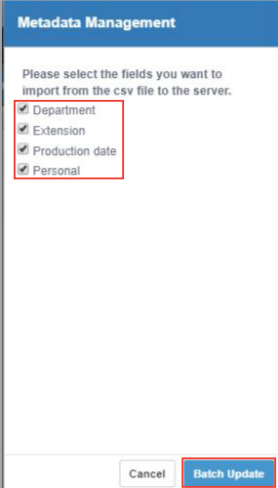
- 1. Click on **Batch Update**.



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

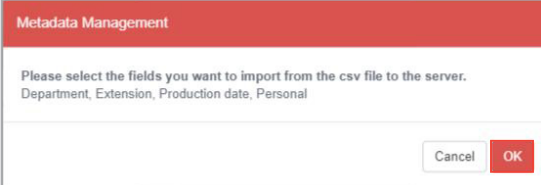


3. Select the metadata field columns to update to the server, then click **Batch Update**.



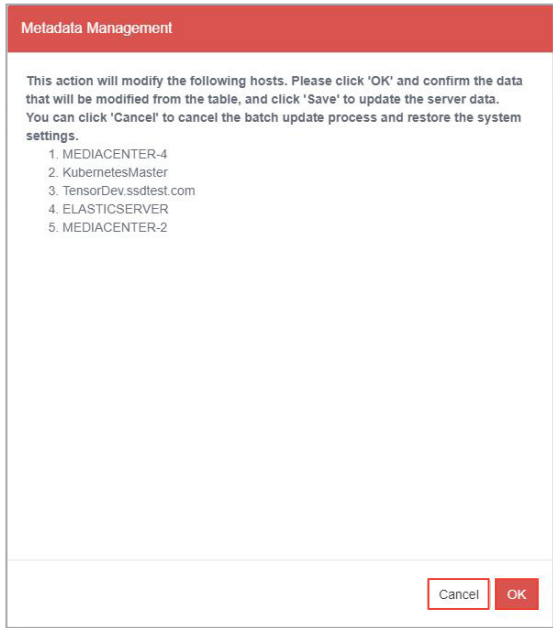
The screenshot shows a dialog box titled "Metadata Management" with a blue header. The main text reads: "Please select the fields you want to import from the csv file to the server." Below this text is a list of four items, each with a checked checkbox: "Department", "Extension", "Production date", and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

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

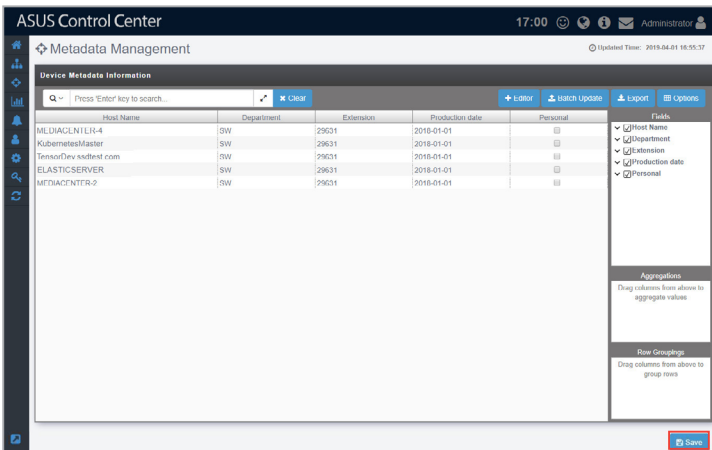


The screenshot shows a confirmation dialog box titled "Metadata Management" with a red header. The main text reads: "Please select the fields you want to import from the csv file to the server." Below this text, the selected fields are listed: "Department, Extension, Production date, Personal". At the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

- 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.



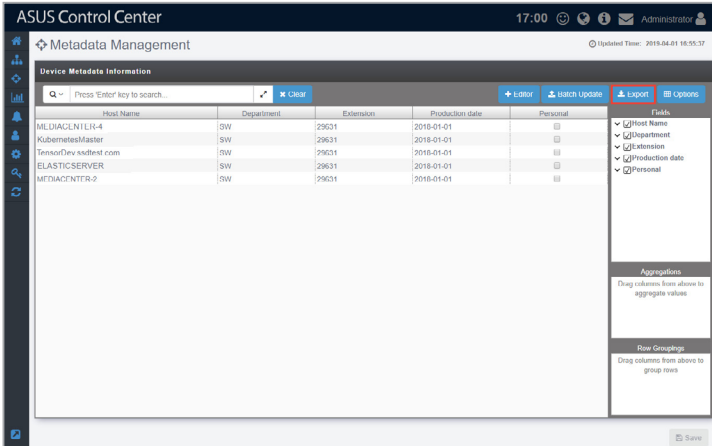
- If you clicked **OK** in the previous step, click on **Save** to save the changes made.



Exporting the metadata value

Exporting the metadata to a CSV file allows you to edit multiple metadata fields together, then update them by importing it back into ASUS Control Center. To import the changes made to the metadata in the CSV file, refer to **Editing the metadata of multiple devices** section under **4.1.2 Add metadata**.

1. Click on **Export**.



The screenshot shows the 'ASUS Control Center' interface with the 'Metadata Management' section active. The 'Device Metadata Information' table is displayed with the following data:

Host Name	Department	Extension	Production date	Personal	Fields
MILJAGN1LR-4	SW	29631	2018-01-01	<input type="checkbox"/>	<input checked="" type="checkbox"/> Host Name
KubernetesMaster	SW	29631	2018-01-01	<input type="checkbox"/>	<input checked="" type="checkbox"/> Department
TenonDev.esstest.com	SW	29631	2018-01-01	<input type="checkbox"/>	<input checked="" type="checkbox"/> Extension
ELASTICSERVER	SW	29631	2018-01-01	<input type="checkbox"/>	<input checked="" type="checkbox"/> Production date
METADACENTER-2	SW	29631	2018-01-01	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Personal

The 'Export' button is highlighted with a red box. The interface also includes a search bar, 'Clear', 'Editor', 'Watch Update', 'Options', 'Aggregations', and 'Row Groupings' sections.


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

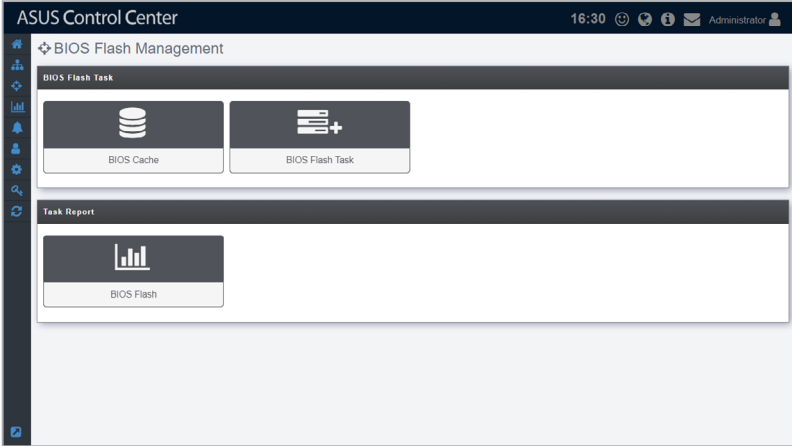


- Use a text editor when editing the exported CSV file.
- Do not edit the **aswm_HostName** and **ClientGUID** fields.
- Only the existing data in the CSV file may be edited, adding new rows and columns to the CSV file may cause failure when importing to the ASUS Control Center.

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.

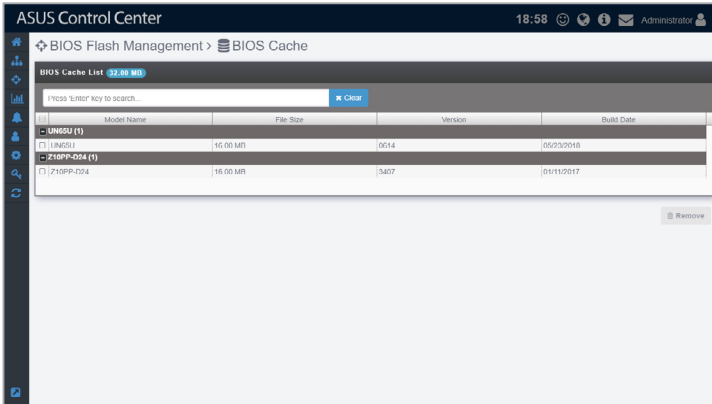
To access **BIOS Flash Management**, click  > **BIOS Flash Management** in the left menu.



- 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 **2.1.4 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 **2.1.3 Options**.

4.2.1 BIOS Cache

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



Adding a BIOS cap file to the BIOS Cache

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

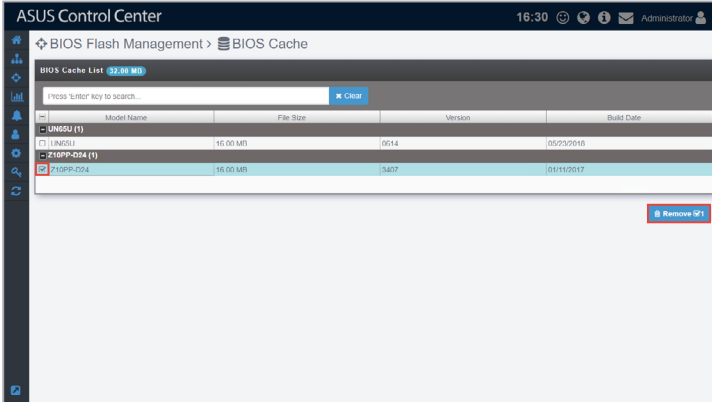


- For more details on manually uploading a BIOS cap file when flashing the BIOS from **Device Information**, please refer to the **BIOS Flash** section under **2.2.7 BIOS**.
- For more details on manually uploading a BIOS cap file when using the **BIOS Flash Task** function, please refer to the **Manually uploading the BIOS cap file** section under **4.2.2 BIOS Flash Task**.

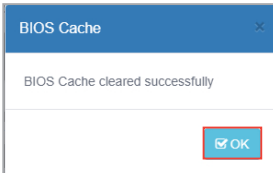
Removing BIOS cap files from BIOS Cache

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

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

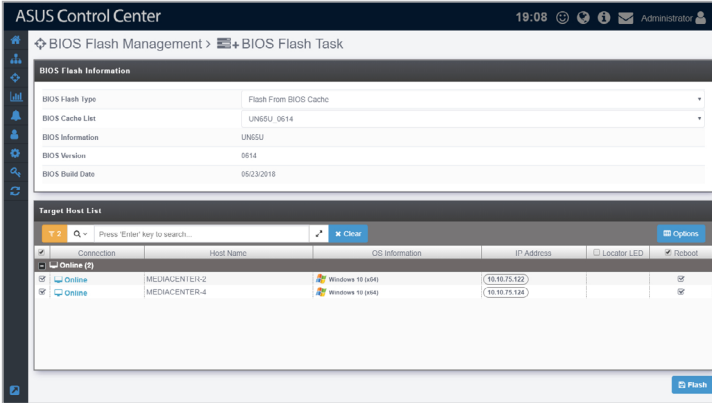


2. When the BIOS cap file(s) have been successfully removed, click **OK**.



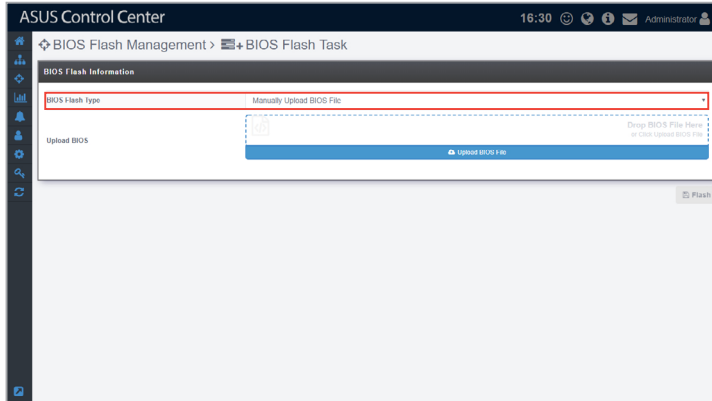
4.2.2 BIOS Flash Task

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

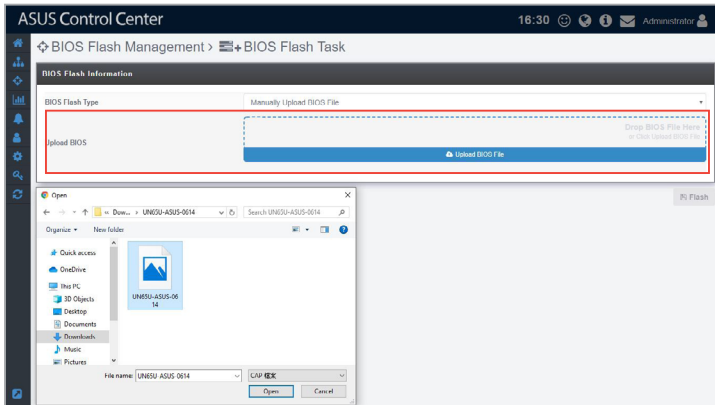


Manually uploading the BIOS cap file

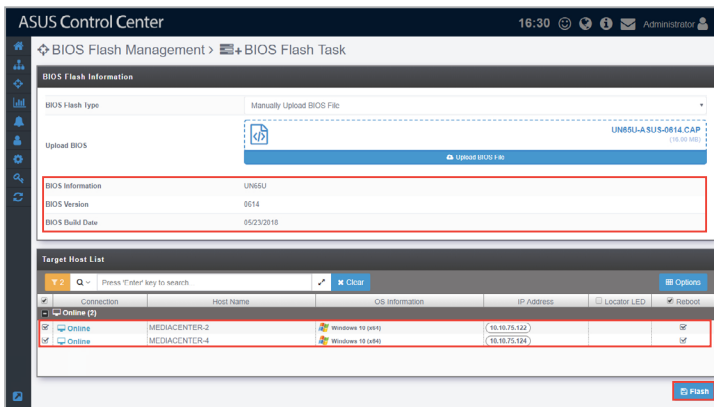
1. Select **Manually Upload BIOS File** from the drop down menu in the **BIOS Flash Type** field.



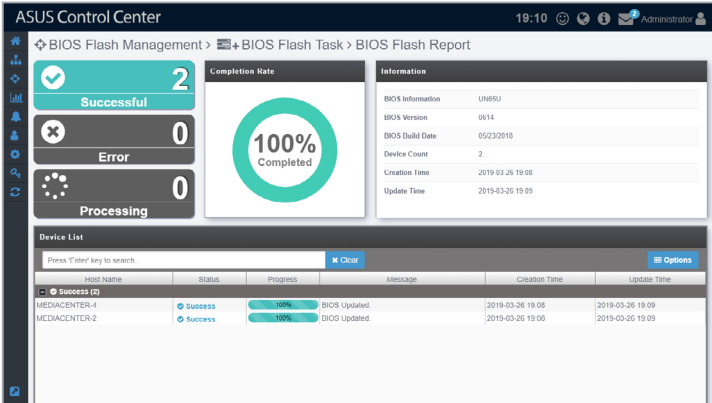
2. Drag and drop the BIOS cap file in the dotted square, or click on **Upload BIOS File** to select a BIOS cap file to upload.



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

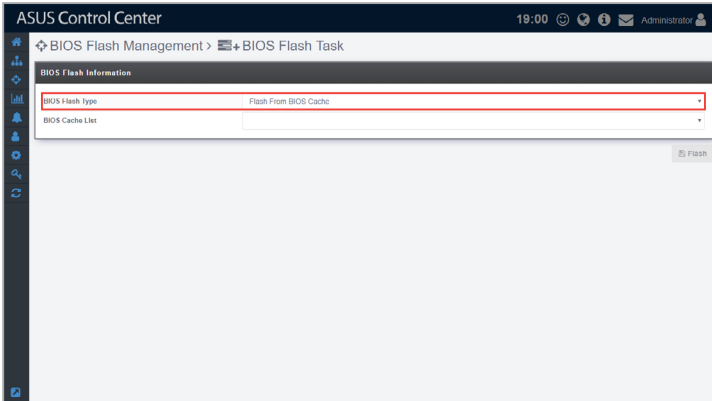


- Once the flash process is finished, a BIOS Flash Report should appear allowing you to check the BIOS Flash status and progress of all selected devices.

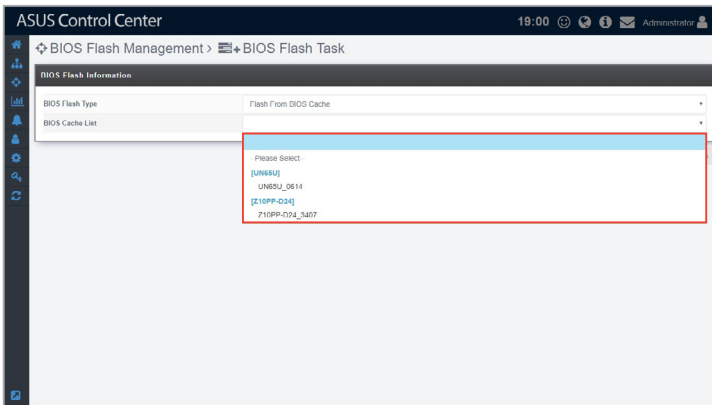


Selecting the BIOS cap file from the BIOS cache

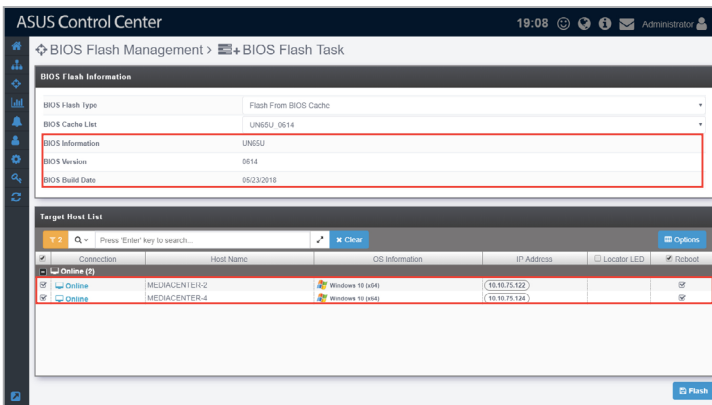
- Select **Flash From BIOS Cache** from the drop down menu in the **BIOS Flash Type** field.



2. Select a BIOS Cache List.



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



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

ASUS Control Center 19:10 Administrator

BIOS Flash Management > BIOS Flash Task > BIOS Flash Report

Successful 2

Error 0

Processing 0

Completion Rate

100% Completed

Information

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

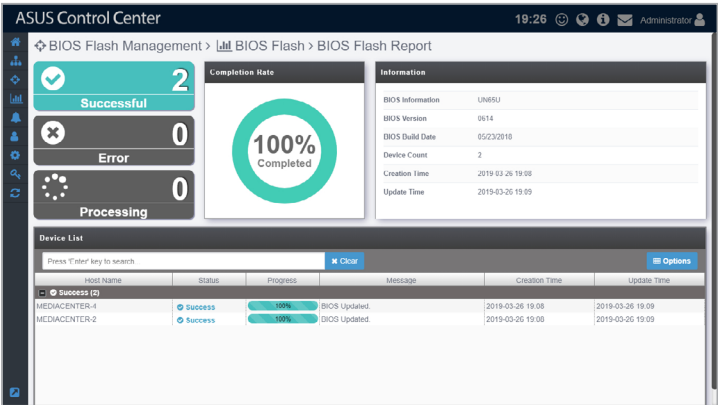
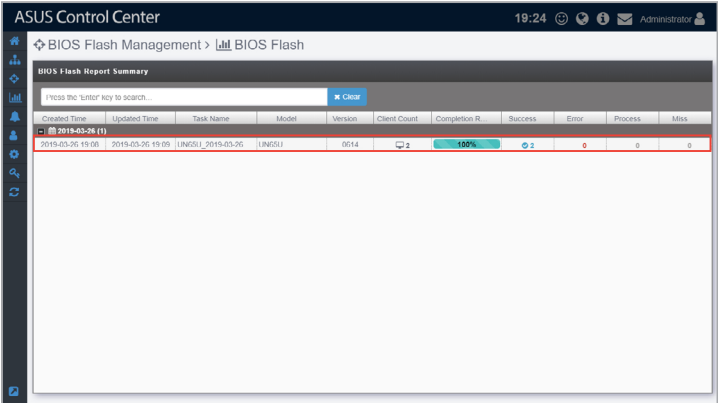
Device List

Press 'Enter' key to search

Host Name	Status	Progress	Message	Creation Time	Update Time
Success (2)					
MEDACENTER-1	Success	100%	BIOS Updated.	2019-03-26 19:08	2019-03-26 19:09
MEDACENTER-2	Success	100%	BIOS Updated.	2019-03-26 19:00	2019-03-26 19:09

4.2.3 BIOS Flash Task Report

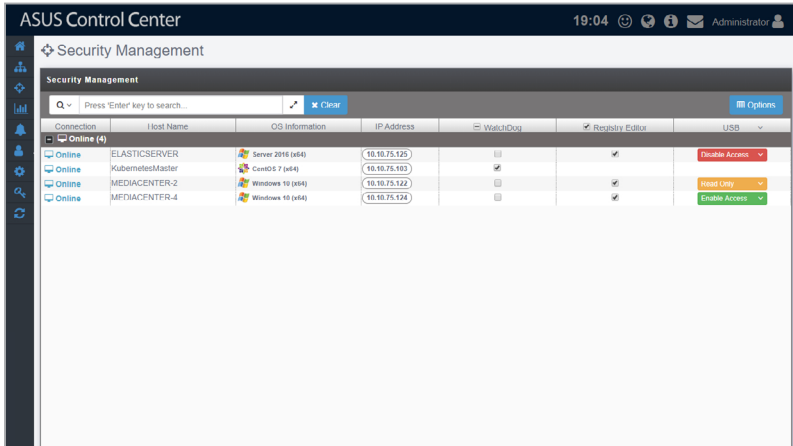
The **BIOS Flash Task Report** function will display a history of BIOS flashes performed using ASUS Control Center. Selecting a BIOS flash task listed in the BIOS Flash Report Summary will allow you to view information on the BIOS, which devices were flashed, and also the status of the BIOS flash to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



4.3 Security Management

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

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



Connection	Host Name	OS Information	IP Address	WatchDog	Registry Editor	USB
Online (4)						
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disable Access
Online	KubernetesMaster	CentOS 7 (x64)	10.10.75.103	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Install Cert
Online	MEDIACENTER-2	Windows 10 (x64)	10.10.75.122	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Enable Access
Online	MFDIACENTER-4	Windows 10 (x64)	10.10.75.124	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Enable Access



- 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 **2.1.4 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 **2.1.3 Options**.
- **Registry Editor** and **USB** configurations are only available for Windows system 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 is 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**.

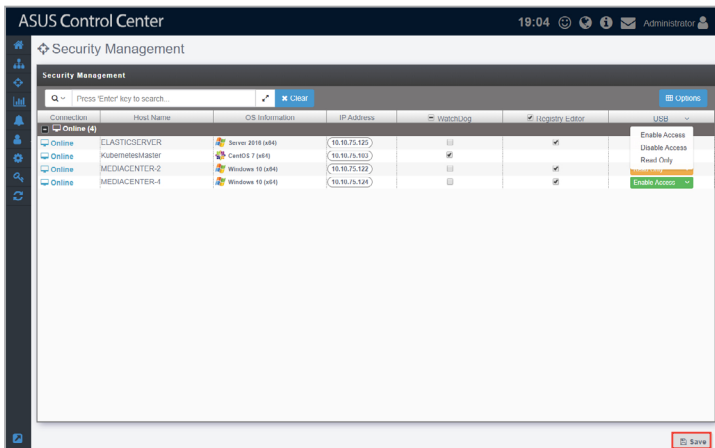
- **Registry Editor (Windows only)**

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.

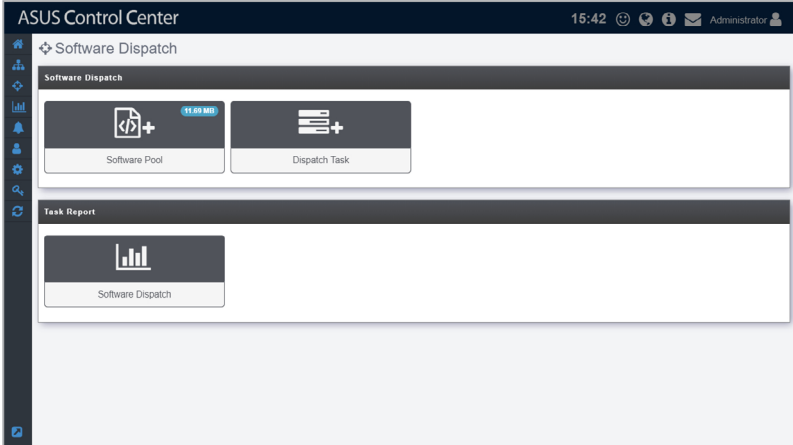
2. Click on **Save** once you have finished making changes to save the changes made.



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.

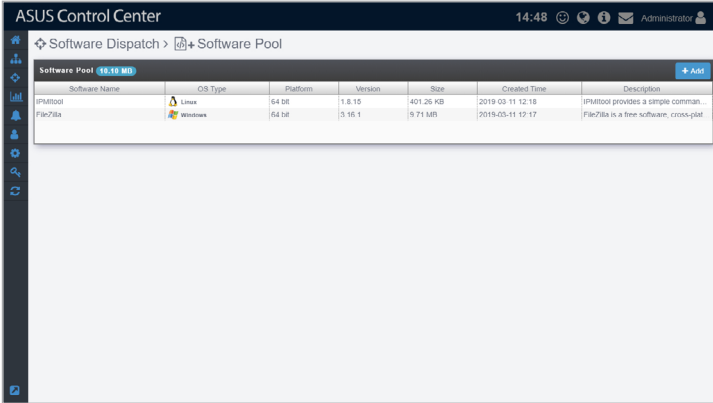
To access **Software Dispatch**, click  > **Software Dispatch** in the left menu.



- 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 **2.1.4 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 **2.1.3 Options**.

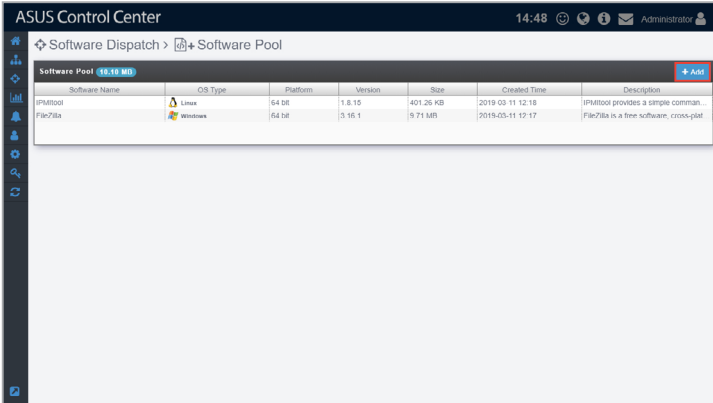
4.4.1 Software Pool

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

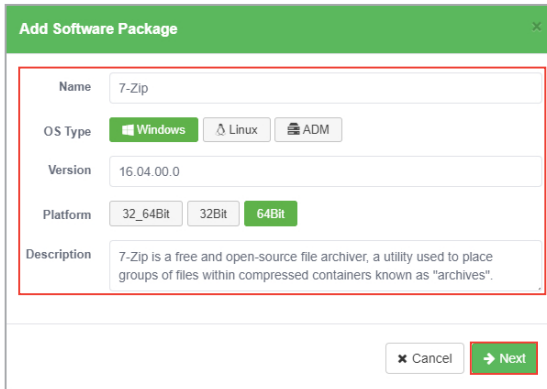


Adding software packages to the Software Pool

1. Click on **Add**.



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



Add Software Package

Name: 7-Zip

OS Type: Windows Linux ADM

Version: 16.04.00.0

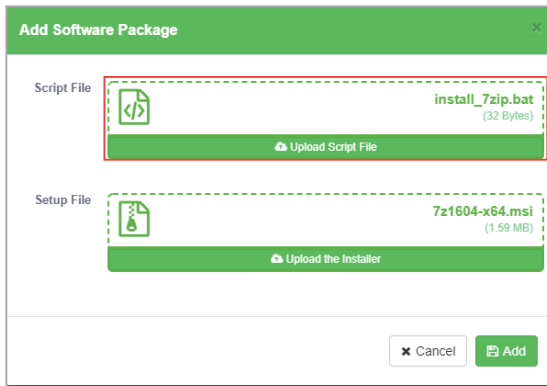
Platform: 32_64Bit 32Bit 64Bit

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


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>.

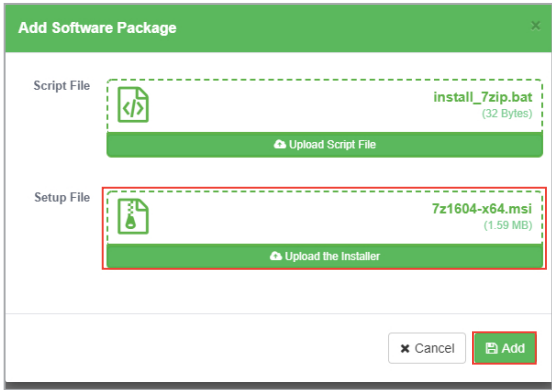


Add Software Package

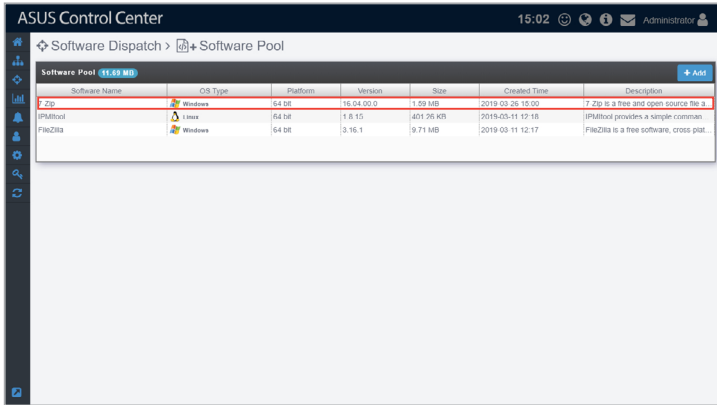
Script File:  **install_7zip.bat** (32 Bytes)

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**.

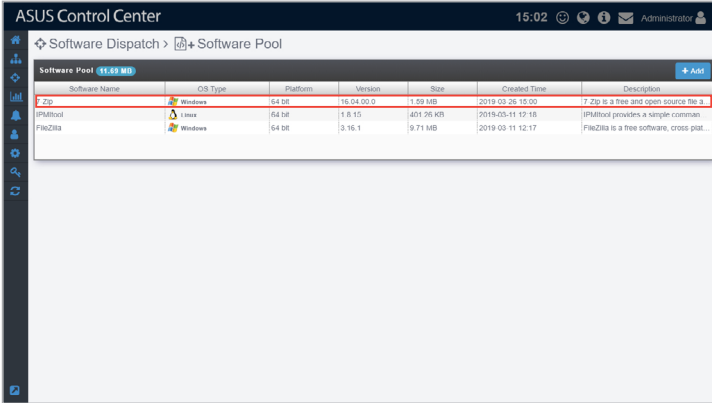


- 5. The newly added software package will appear in the Software Pool list.

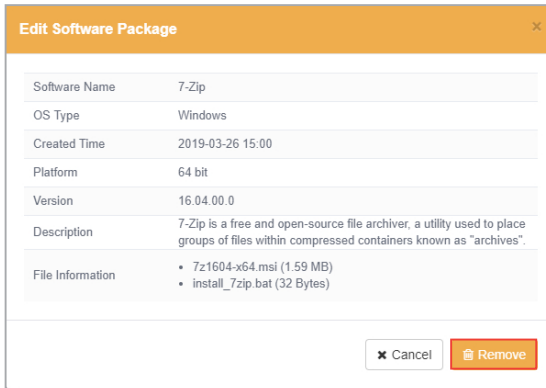


Removing software packages from the Software Pool

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



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



4.4.2 Software Dispatch Task

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



To add or view software packages in the Software Pool, please refer to **4.4.1 Software Pool**.

The screenshot shows the ASUS Control Center interface for the Software Dispatch Task. The top navigation bar includes the title 'ASUS Control Center', the time '15:30', and the user 'Administrator'. The main content area is titled 'Software Dispatch > Software Dispatch Task'.

Package List

Name	Version	Platform	OS Type	File Informa...	Description	Time Created
7-Zip	16.04.00.0	64 bit	Windows	1.53 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
IPMftool	1.8.15	64 bit	Linux	401.26 KB	IPMftool provides a simple command-line ut...	2019-03-11 12:18

Selected package: 7-Zip: D/E: 64 (16.04.00.0)

Device List

Connection	Host Name	OS Information	IP Address	Platform
Online (0)				
Online	ELASTICSERVER	Server 2016 (x64)	10.10.75.125	64 bit
Online	MEFIACENTER-2	Windows 10 (x64)	10.10.75.122	64 bit
Online	MEFIACENTER-4	Windows 10 (x64)	10.10.75.124	64 bit

Dispatch RC 1

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 15:30 Administrator

Software Dispatch > Software Dispatch Task

Package List

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

Name	Version	Platform	OS Type	File Info	Description	Time Created
7-Zip	16.04.00	64 bit	Windows	1.59 MB	7-Zip is a free and open-source file archiver...	2019-03-26 15:00
FlacZilla	3.16.1	64 bit	Windows	9.71 MB	FlacZilla is a free software, cross platform FT...	2019-03-11 12:17
IPMTool	1.8.15	64 bit	Linux	401.26 KB	IPMTool provides a simple command-line int...	2019-03-11 12:18

Selected package: 7-Zip, Bit: 64 (16.04.00.0)

Device List

Press 'Enter' key to search. Clear Option

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

Dispatch 8/1

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 15:30 Administrator

Software Dispatch > Software Dispatch Task

Package List

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

Name	Version	Platform	OS Type	File Info	Description	Time Created
7-Zip	16.04.00	64 bit	Windows	1.59 MB	7-Zip is a free and open-source file archiver...	2019-03-26 15:00
FlacZilla	3.16.1	64 bit	Windows	9.71 MB	FlacZilla is a free software, cross platform FT...	2019-03-11 12:17
IPMTool	1.8.15	64 bit	Linux	401.26 KB	IPMTool provides a simple command-line int...	2019-03-11 12:18

Selected package: 7-Zip, Bit: 64 (16.04.00.0)

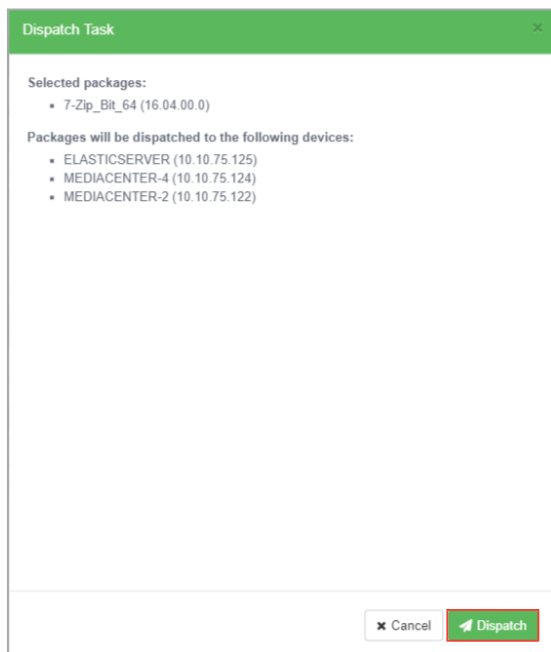
Device List

Press 'Enter' key to search. Clear Option

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

Dispatch 8/1

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



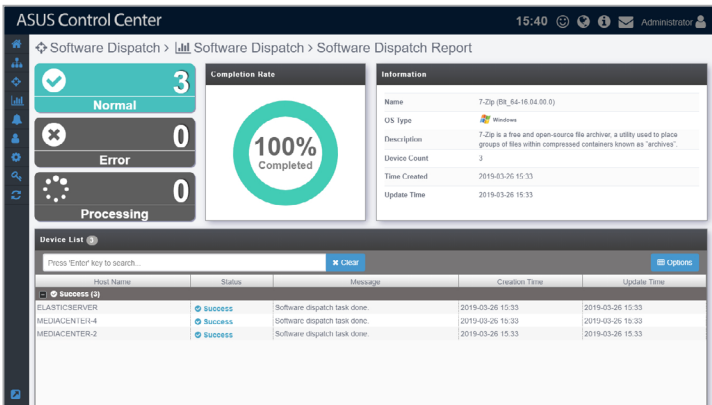
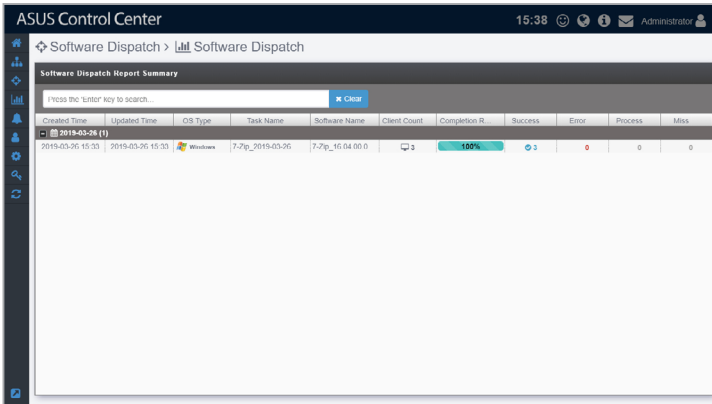
4. After the software packages have been dispatched, you will be redirected to the Software Dispatch Task Report screen.



For more details on the Software Dispatch Task Report, refer to **4.4.3 Software Dispatch Task Report**.

4.4.3 Software Dispatch Task Report

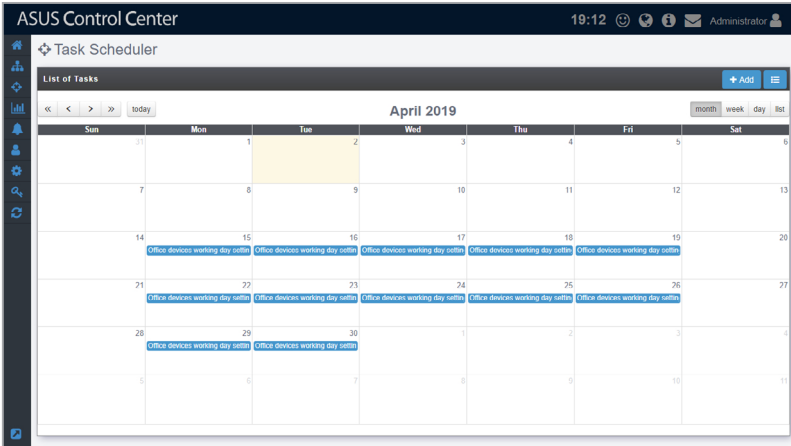
The **Software Dispatch Task Report** function will display a history of all software dispatch tasks performed using ASUS Control Center. Selecting a software dispatch task listed in the Software Dispatch Report Summary will allow you to view information on the software, which devices the software was dispatched to, and also the status of the software dispatch to managed devices. This provides you with a quick overview of your software dispatch tasks and also help you pinpoint failed software dispatches.



4.5 Task Scheduler



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


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

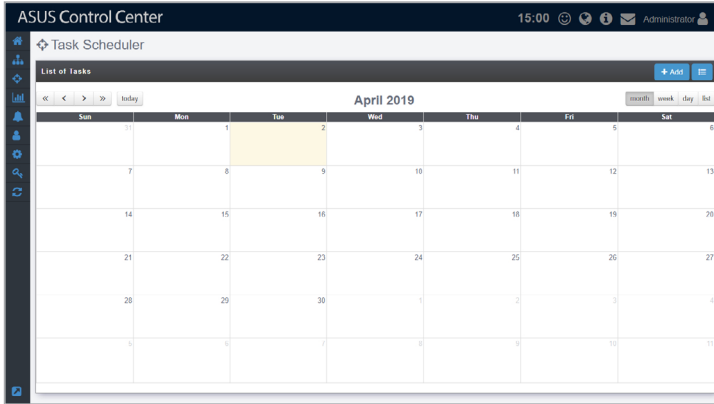


- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to **2.1.4 Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to **2.1.3 Options**.







Task Scheduler Overview

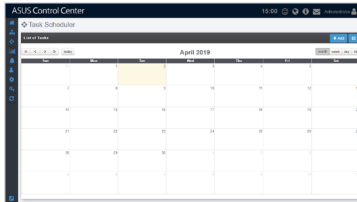
Toggle between the different Task Scheduler views by clicking on the  /  icon. You can click on any task displayed to view more details on the task.

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

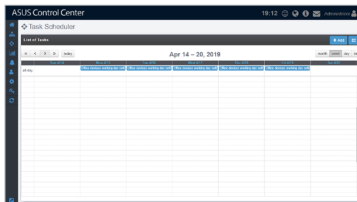


You can switch the time period displayed in Calendar view by using the following:

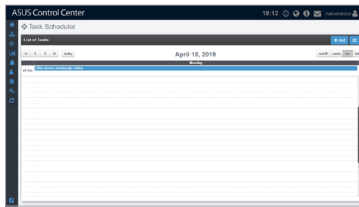
-  View previous year
-  View next year
-  View previous month / week / day
-  View next month / week / day
-  Move to the current day. The current day will be highlighted on the calendar.
-  Display month view



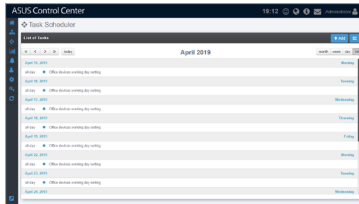
-  Display week view



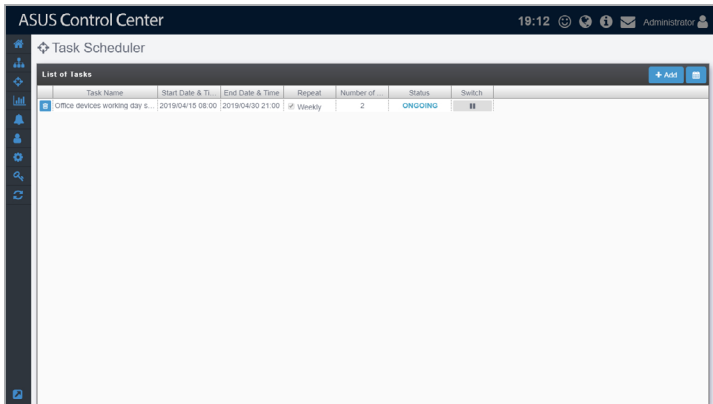
day Display day view



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

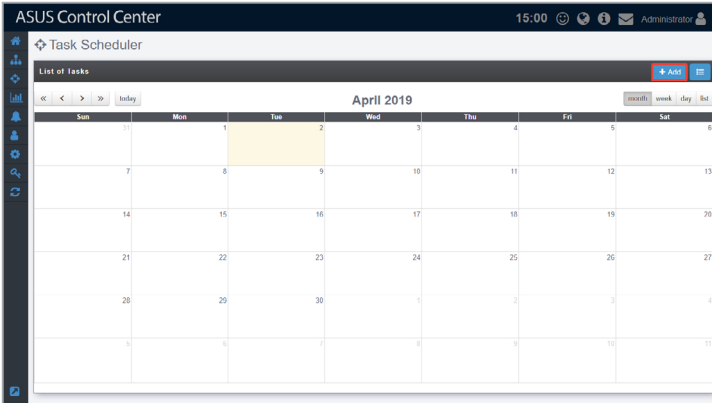


☰ : History list of all tasks, including Task Name, Start Date & Time, End Date & Time, Repeat, Number of Clients, Status, and Switch.

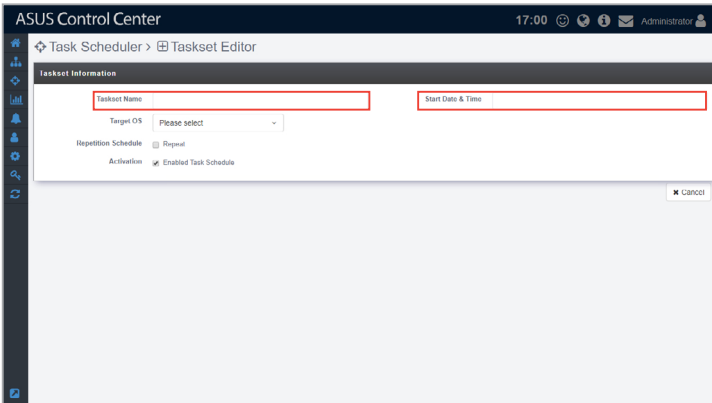


Adding a scheduled task

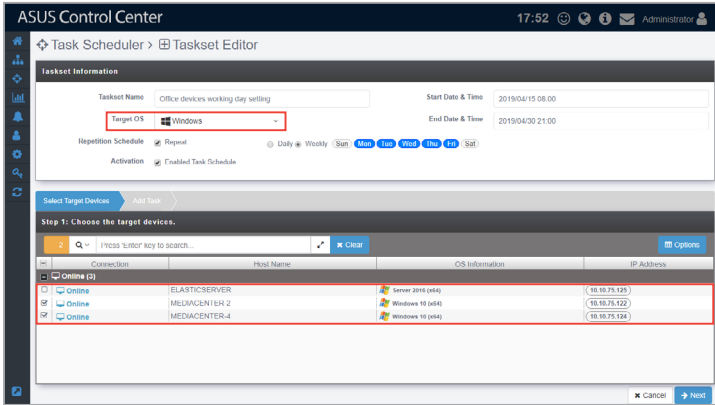
1. Click on **Add**.



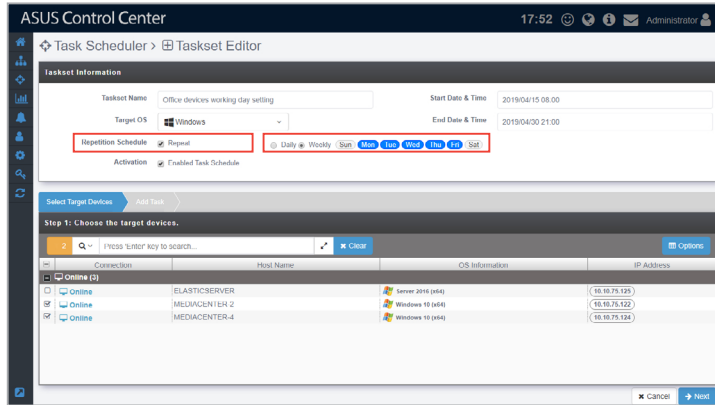
2. Enter the **Taskset Name**, then select a **Start Date & Time**.



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



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



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



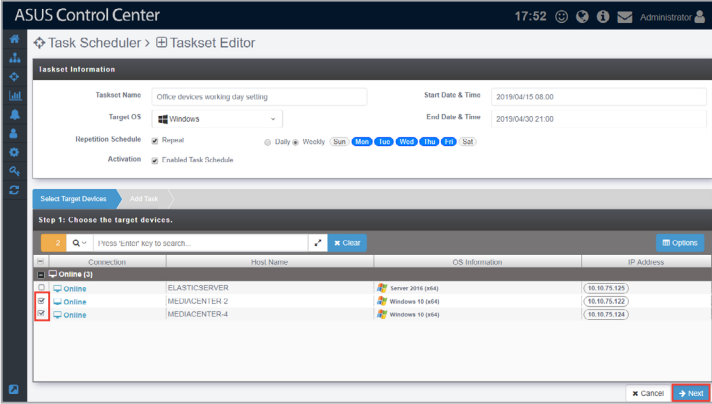
The **End Date & Time** option only appears when **Repeat** has been checked.

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

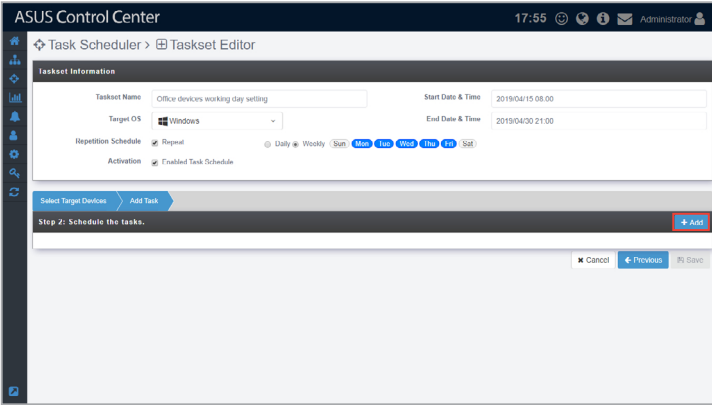
6. **Enabled Task Schedule** is enabled by default, if you wish to disable the task, uncheck **Enabled Task Schedule** in the **Activation** field.

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

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



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



- 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:

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:

Action Type	Options	Description
Service Control	Service Name:	Enter the name of the service. If you are unsure of the name of the service you can refer to 2.2.5 Software .
	Start:	Activate the service.
	Stop:	Stop the service.
	Restart:	Restart the service.

Software Dispatch:

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:

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, Power Off, Power Reboot

Cancel Save

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 18:26 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 Wooly Sun Mon Tue Wed Thu Fri Sat

Activation: Enabled Task Schedule

Select Target Devices Add Task

Step 2: Schedule the tasks.

1 Power On Power Control

2 SNMP TRAP Service Control

3 7-Zip Software Dispatch

4 USB Control Security

Cancel Previous Save

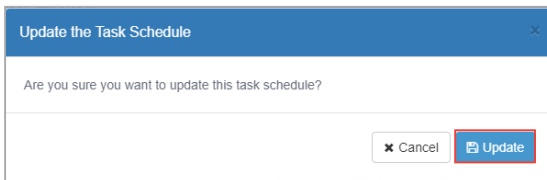
Editing a scheduled task

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.



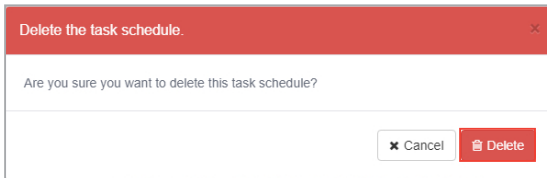
You can refer to step 2 to 12 of the **Add Scheduled task** section of **4.5 Task Scheduler** for the steps on editing a task; the steps are the same.

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



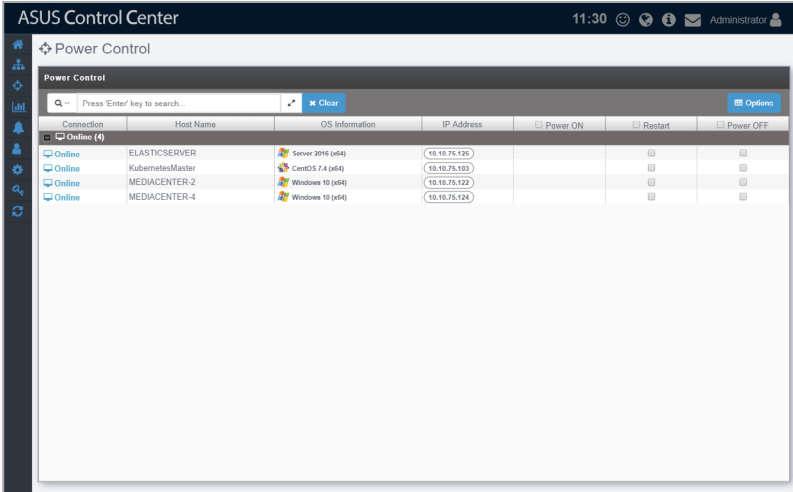
Deleting a scheduled task

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



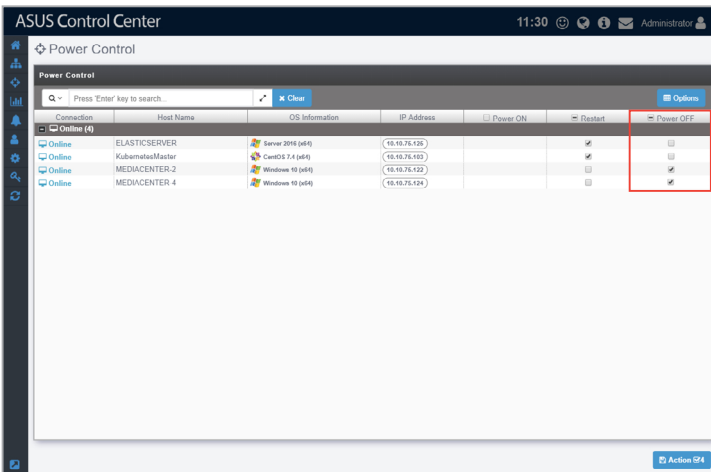
4.6 Power Control

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



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

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





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).

ASUS Control Center 11:30 Administrator

Power Control

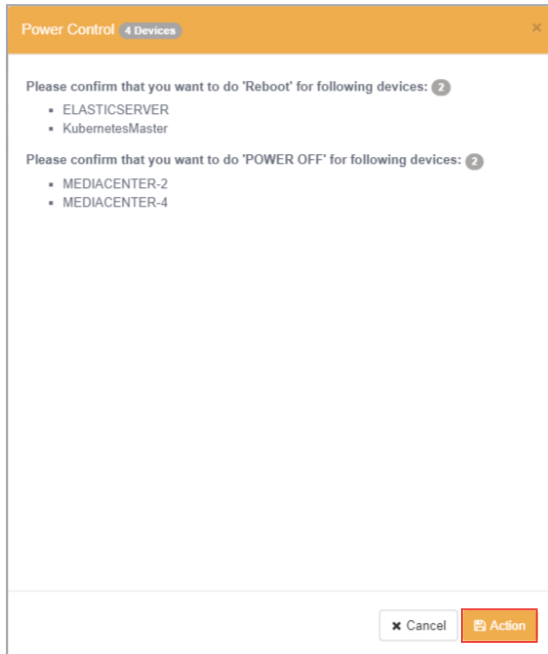
Power Control

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

Connection	Host Name	OS Information	IP Address	Power ON	Restart	Power OFF
Online (4)						
Online	ELASTICSERVER	Server 2016 (x64)	10.10.76.128	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Online	KubamatasMaster	CentOS 7 (x64)	10.10.76.102	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Online	MEDVACENTER-2	Windows 10 (x64)	10.10.76.122	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Online	MEDVACENTER 4	Windows 10 (x64)	10.10.76.124	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Action 4

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.



Chapter 5

This chapter describes the various settings available for reports on devices and software.

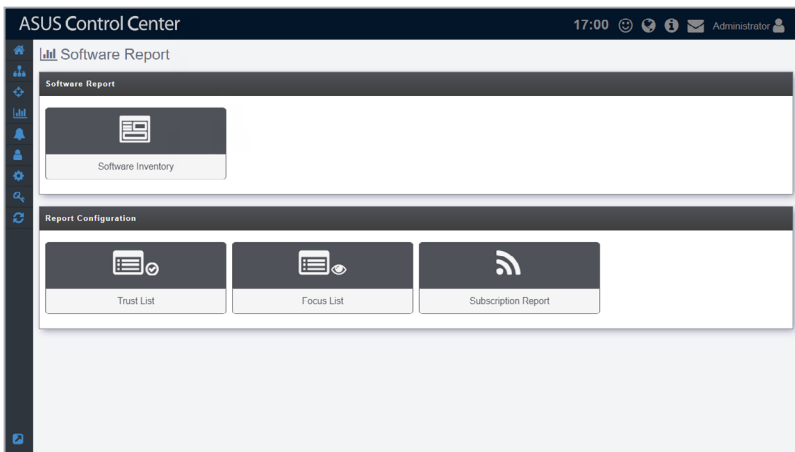
5.1 Software Report



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**.



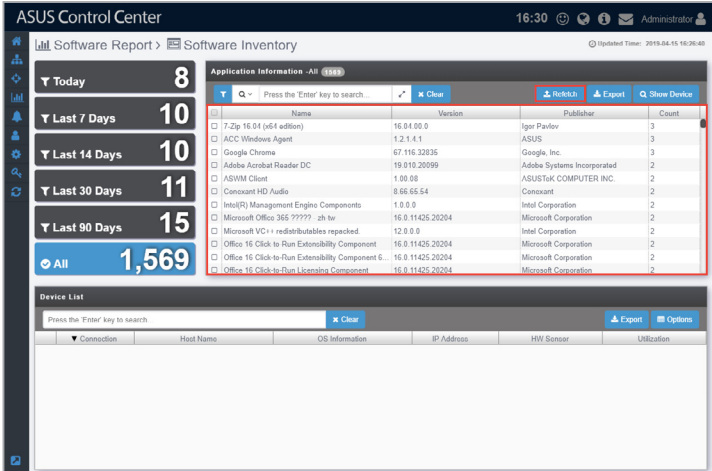
- If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to **2.1.4 Search and Filter devices** section.
- If the Options function is available for a function in this section You can group managed devices according to metadata fields. For more information refer to **2.1.3 Options**.

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.

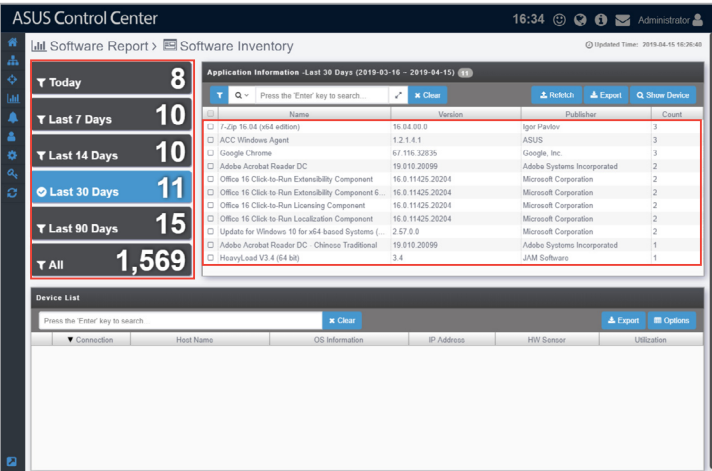
Refetch Application

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



Filter newly installed applications

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



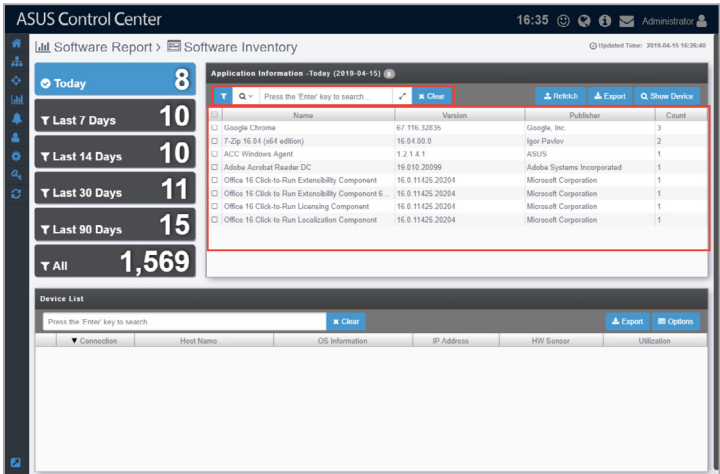
Search for applications using keywords


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

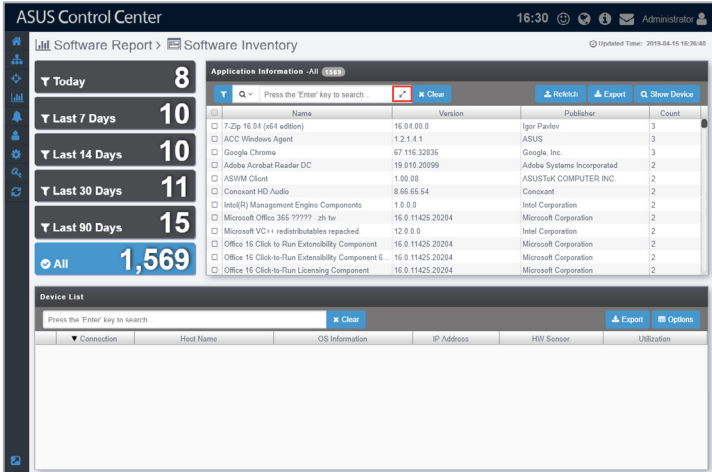
1. Enter the keywords you wish to search for using the following methods:

- **Directly entering the keywords**

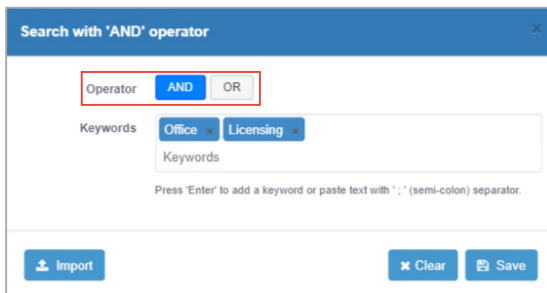
Enter the keyword(s) you wish to search with into the search bar and press <Enter>. Click on to toggle between searching with the **AND** operator or **OR** operator. Searching using **AND** will search for items which contain all keywords entered, whilst searching using **OR** will search for items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



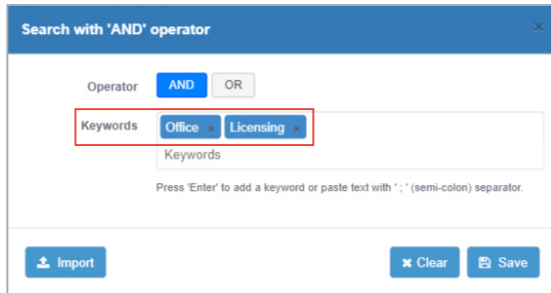
- Importing multiple keywords from a .csv file
 - a. Click on  to bring up the search condition pop-up window.



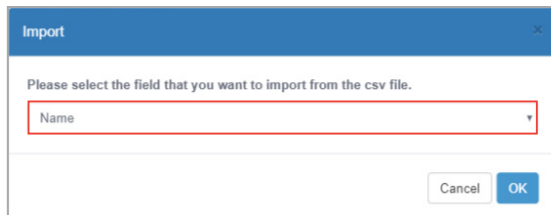
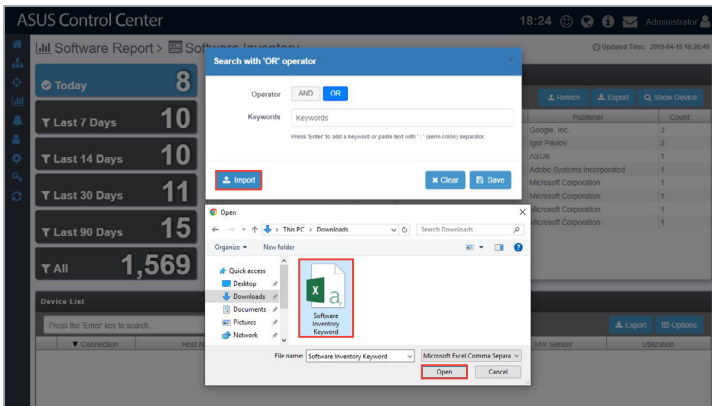
- b. Select the operator you wish to use. **AND** will search for items which contain all the keywords entered, whilst **OR** will search for items which contain at least one of the keywords entered.



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



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.



- 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.

Buttons: Import, Clear, Save

2. If you wish to view the devices an application is installed on, check the application, then click on **Show Device**. The list of devices the selected application is installed on should be displayed in the **Device List** window

ASUS Control Center 14:33 Administrator


Software Report > Software Inventory (Updated Time: 2019-04-09 11:08:31)

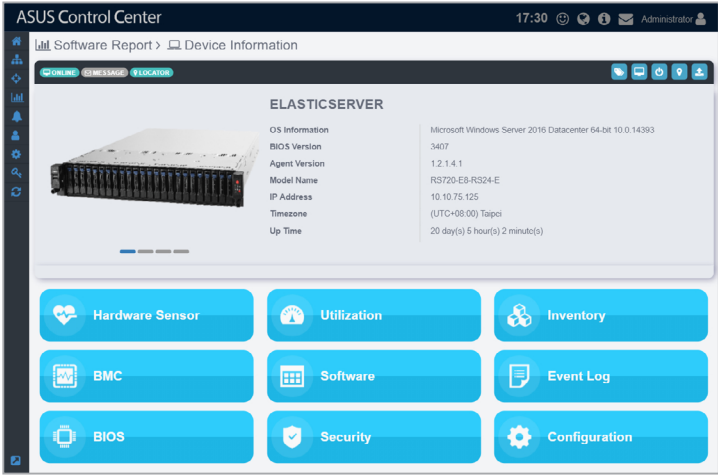
Application Information - Today (2019-04-15)

Name	Version	Publisher	Count
Google Chrome	73.0.3683.103	Google, Inc	3
iTop 16.04 (i64 edition)	16.04.09.0	iTop Reader	2
ACC Windows Agent	1.2.1.1.1	ASUS	1
Adobe Acrobat Reader DC	19.010.20999	Adobe Systems Incorporated	1
Office 16 Click to Run Extensibility Component	16.0.11426.20204	Microsoft Corporation	1
Office 16 Click to Run Extensibility Component 6	16.0.11426.20204	Microsoft Corporation	1
Office 16 Click to Run Licensing Component	16.0.11426.20204	Microsoft Corporation	1
Office 16 Click to Run Localization Component	16.0.11426.20204	Microsoft Corporation	1

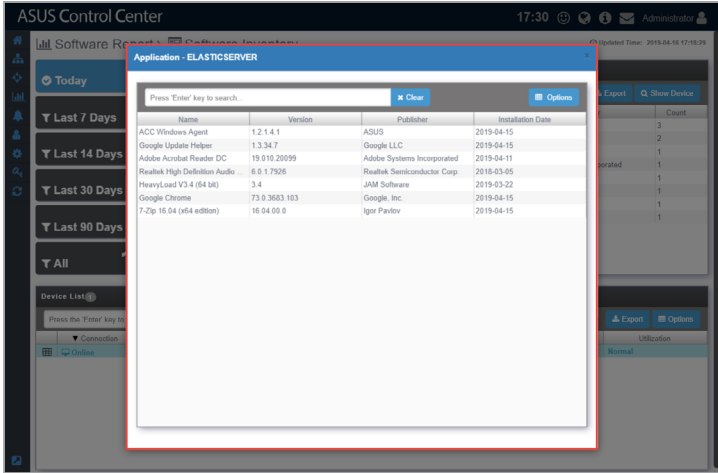
Device List

Connection	Host Name	OS Information	IP Address	HV Sensor	Utilization
Online	ELASTICSERVER	server 2016 (x64)	(10.19.76.128)	Normal	Normal

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



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

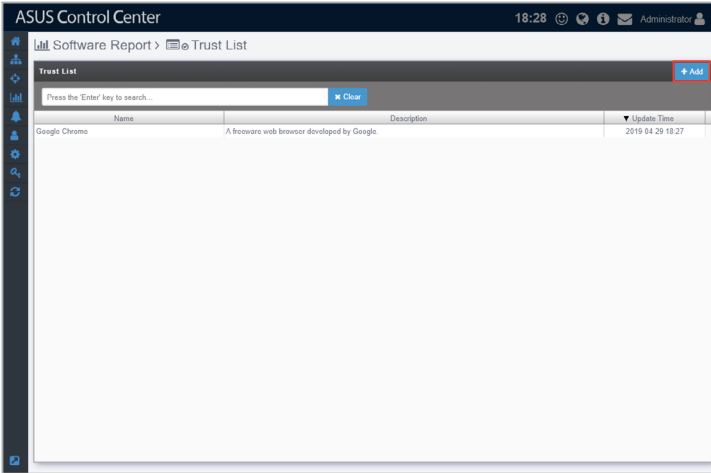


5.1.2 Trust List

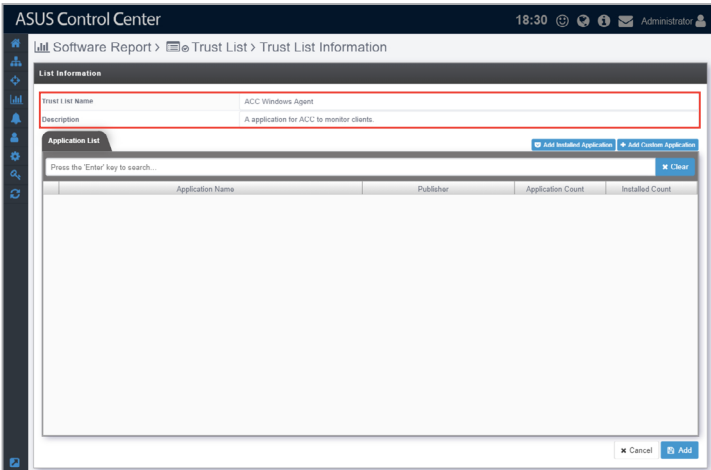
You may view your trusted lists or add new trusted lists, these applications are not included in the subscribed software report generated. This allows you to create white lists of applications which you trust and do not need to monitor, such as trusted applications which are mandatory on all devices within a company.

To create a new trusted list:

1. Click on **Add** on the Trust List main screen to create a new trust list.



2. Enter the Trust list name as well as a brief description of the trust list into their respective fields.

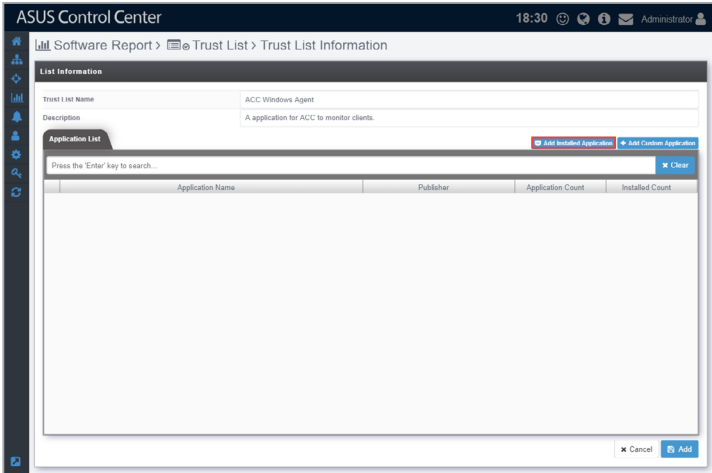


3. You may add applications to your trust list using the following methods:

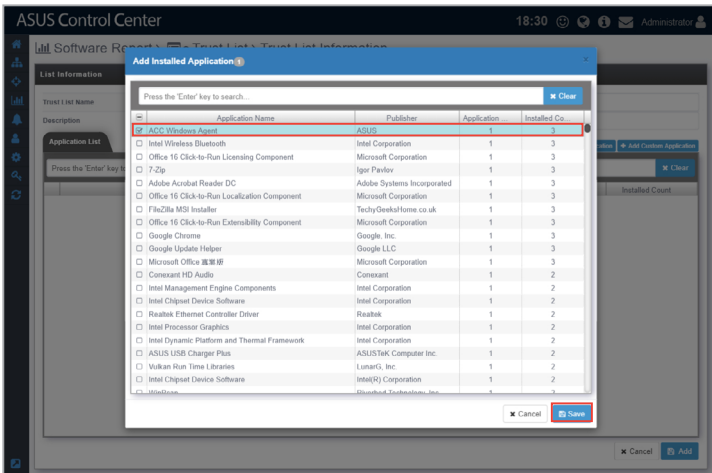
- Selecting multiple applications

You may select multiple applications from a list of all your installed applications to add to your trusted list.

a. Click on **Add Installed Application**.



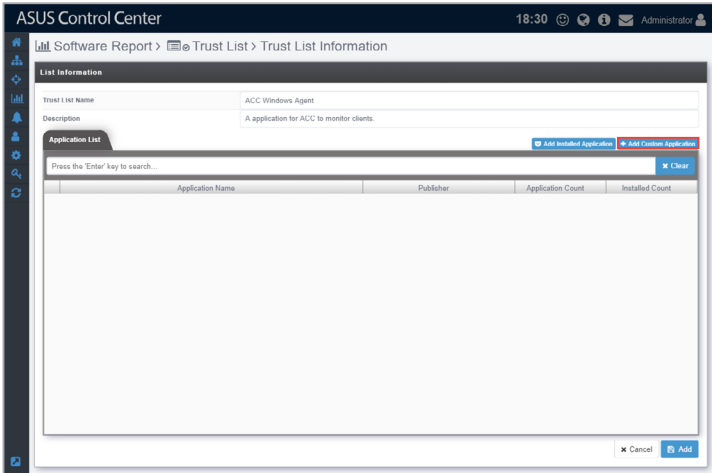
b. Scroll through the list of installed applications and check the applications you wish to add to your trust list, then click on **Save**.



- Manually adding a custom application

You may use this method if you cannot find the application you wish to add in the **Add Installed Application** list, or if you already know which application you wish to add.

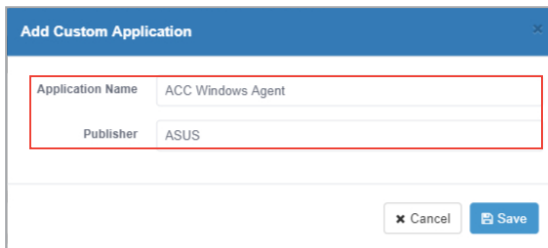
- a. Click on **Add Custom Application**.



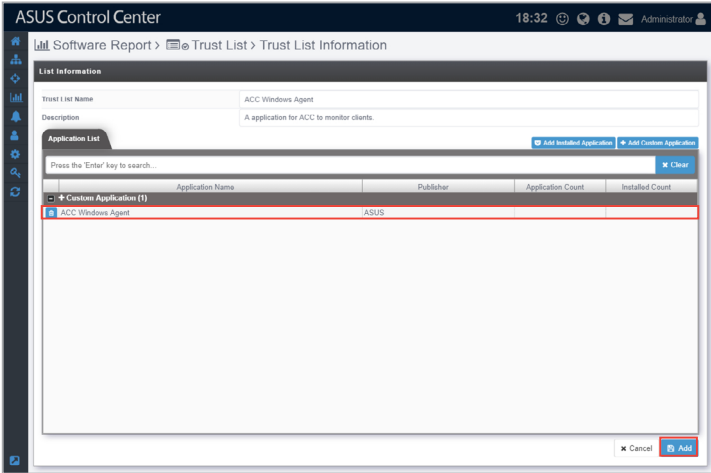
- b. Enter the **Application Name** and **Publisher** of the application, then click on **Save** to add the application to your trust list.



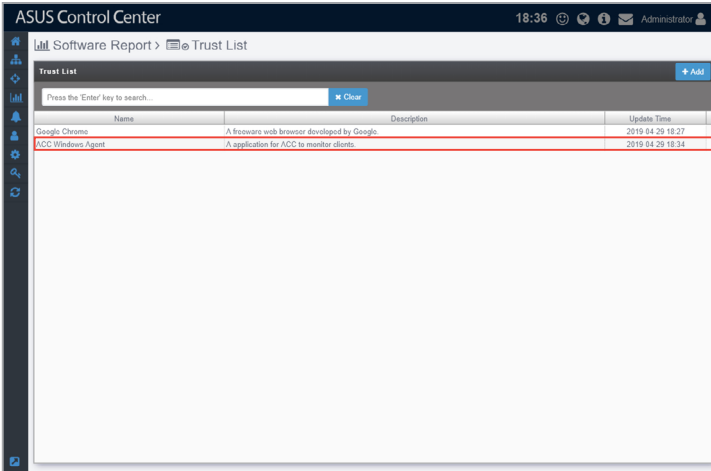
If you are not sure what the Application Name and Publisher of the application is, you may search for it in the local program collection of your device, for example Programs and Features on a Windows OS. This may vary between OS.



- The applications you have added to your trust list should be displayed in the **Application List** window. Once you have finished adding applications, click on **Add** to save your trust list.

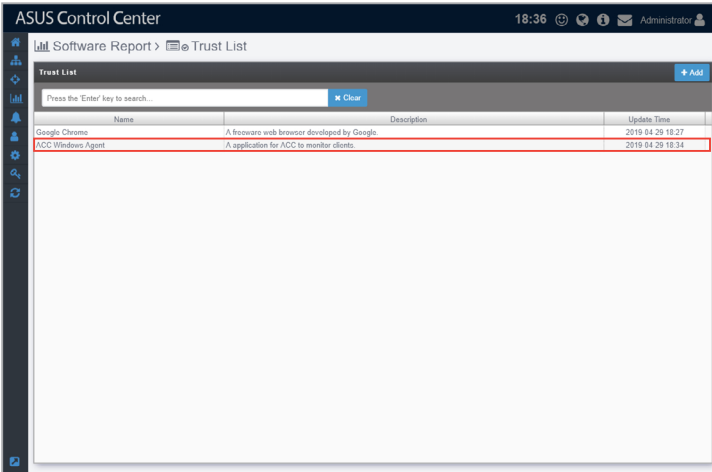


- Your new trust list should appear in the **Trust List** window.

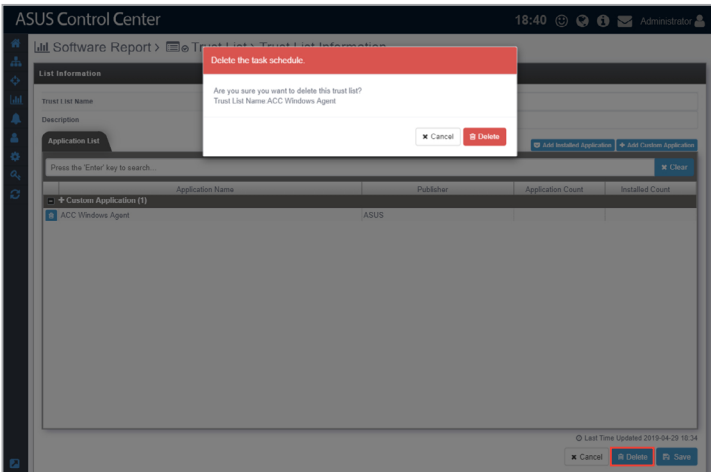


To edit or delete a trusted list:

1. Click on the trusted list you wish to edit.



2. Repeat steps 3 and 4 of the **To create a new trusted list** section to edit a trust list, or click on **Delete** to delete the trusted list.

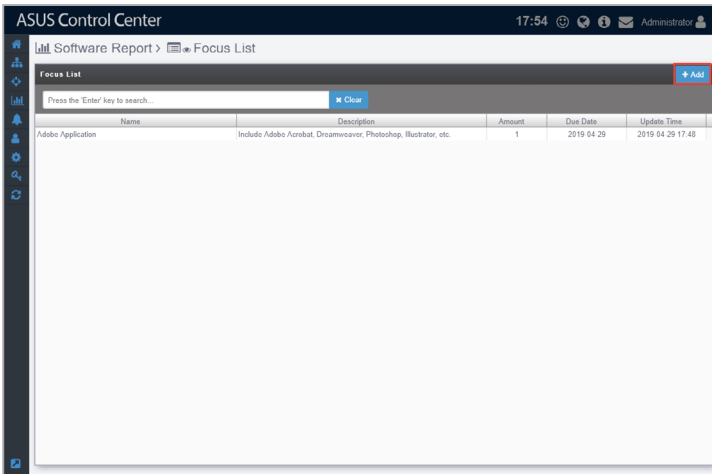


5.1.3 Focus List

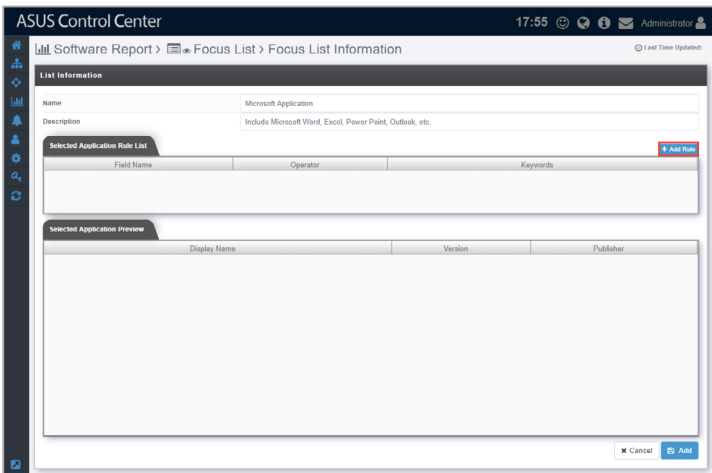
The focus list allows you to set rules on applications you wish to receive software reports on. You may select the applications you wish to focus on by entering keywords, you may also select conditions such as, containing the keyword, or applications which do not contain this keyword. This allows you to specifically focus on a group of applications which may contain a common keyword and are high-priority to receive software reports on.

To create a new focus list:

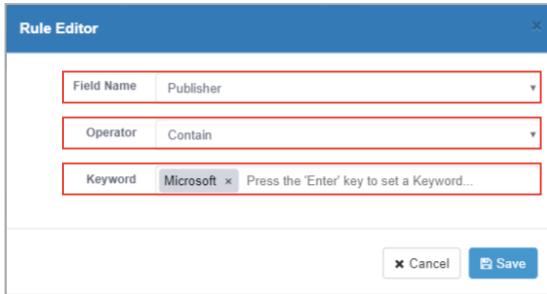
1. Click on **Add** on the Focus List main screen to create a new focus list.



2. Click on **Add Rule** to add a new rule to your focus list.

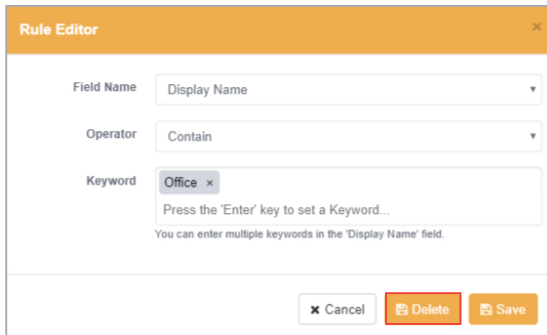


3. Select a **Field Name** to filter from between **Publisher**, **Display Name**, and **Version**.
4. Now select the **Operator (Equal, Contain, Doesn't Contain)** this will allow you to set the conditions for the keywords you enter in the next step.
5. Enter your keyword(s). This will be used as the filter keyword for your condition you set in the previous step. Then click on **Save** to add this rule.



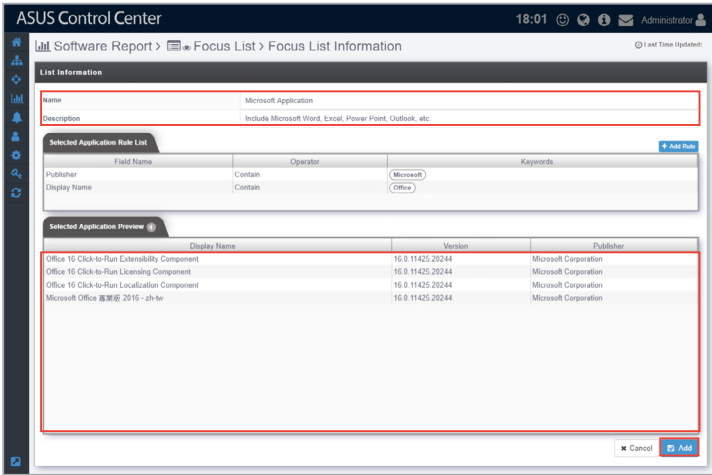
The screenshot shows a 'Rule Editor' dialog box with a blue header. It contains three input fields: 'Field Name' with 'Publisher' selected, 'Operator' with 'Contain' selected, and 'Keyword' with 'Microsoft' entered. A red box highlights each of these three fields. At the bottom right, there are 'Cancel' and 'Save' buttons.

6. Repeat steps 2 to 5 to add another rule.
7. (optional) You may also edit or delete a rule by clicking on the rule, then repeat steps 3 to 5 to edit the rule, or click on **Delete** to delete the rule.

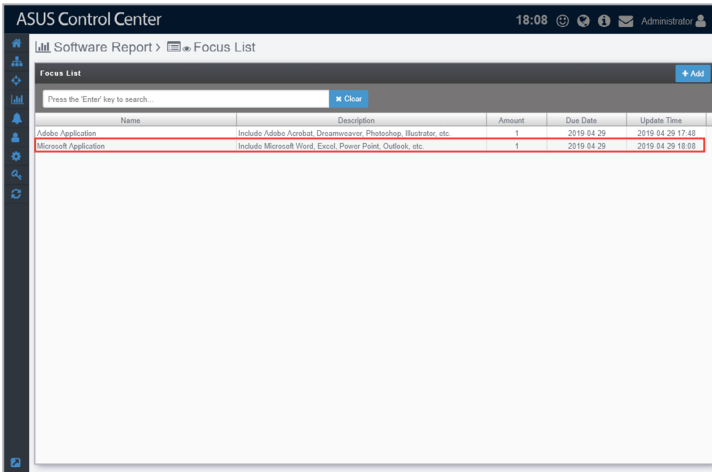


The screenshot shows a 'Rule Editor' dialog box with an orange header. It contains three input fields: 'Field Name' with 'Display Name' selected, 'Operator' with 'Contain' selected, and 'Keyword' with 'Office' entered. Below the keyword field, there is a note: 'You can enter multiple keywords in the 'Display Name' field.' At the bottom right, there are 'Cancel', 'Delete', and 'Save' buttons.

8. All installed applications will be filtered depending on the rule(s) you set in the previous steps and be displayed in the **Selected Application Preview** window. The filtered applications will be added to the focus list.
9. Enter the Focus list name as well as a brief description of the focus list into their respective fields, then click on **Add** to save your focus list.

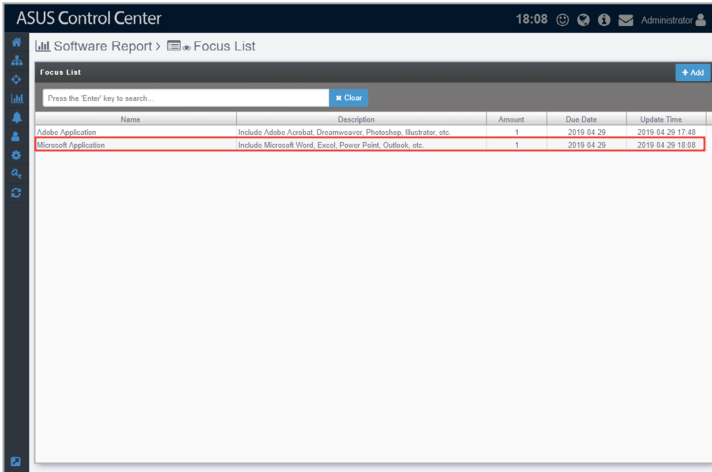


10. Your new focus list should appear in the **Focus List** window.

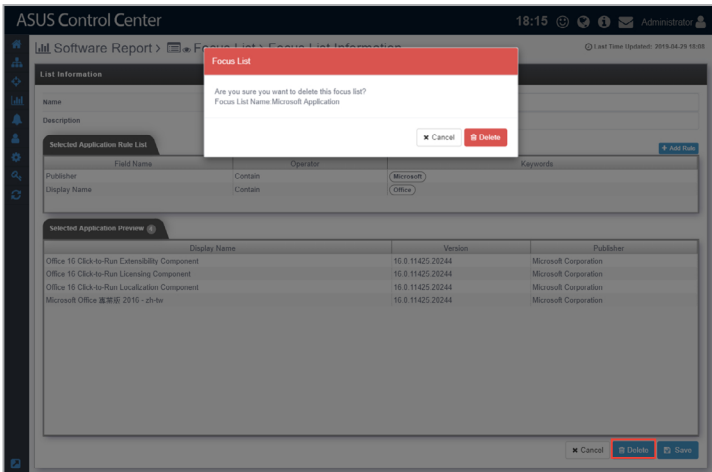


To edit or delete a focus list:

1. Click on the focus list you wish to edit.



2. Repeat steps 3 to 9 of the **To create a new focus list** section to edit a focus list, or click on **Delete** to delete the focus list.



5.1.4 Subscription Report

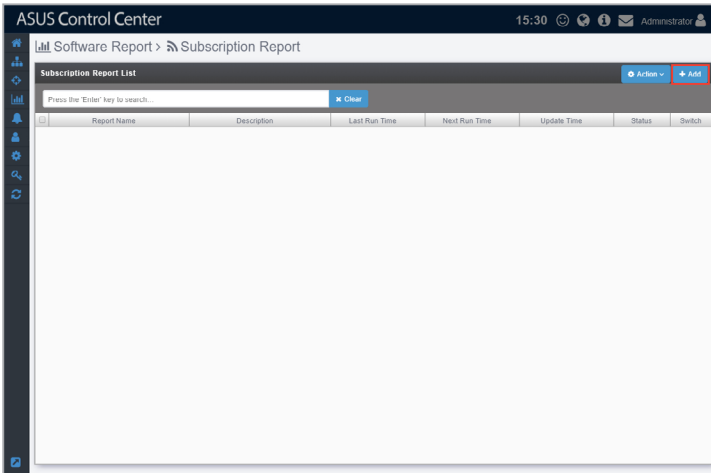
Subscription Report allows you to manage your Software Reports such as which list set to apply (Trust List or Focus list), the receiver of the report, which devices to create reports on and when to receive the reports. This gives you the flexibility to tailor each subscription report according to your 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.

To create a Subscription Report:

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 or Focus, and select the specific list(s) you wish to apply.



- Selecting the **Apply Trust List** option will exclude applications on the trust list when a report is generated. For more information please refer to the **Trust List** section of this chapter.
- Selecting the **Apply Focus List** option will only include applications on the focus list when a report is generated. For more information please refer to the **Focus List** section of this chapter.

ASUS Control Center 15:38 Administrator

Software Report > Subscription Report > Subscription Report Information

Subscription Report Information

Report Name: Software Report by Trust List
Description: Show all application but ignore known application from trust list.
Apply List: Apply Trust List Apply Focus List
 Google Chrome ACC Windows Agent Select from software trust list

Enable: Enable Report

Mail Template | Main 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 List
Mail Content: Dear Directs, Your department's software report as below, please ensure these application are followed company's policy.

Cancel Next

3. Check **Enable Report** to enable this report.

ASUS Control Center 17:16 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 | Main 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 Focus List
Mail Content: Dear Directs, Your department's software report as below, please ensure these application's license are enough.

Cancel Next

4. Select a metadata tag or enter an email address into the **Mail Receiver** field, then enter your mail title and mail content. Click on **Next** once you have finished editing your Mail Template.



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. In the Rule Settings step, you have to filter out the managed devices you wish to generate this report on.
6. Click on **Add Rule**.

ASUS Control Center 17:20 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 Trial List Apply Focus List

Enable: Enable Report

Buttons: Add Application, Microsoft Application, Select from software focus list

Navigation: Mail Template, Rule Settings, Item View, Preview Selected Device, Add Rule

Step 2: Set the selected device's rules

Field Name	Operator	Keywords
Department	Contains	SW

Buttons: Cancel, Previous, Next

7. 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**.

Rule Editor

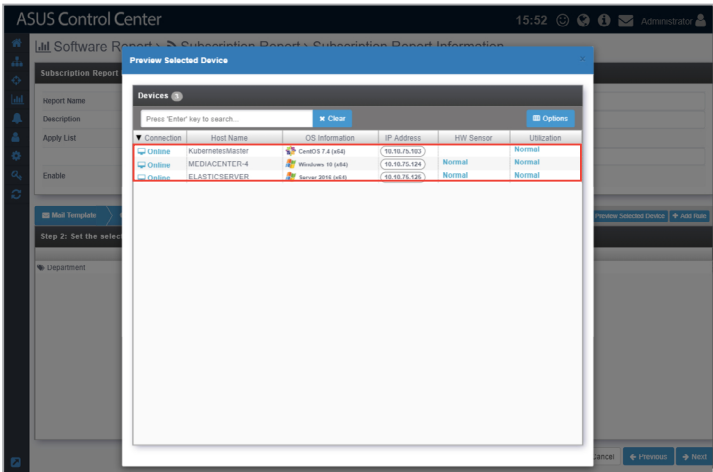
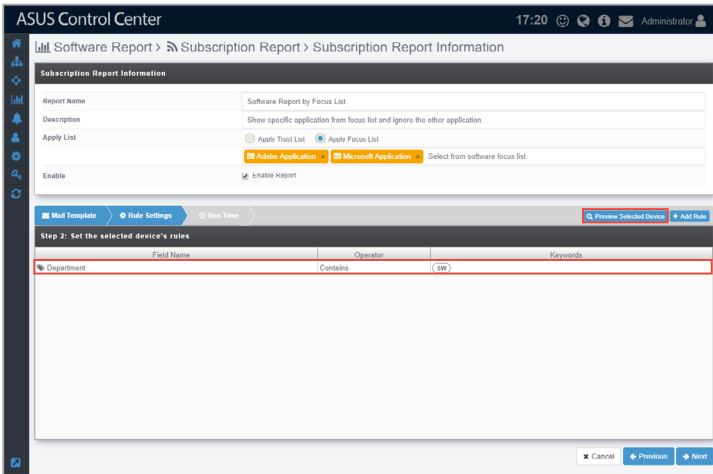
Field Name: Department

Operator: Contains

Keyword: SW x Press the 'Enter' key to set a Keyword

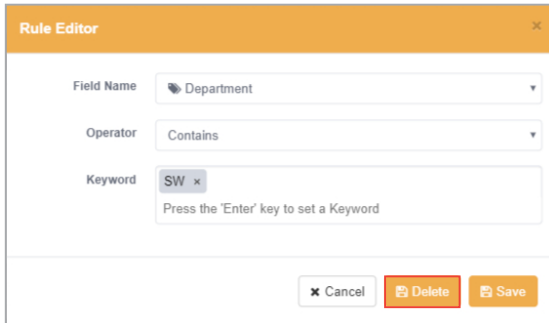
Buttons: Cancel, Save

- 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.



- Repeat steps 6 and 7 to add another rule.

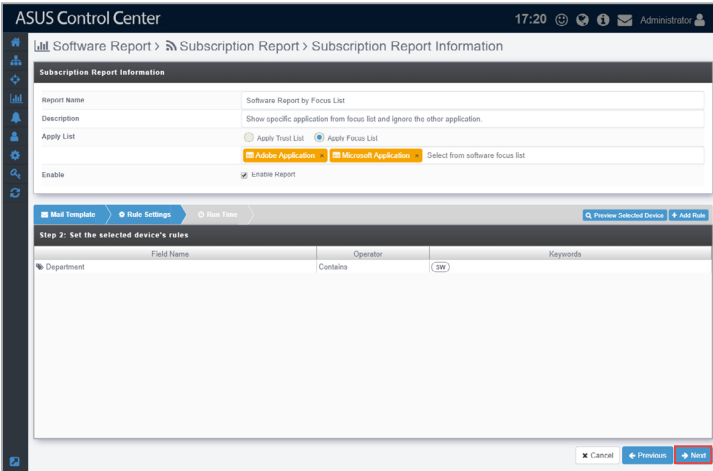
10. (optional) You may also edit or delete a rule by clicking on the rule, then repeat steps 4 to edit the rule, or click on **Delete** to delete the rule.



The screenshot shows a 'Rule Editor' dialog box with the following fields and controls:

- Field Name:** A dropdown menu with 'Department' selected.
- Operator:** A dropdown menu with 'Contains' selected.
- Keyword:** A text input field containing 'SW' with a small 'x' icon to its right. Below the field is the instruction 'Press the 'Enter' key to set a Keyword'.
- Buttons:** 'Cancel', 'Delete', and 'Save' buttons are located at the bottom right.

11. Click on **Next** once you are finished.



The screenshot shows the ASUS Control Center interface with the following elements:

- Header:** 'ASUS Control Center' and '17:20'.
- Breadcrumbs:** '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:** Radio buttons for 'Apply Trial List' and 'Apply Focus List' (selected).
 - Enable:** A checked checkbox for 'Enable report'.
- Step 2: Set the selected device's rules:**

Field Name	Operator	Keywords
Department	Contains	SW
- Navigation:** 'Cancel', 'Previous', and 'Next' buttons at the bottom right.

12. 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 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 17:35 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:

Days: Days Months All
Data Period: Months
 Entire month
 Depend on send date

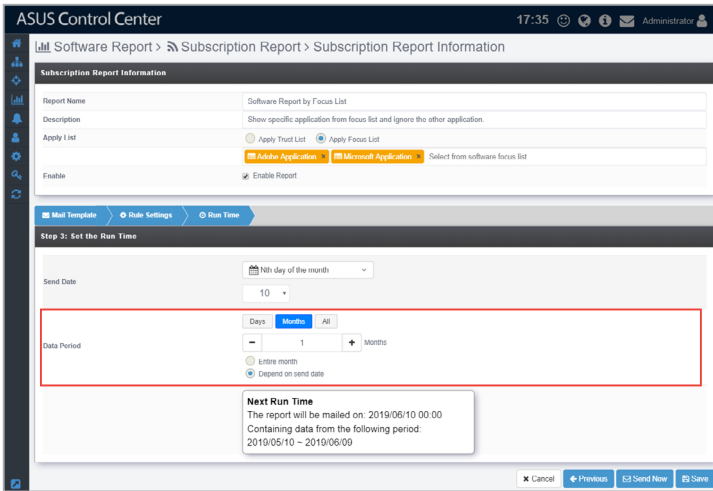
Next Run Time
The report will be mailed on: 2019/06/10 00:00
Containing data from the following period:
2019/05/10 - 2019/06/09

Cancel Previous Edit Send New Save

13. 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.



- You can view information on when you will receive the next report, and the time period the report is generated 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 **Update** to save your settings.

ASUS Control Center 17:35 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 | **Run Settings** | Run Time

Step 3: Set the Run Time

Send Date: Nth day of the month
 10

Days: Days Months All
 Data Period: 1 Months
 Listen 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 - 2019/06/00

Cancel Previous **Send Now** Save

- Report as a result of applying **Trust List**. (Does not show white listed applications)

ASUS Control Center -asuserver@asus.com

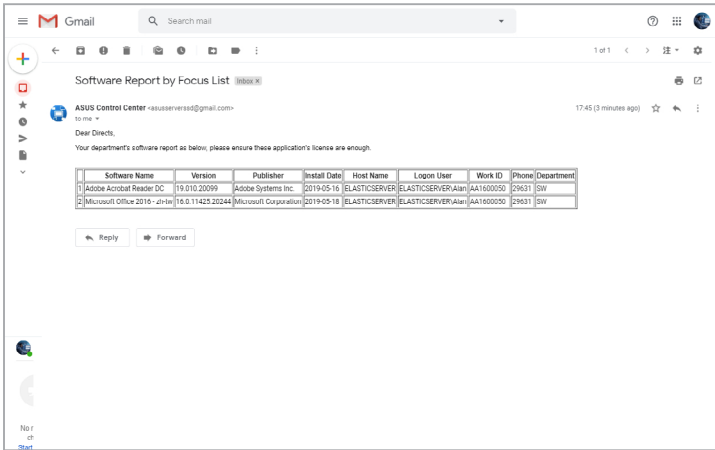
Dear Directs,

Your department's software report as below, please ensure these application are followed company's policy.

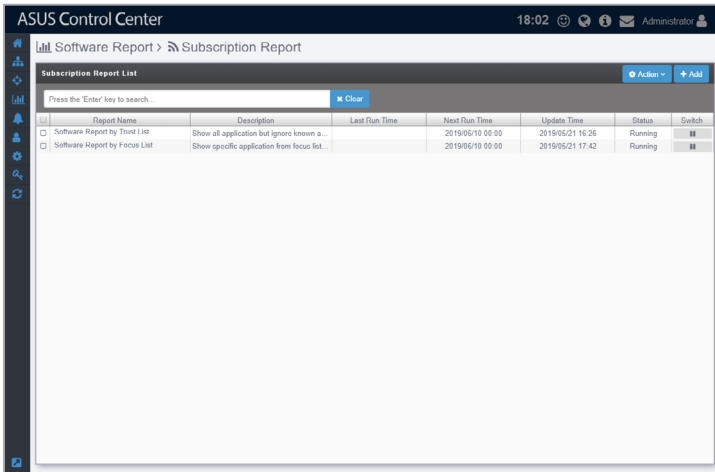
	Software Name	Version	Publisher	Install Date	Host Name	Logon User	Work ID	Phone	Department
1	HeavyLoad V3.51 (64-bit)	3.51	LLM Software	2019-05-10	ELASTICSERVER	ELASTICSERVER\Alan	AA1000050	29631	ISW
2	Coreland HD Audio	8.00.05.54	Coreland	2019-05-11	ELASTICSERVER	ELASTICSERVER\Alan	AA1000020	29631	ISW
3	Intel(R) Management Engine Components	1.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	ISW
4	Microsoft VC++ redistributable repackaged	12.0.0.0	Intel Corporation	2019-05-12	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	ISW
5	VMware Run Time 4.1.0.65.1	1.0.65.1	vmware, inc.	2019-05-13	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	ISW
6	NetBeans IDE 8.2	8.2	NetBeans.org	2019-05-14	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	ISW
7	JWS2, version 3.3 CE	3.3.10	Crucial Corporation	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1600050	29631	ISW
8	PuTTY release 0.71 (64-bit)	0.71.0.0	Simon Tatham	2019-05-15	ELASTICSERVER	ELASTICSERVER\Alan	AA1000020	29631	ISW
9	Python 3.6 pip Bootstrapper (32-bit)	3.6.4195.0	Python Foundation	2019-05-16	ELASTICSERVER	ELASTICSERVER\Alan	AA1000050	29631	ISW
10	libwpd	0.3.0	CamTAS	2019-05-17	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW
11	webaligh4-plugin-process-gp2	2.14.7	CentOS	2019-05-18	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW
12	gmp3-mp3	16.0.114429.20144	CentOS	2019-05-19	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW
13	PackageKit.gtk3-theme-plugin	1.1.5	CentOS	2019-05-19	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW
14	python-decorator	3.4.0	CentOS	2019-05-20	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW
15	gnome-shell-extension-common	3.27.2	CentOS	2019-05-20	KubernetesMaster	KubernetesMaster\Charles	AA1600051	29768	ISW

Reply Forward

- Report as a result of applying **Focus List**. (Only shows applications on the focus list)

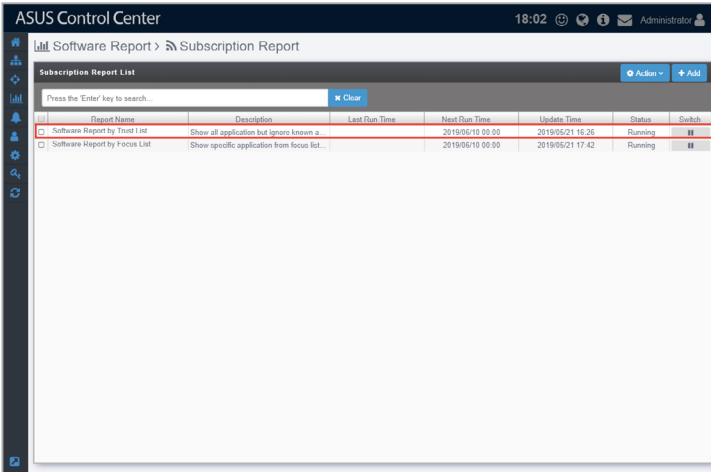


15. Your new report subscription should appear in the Subscription Report List on the main screen of **Subscription Report**.

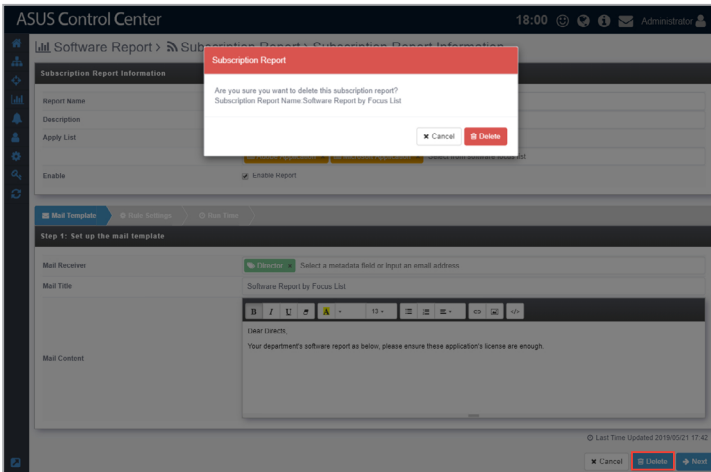


To edit or delete a subscription report:

1. Click on the subscription report you wish to edit.

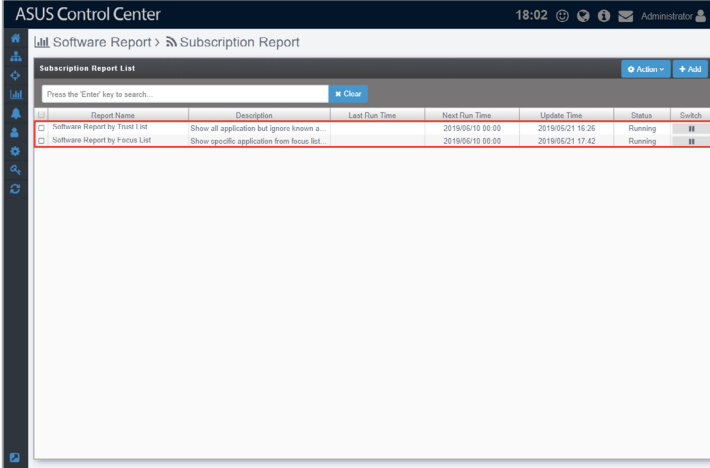


2. Repeat steps 2 to 14 of the **To create a Subscription Report** section to edit a subscription report, or click on **Delete** to delete the subscription report.

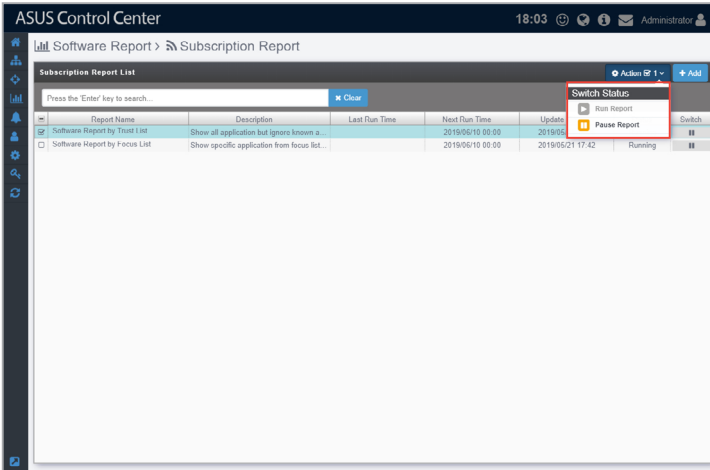


Switching the status of a subscription reports:

1. Click on the subscription reports you wish to switch the subscription status of.



2. Click on **Action**, then select if you want to pause or run the report.



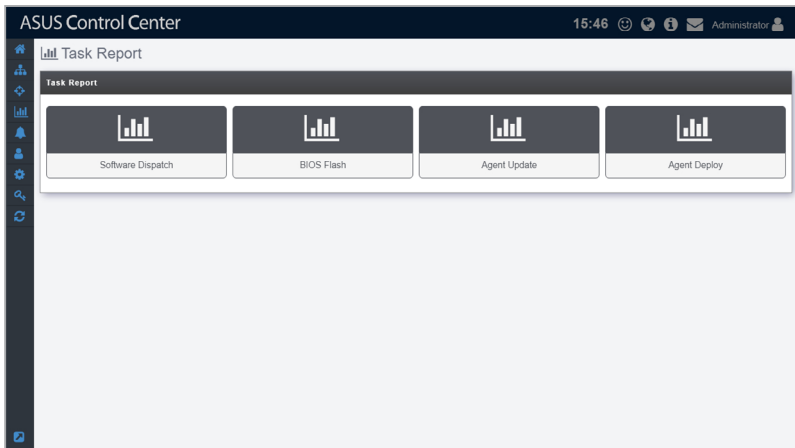
5.2 Task Report



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.

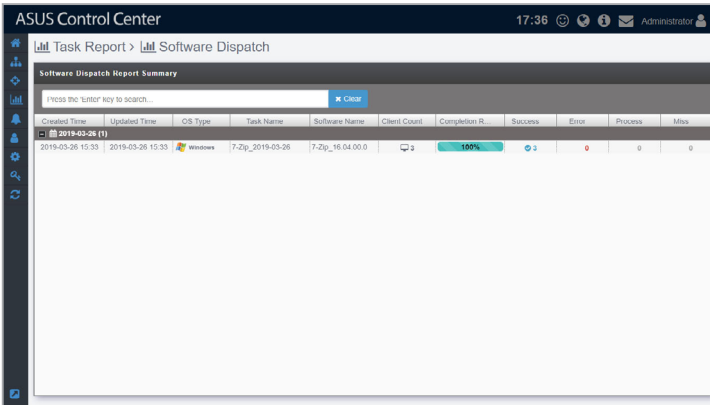
To access **Task Report**, click  > **Task Report** in the left menu.



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 **2.1.4 Search and Filter devices** section.

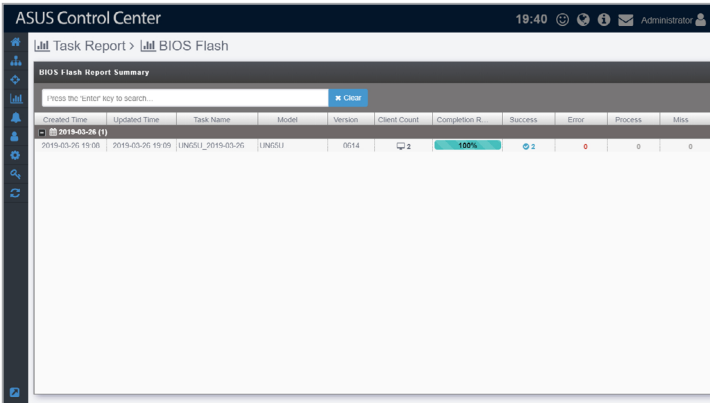
5.2.1 Software Dispatch Report

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 **4.4.3 Software Dispatch Task Report** for more details.



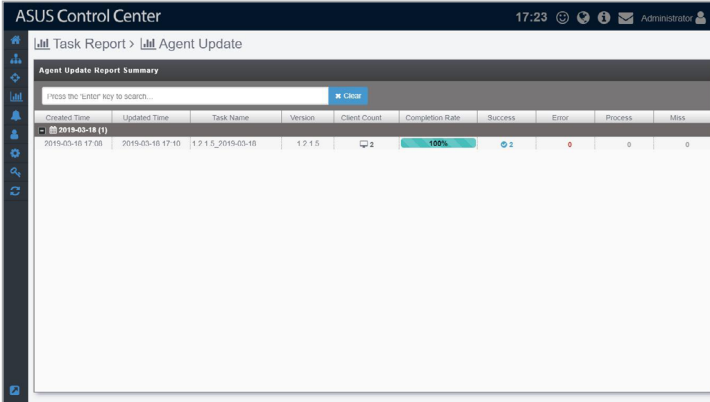
5.2.2 BIOS Flash Report

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 **4.2.3 BIOS Flash Task Report** for more details.



5.2.3 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 **10.1.2 Agent Update Report** for more details.

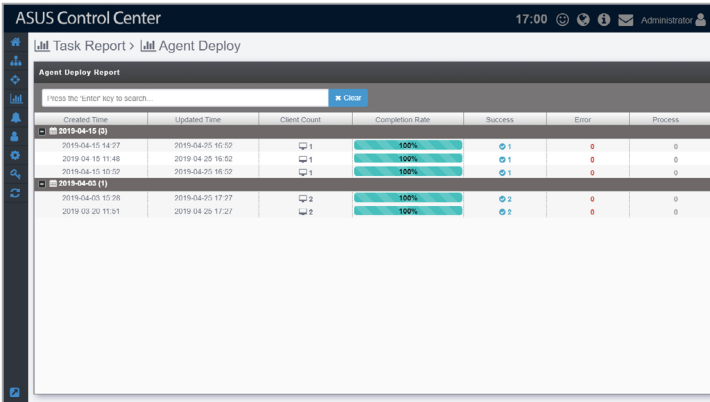


The screenshot shows the ASUS Control Center interface for the Agent Update Report. The title bar indicates the time is 17:23 and the user is Administrator. The breadcrumb navigation shows 'Task Report > Agent Update'. Below the title is a search bar with a 'Clear' button. The main table displays the following data:

Created Time	Updated Time	Task Name	Version	Client Count	Completion Rate	Success	Error	Process	Mis
2019-03-18 17:00	2019-03-18 17:05	1.2.1.5_2019-03-18	1.2.1.5	2	100%	2	0	0	0

5.2.4 Agent Deploy Report

The **Agent Deploy Report** will display information on each time agent(s) are deployed onto managed devices. The list of agent deployment results are grouped by each batch of agent deployments. You can refer to **3.1.6 Agent Deploy Report** for more details.



The screenshot shows the ASUS Control Center interface for the Agent Deploy Report. The title bar indicates the time is 17:00 and the user is Administrator. The breadcrumb navigation shows 'Task Report > Agent Deploy'. Below the title is a search bar with a 'Clear' button. The main table displays the following data:

Created Time	Updated Time	Client Count	Completion Rate	Success	Error	Process
2019-04-15 (2)						
2019-04-15 14:27	2019-04-25 16:50	1	100%	1	0	0
2019-04-15 11:48	2019-04-25 16:52	1	100%	1	0	0
2019-04-15 10:59	2019-04-25 16:59	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 11:31	2019-04-25 17:27	2	100%	2	0	0

Chapter 6

This chapter describes setting the notifications and SMTP Server

Notification

6.1 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**.



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.

ASUS Control Center 15:38 Administrator

SMTP Settings

Display Name
ASUS Control Center SMTP

SMTP Server
smtp.gmail.com

SMTP Port
587

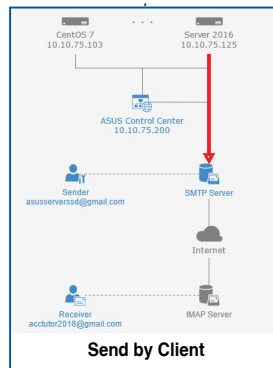
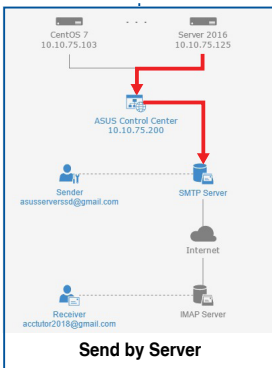
Sender Address
asusserverssd@gmail.com

Sender Password
.....

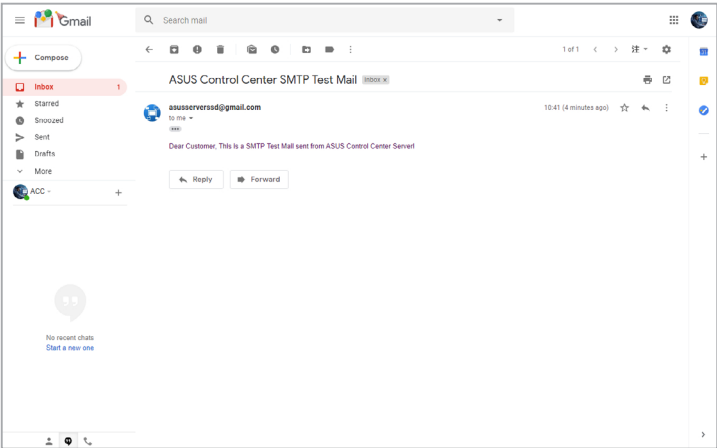
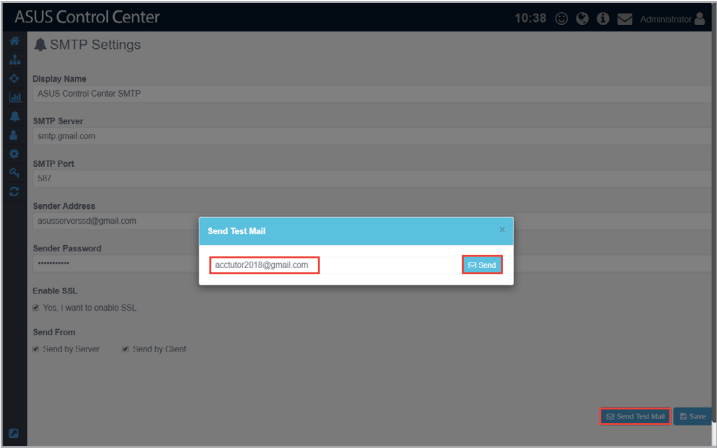
Enable SSL
 Yes, I want to enable SSL

Send From
 Send by Server Send by Client

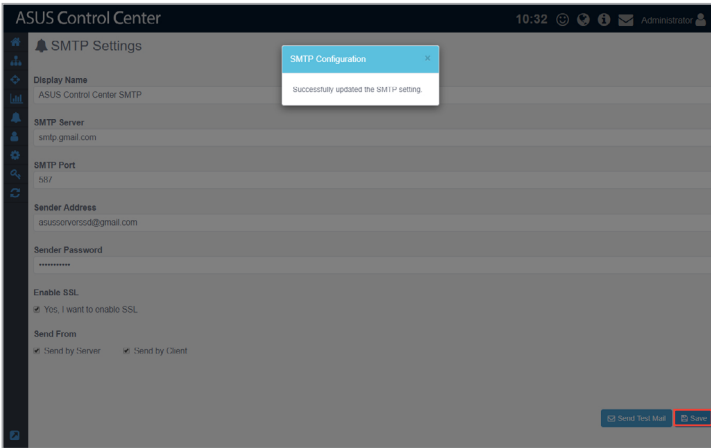
Send Test Mail Save



- 2. (optional) Click on **Send Test Mail**, then enter an email and click **Send** to receive the test mail to check the status of the SMTP. If the SMTP is functioning properly, you should receive an email.



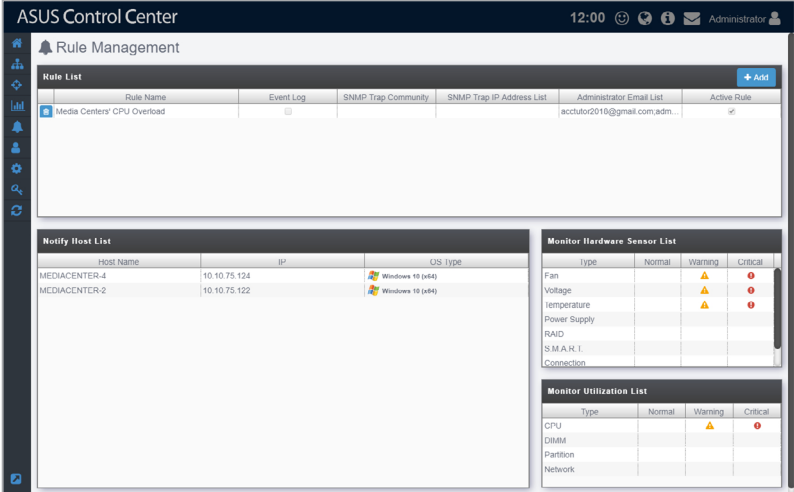
3. Click **Save** to save the changes made.



6.2 Rule Management

Rule management allows you to add or delete rules on notifications. When a device is in warning or critical status, a notification will be sent to the system administrator.

To access **Rule Management**, click  in the left menu, then click on **Rule Management**.



The screenshot shows the ASUS Control Center interface. At the top, it says "ASUS Control Center" and "12:00" with system icons. The main heading is "Rule Management". Below it is a "Rule List" table with one entry: "Media Centers' CPU Overload".

Rule Name	Event Log	SNMP Trap Community	SNMP Trap IP Address List	Administrator Email List	Active Rule
Media Centers' CPU Overload				acctutor2016@gmail.com;adm...	<input checked="" type="checkbox"/>

Below the Rule List are three monitoring sections:

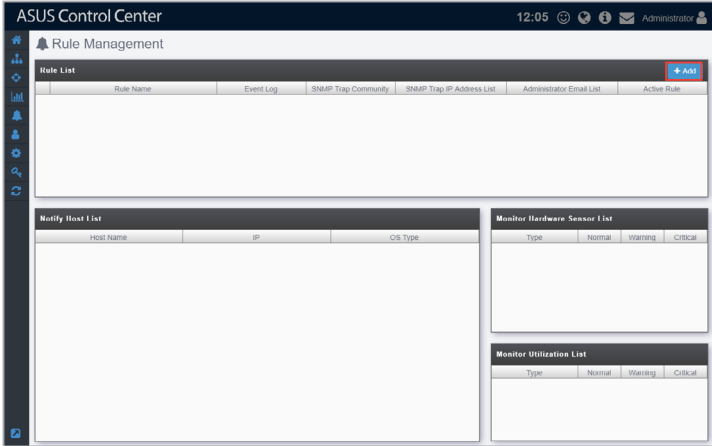
- Notify Host List:** A table with columns: Host Name, IP, OS Type. It lists two hosts: MEDIACENTER-4 (IP: 10.10.75.124, OS: Windows 10 (x64)) and MEDIACENTER-2 (IP: 10.10.75.122, OS: Windows 10 (x64)).
- Monitor Hardware Sensor List:** A table with columns: Type, Normal, Warning, Critical. It lists sensors: Fan, Voltage, Temperature, Power Supply, RAID, S.M.A.R.T., and Connection. Fan, Voltage, and Temperature show warning (yellow triangle) and critical (red circle) status.
- Monitor Utilization List:** A table with columns: Type, Normal, Warning, Critical. It lists utilization metrics: CPU, DIMM, Partition, and Network. CPU shows warning (yellow triangle) and critical (red circle) status.



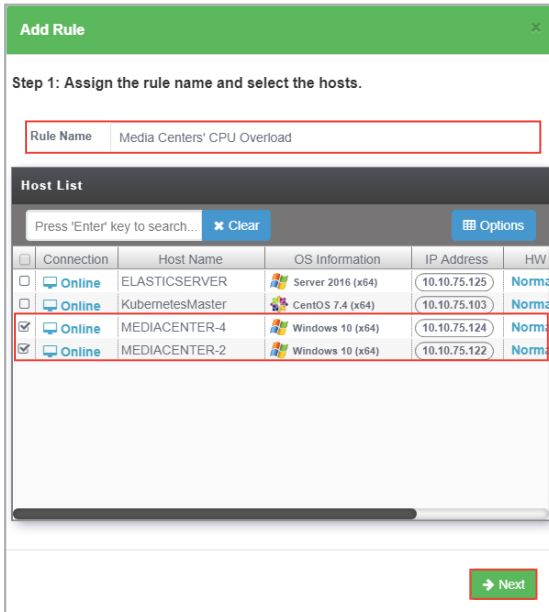
If the Search Bar is available for a function in this section, you can use the Search Bar to search and filter managed devices. For more information, please refer to **2.1.4 Search and Filter devices** section.

Adding a new rule

1. Click **Add**.



2. Enter a rule name, then select the devices to apply the rule to. Click **Next**.



3. Select conditions (type and status of hardware or utilization sensors) 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 **2.2.2 Utilization**.

Add Rule ✕

Step 2: Select the hardware sensor or utilization type and status.

Hardware Sensor Type	Normal	Warning	Critical
<input checked="" type="checkbox"/> Fan	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Voltage	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Temperature	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Power Supply	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> RAID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> S.M.A.R.T.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Connection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Backplane	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Utilization Type	Normal	Warning	Critical
<input checked="" type="checkbox"/> CPU	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> DIMM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Partition	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

← Previous Next →

4. Select the notification method between the following options (multiple notification methods may be selected):
- Event Log
The notification will be displayed on the device's event log and system overview.

The screenshot shows a web-based configuration window titled "Add Rule" with a green header and a close button (X) in the top right corner. The main content area has a heading "Select 3: Select at least one notification method." Below this, there are three notification method options, each with a checkbox and a text input field for configuration:

- Event Log**: This option is selected, and its label is highlighted with a red rectangular box.
- SNMP Trap**: This option is not selected. It includes a "Community" field with the example value "EX: asus" and a "Receiver's IP address" field with the example value "EX: 192.168.0.1".
- Email**: This option is selected. It includes a "Device administrator's email address" field containing two email addresses: "acctutor2018@gmail.com" and "admin1@asus.com", each with a small 'X' icon to its right. Below this field is an example value: "EX: admin1@asus.com;admin2@asus.com;".

Below the email configuration, there is a tip: "Tip: Press <Enter> to add another email address separated by a semi-colon." At the bottom right of the window, there are two green buttons: "← Previous" and "Save".

- **SNMP Trap**

The notification is recorded in the SNMP Trap Receiver, ensure to enter the corresponding information into the **Community** and **Receiver's IP address** fields.

The screenshot shows a web-based configuration window titled "Add Rule" with a close button (X) in the top right corner. The main heading is "Select 3: Select at least one notification method." Below this, there are two notification methods: "Event Log" (unchecked) and "SNMP Trap" (checked). The "SNMP Trap" section is highlighted with a red border and contains two input fields: "Community" with the example "EX: asus" and "Receiver's IP address" with the example "EX: 192.168.0.1". Below the "SNMP Trap" section, the "Email" method is also checked. It has a label "Device administrator's email address" and a multi-line input field containing two email addresses: "acctutor2018@gmail.com" and "admin1@asus.com", each with a close button (X). Below the input field is the example "EX: admin1@asus.com,admin2@asus.com;". A tip below reads: "Tip: Press <Enter> to add another email address separated by a semi-colon." At the bottom right of the window are two green buttons: "Previous" with a left arrow and "Save" with a floppy disk icon.

- 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 **5.1 Setting up the SMTP Server**.



When entering multiple emails, use a semicolon ‘;’ to separate the emails.

Add Rule [Close]

Select 3: Select at least one notification method.

Event Log

SNMP Trap

Community
EX: asus

Receiver's IP address
EX: 192.168.0.1

Email

Device administrator's email address
acclutor2018@gmail.com x admin1@asus.com x
EX: admin1@asus.com;admin2@asus.com;

Tip: Press <Enter> to add another email address separated by a semicolon.

← Previous Save

- 5. Click on **Save** after finished selecting your notification method(s).

Add Rule ✕

Select 3: Select at least one notification method.

Event Log

SNMP Trap

Community
EX: asus

Receiver's IP address
EX: 192.168.0.1

Email

Device administrator's email address

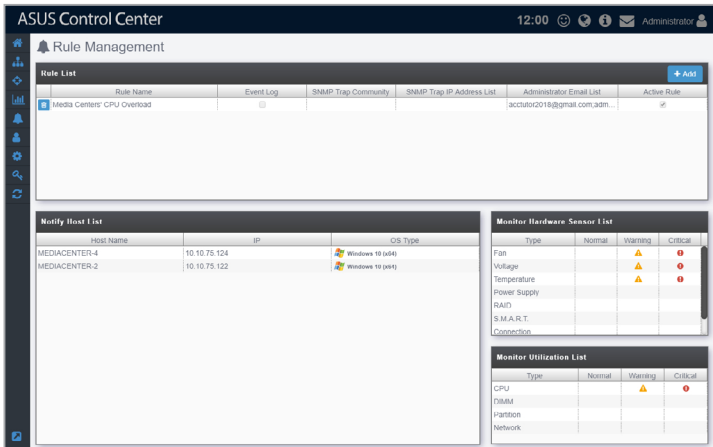
acctutor2018@gmail.com ✕ admin1@asus.com ✕

EX: admin1@asus.com,admin2@asus.com,


Tip: Press <Enter> to add another email address separated by a semi-colon.

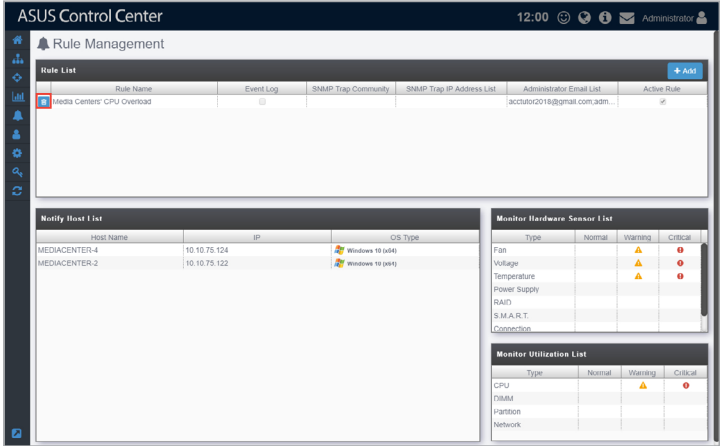
← Previous Save

Your newly added rule should appear in the main Rule Management 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**.

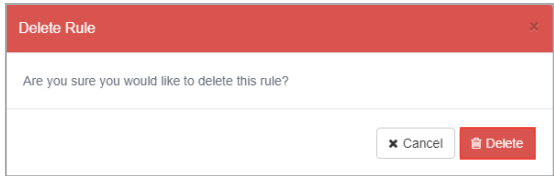


Deleting a notification rule

1. Select a rule in the **Rule List** you wish to delete, then click on  in the **Delete Rule** column.




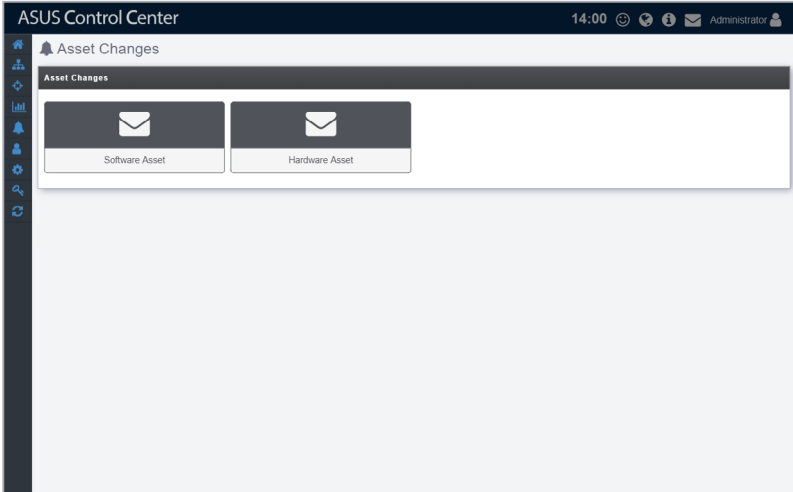
2. Click **Delete** to delete the rule.



6.3 Asset Changes

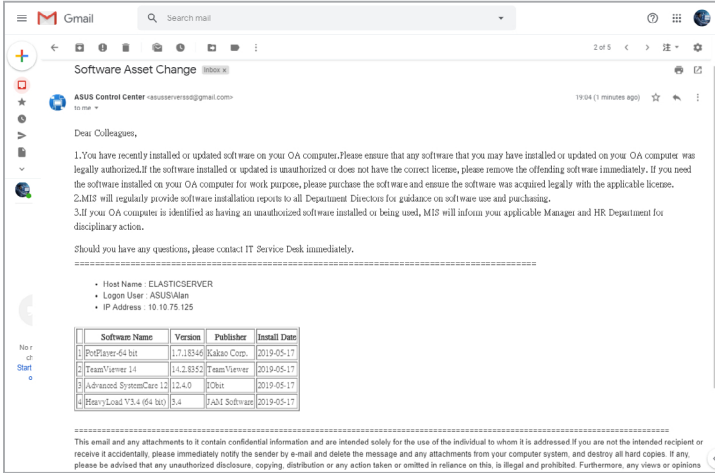
Asset Changes allows you to set notifications for software or hardware changes on managed devices. Notifications are sent when software not on the Trust list have been installed on managed devices, or if hardware such as CPUs or DIMMs that do not comply to company specifications are installed onto managed devices. This function will keep you alerted of potential risks to managed devices.

To access **Asset Changes**, click  in the left menu, then click on **Asset Changes**.



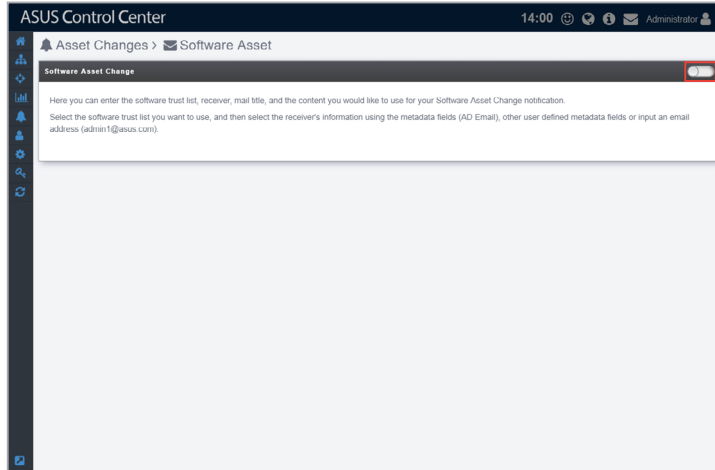
6.3.1 Software Asset

Software Asset allows you to set notifications when there are applications not in the Trust List being installed on managed devices. These notifications will be sent immediately to the owner of managed device as well as his/her director.



To enable software asset :

1. Click on the button to configure and enable software change notifications.



2. Select a Trust List to apply. Notifications will be sent when new software is installed on managed devices which do not appear on the Trust List.



For more information on Trust List, please refer to **5.1.2 Trust List** section of this manual.

3. Enter the recipients of the notification email.
4. Click on **Save** after composing the title and content of the notification email.

ASUS Control Center 14:00 Administrator

Asset Changes > Software Asset

Software Asset Change [ON/OFF]

Here you can enter the software trust list, receiver, mail title, and the content you would like to use for your Software Asset Change notification.

Select the software trust 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)

Apply Software Trust List: ACC Windows Agent, Google Chrome. Select from software trust list

To: AD Mail. Select a metadata field or input an email address

CC: admin1@asus.com. Select a metadata field or input an email address

BCC: Director. Select a metadata field or input an email address

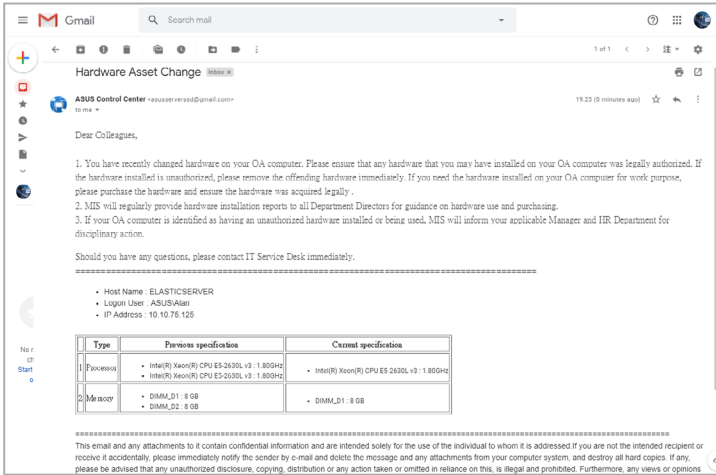
Mail Title: Software Asset Change

Mail Content: 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.

Save

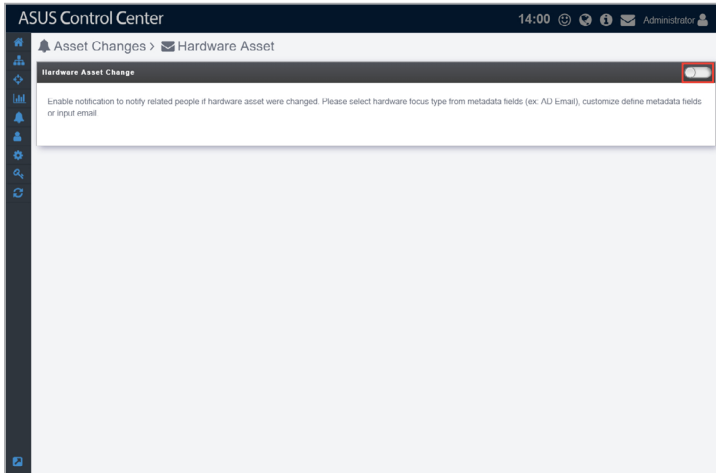
6.3.2 Hardware Asset

Hardware Asset allows you to set notifications when there are hardware components which do not comply to company specifications being installed on managed devices. These notifications will be sent immediately to the owner of managed device as well as his/her director and will list the hardware changes.



To enable hardware asset :

- Click on the button to configure and enable software change notifications.



2. Select which hardware components 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.

ASUS Control Center 14:00 Administrator

Asset Changes > Hardware Asset

Hardware Asset Change

Enable notification to notify related people if hardware asset were changed. Please select hardware focus type from metadata fields (ex: AD Email), customize define metadata fields or input email

Hardware Focus Type: Processor, Memory (Select from hardware type list)

To: AD Mail (Select from metadata fields or input email)

CC: admin1@asus.com (Select from metadata fields or input email)

BCC: Director (Select from metadata fields or input email)

Mail Title: Hardware Asset Change

Mail Content

Dear Colleagues,

1. You have recently changed hardware on your OA computer. Please ensure that any hardware that you may have installed on your OA computer was legally authorized. If the hardware installed is unauthorized, please remove the offending hardware immediately. If you need the hardware installed on your OA computer for work purpose, please purchase the hardware and ensure the hardware was acquired legally.
2. MIB will regularly provide hardware installation reports to all Department Directors for guidance on hardware use and purchasing.
3. If your OA computer is identified as having an unauthorized hardware installed or being used, MIB will inform your appropriate Manager and HR Department for disciplinary action. Should you have any questions, please contact IT Service Desk immediately.

Save

Chapter 7

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


Account Management

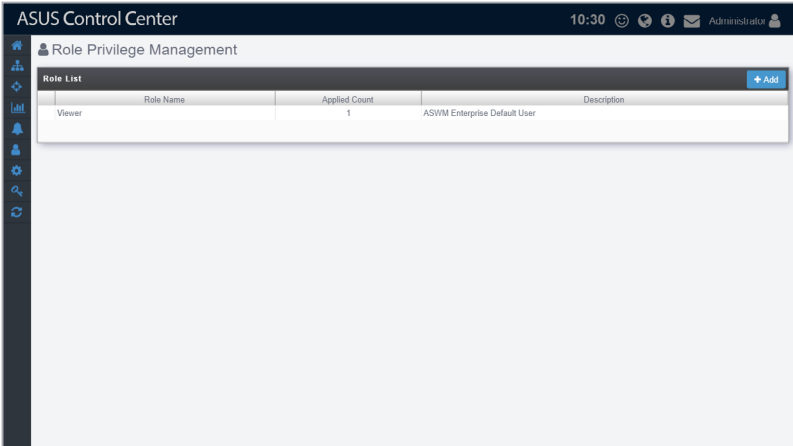
7.1 Role Privilege Management

Role Privilege will allow you to create roles with different permissions which gives you control over the functions and information accessible to each role created. A **Viewer** role privilege is available by default, which only allows accounts assigned with this role privilege to view all the functions, but cannot edit customized roles. There is no Administrator role in the **Role List** by default, but you can create one by enabling all permissions when creating a new role, this will allow accounts assigned with this role to add, edit, or delete when using any function, and also allows you to customize roles.



The **Admin** role assigned to the default Administrator account of ASUS Control Center will not appear in the **Role List** and cannot be edited.

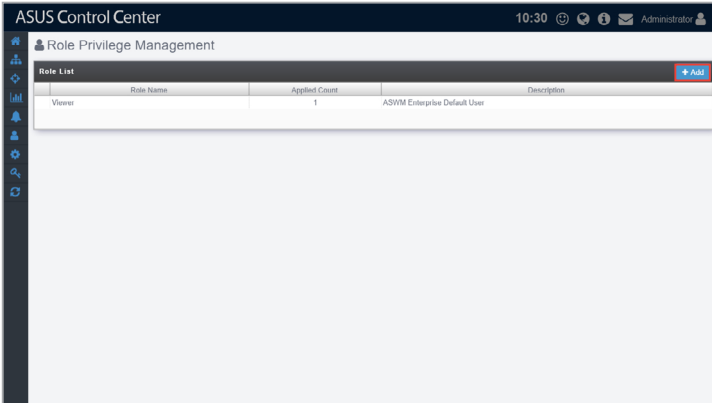
To access **Role Privilege Management**, Click  in the left menu, then click on **Role Privilege**.



Adding a new role

You can add new roles and set the permissions of this role. For example, assigning an account with Software User role which is customized to only allow users with this role access to ASUS Control Center software related functions, or creating an account with BIOS User role which is customized to only allow users access to ASUS Control Center BIOS related functions.

1. Click on **Add**.



2. Select between **Create new role** and **Copy from exist role**, then click **OK**.



- **Create new role:** Create a new role with no permissions enabled in **Privilege Configurations**.
- **Copy from exist role:** Select from an existing role (including the Admin role assigned to ASUS Control Center's default administrator account), this will load the **Privilege Configurations** of the selected account into the new role.

The screenshot shows a dialog box titled "Role Information" with a blue header. The main text asks, "Create a new role from blank privilege configuration or copy privilege configuration from exist role?". Below this, there are two buttons under the label "Create Type": "Create new role" (highlighted with a red box) and "Copy from exist role". At the bottom right, there are two buttons: "Cancel" and "OK" (highlighted with a red box).

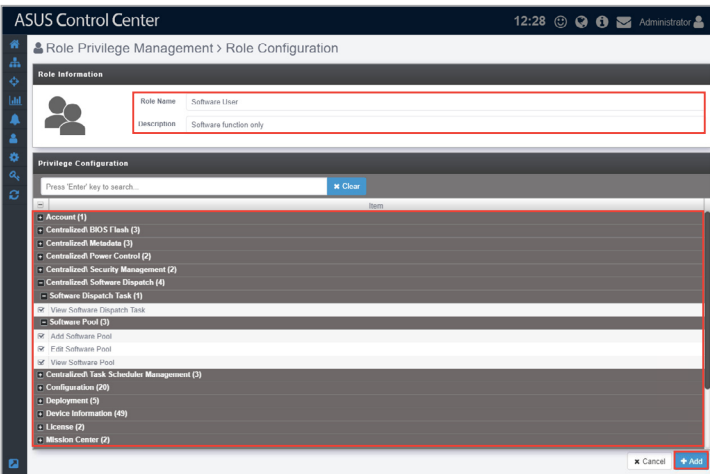
The screenshot shows a dialog box titled "Role Information" with a blue header. The main text asks, "Create a new role using blank privilege configurations or in copy privilege configurations from an existing role?". Below this, there are two buttons under the label "Create Type": "Create new role" and "Copy from existing role" (highlighted with a red box). Below the buttons is a "Role Name" field with a dropdown menu showing "Software User" (highlighted with a red box). At the bottom right, there are two buttons: "Cancel" and "OK" (highlighted with a red box).

3. Enter the Role Name and Description of the new role.
4. Select and check / uncheck the permissions to enable / disable for the role in the **Privilege Configuration** block.



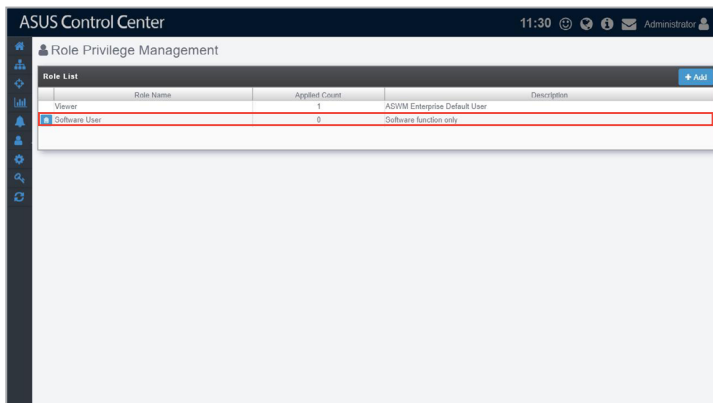
- If you chose **Copy from exist role** in step 2, your **Privilege Configurations** list should be the same as the role you selected to copy from. You can still customize the permissions for this new role.
- You can click on **+** / **-** next to each permission category to expand / collapse the category to view / hide the permissions available for that permission category.
- You can use the Search Bar to search and filter through the permission items in the **Privilege Configurations** list.

5. Click **Add** once you have finished.

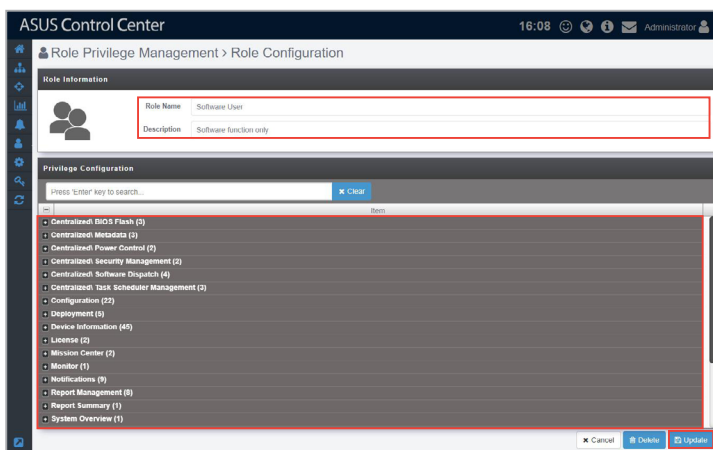


Editing a role

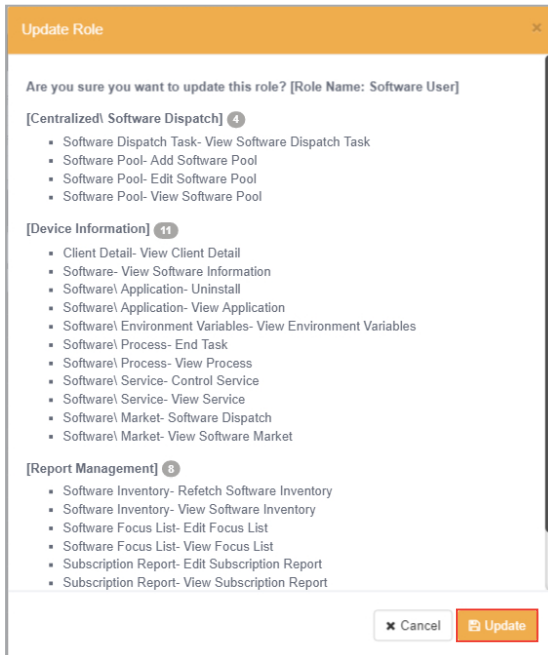
1. Click on the role you wish to edit from the Role List block.



2. You can edit the **Role Name** and **Description**, and also configure the permissions in the Privilege Configuration list. Once you are finished click on **Update**.



3. A pop-up window should appear and allow you to check the changes made to the role, click on **Update** to confirm these changes.




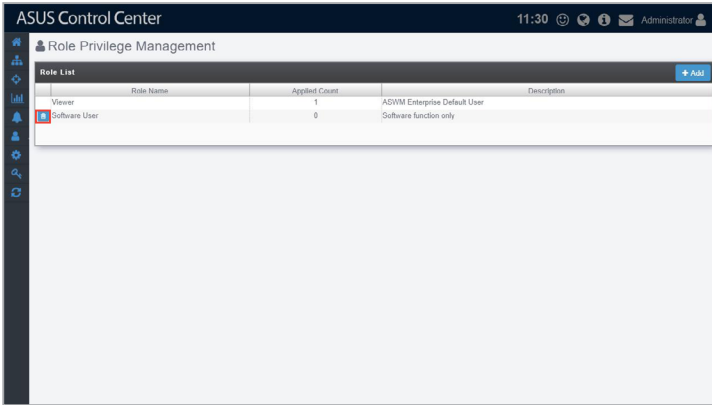
Deleting a role



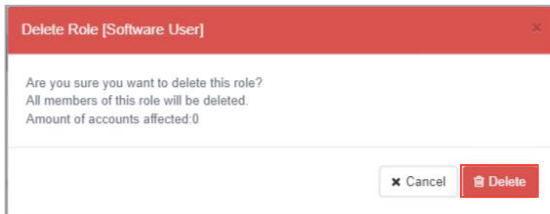
Account(s) associated with a role will be deleted too when you delete a role. You can check how many accounts are associated with the role in the Applied Count column. For more information on managing accounts, please refer to **7.2 Accounts Management**.

You can delete a role using the following methods:

- Deleting the role from the Role List
 1. Click on  next to the role you wish to delete.

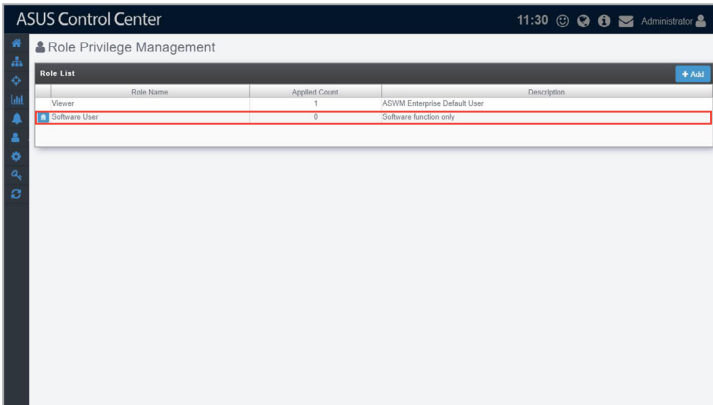


2. Click Delete to delete the role.

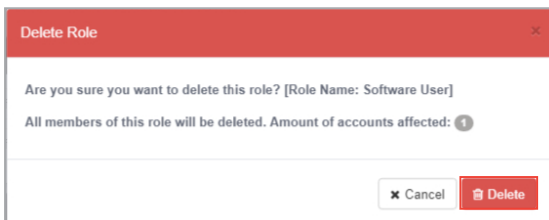
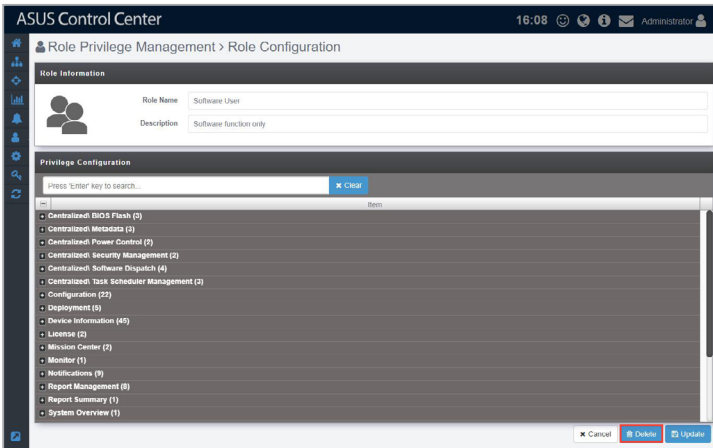


- Deleting the role from Role Configuration

1. Click on the role you wish to delete from the **Role List** block.





2. Click Delete to delete the role.

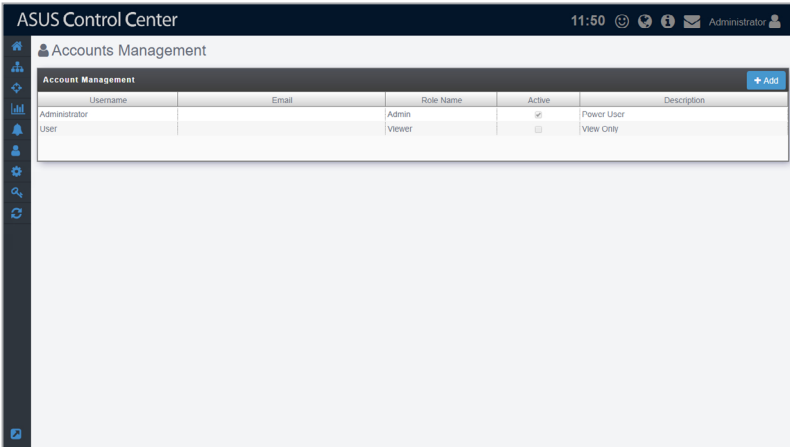


7.2 Accounts Management

Accounts Management displays all user accounts on ASUS Control Center, and allows you to add, edit, or delete accounts. ASUS Control Center comes with a default Administrator account with Admin role privileges, and a User account with Viewer role privileges.

To access **Accounts Management**, you can use the following methods:

- Click  in the left menu, then click on **Accounts Management**.
- Click  (**Account Information**) in the top right corner, then select **Settings**.



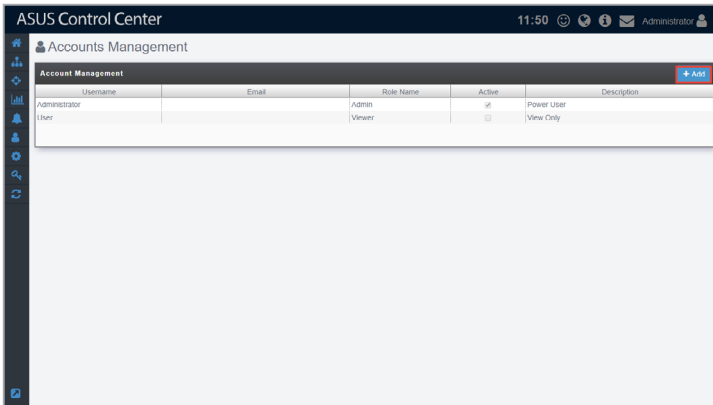
Adding a new account

You can add new accounts and apply customized roles to them, allowing you to and control the functions and information each account can access with ease. For example, assigning an account with Software User role which is customized to only allow users with this role access to ASUS Control Center software related functions, or creating an account with BIOS User role which is customized to only allow users access to ASUS Control Center BIOS related functions.



For more details on role privileges, please refer to **7.1 Role Privilege Management**.

1. Click on **Add**.



- 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 **7.1 Role Privilege Management**.

- 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.

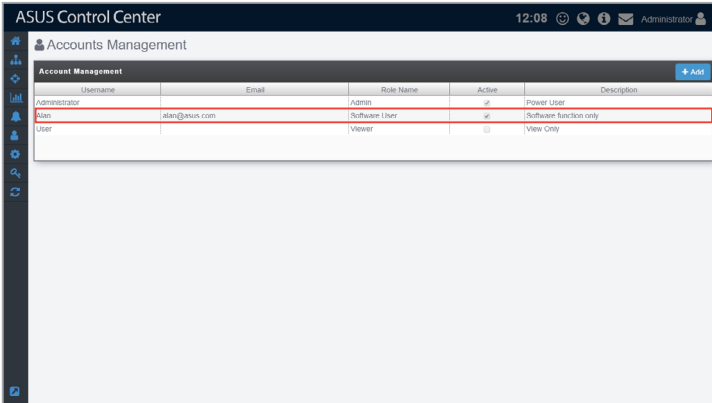
- 6. Click on **Save** once you have finished.

The screenshot shows a dialog box titled "Add New Account" with a green header. The form contains the following fields and values:

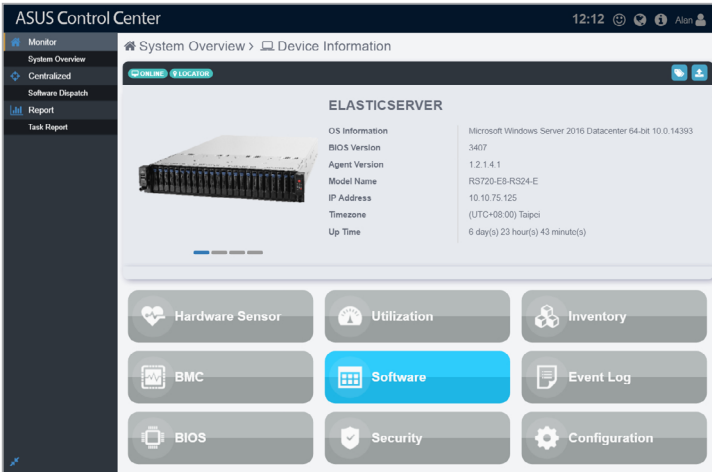
- Username: Alan
- Password: [masked]
- Confirm Password: [masked]
- Email: alan@asus.com
- Role Name: Software User
- Description: Software function only
- Active: Enable the account

At the bottom right, there are two buttons: "Cancel" and "Save".

7. Your newly created account should appear in the **Account Management** list.

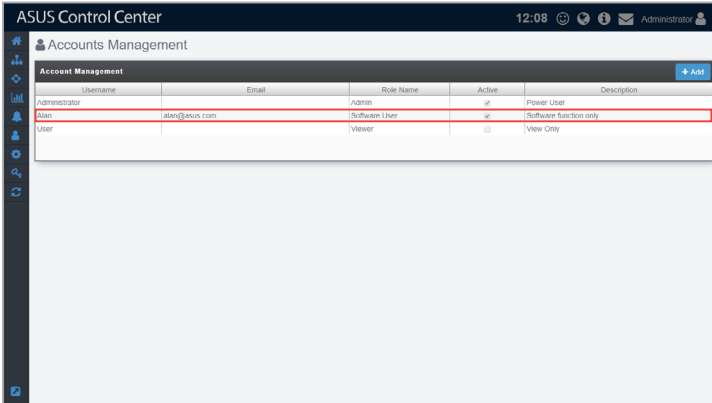


Logging in to ASUS Control Center using different accounts with different roles assigned will affect the items the account can gain access to, depending on the permissions assigned to the role selected. For example, logging in an account which you have set to a role with access only to Software related functions will result in the following screenshot.



Editing an account

1. Click on the account you wish to edit.



2. You can edit the **Password**, **Email**, **Role Name**, **Description**, and **Active** fields. Once you have finished editing click on **Save** to save the changes made.

The 'Edit Account' dialog box contains the following fields and options:

- 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

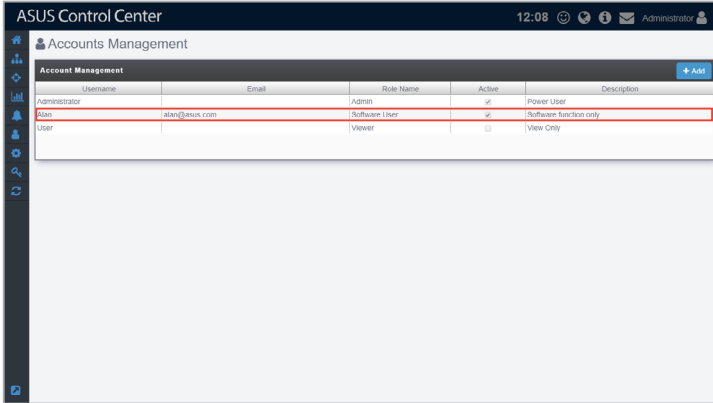
Buttons at the bottom: Cancel, Delete, Save.

Deleting an account

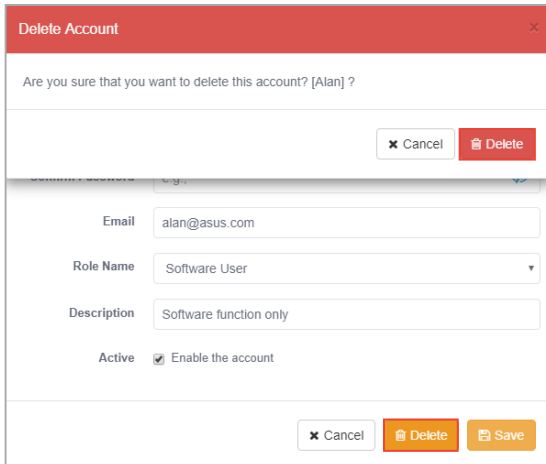


The default **Administrator** and **User** accounts cannot be deleted.

1. Click on the account you wish to delete.



2. Click on **Delete**, then click on **Delete** again on the confirmation pop-up to delete the account.




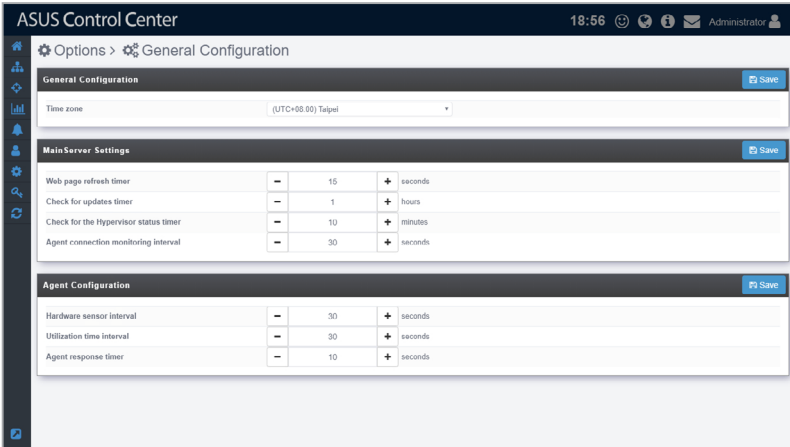
Chapter 8

This chapter describes system configuration options, and also backup and maintenance configurations.

8.1 General Configuration


The **General Configuration** allows you to configure different settings for the main ASUS Control Center server and agents, as well as set the time zone.

To access **General Configuration**, click  in the left menu, then click on **General Configuration**.







Adjusting items on the General configurations page

Configure the items in the **General Configurations** block, **MainServer Settings** block, and **Agent Configuration** block then click on **Save** to save the changes made. For more details on the different configuration options available, please refer to the tables below:

General Configurations	
Time Zone	<p>Adjust the time zone of the underlying Linux system the ASUS Control Center's main server is installed on.</p>  <ul style="list-style-type: none">• 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.

MainServer Settings


Web page refresh timer	<p>Set the time interval in seconds between each refresh of data on all webpages of the main server.</p>  <p>This setting will affect the response time for items such as System Overview and Event Log.</p>
Check for updates timer	<p>Set the time interval in hours for the main server and agent update check.</p>  <p>This setting will affect the main server and agent version check timer in the Updates page, and may require an Internet connection.</p>
Check for the Hypervisor status timer	<p>Set the time interval in minutes ASUS Control Center should perform a status check on managed vSpheres.</p>  <p>This setting will affect the response times for items in the VM Overview page such as vSphere hardware sensors and utilization .</p>
Device connection monitoring interval	<p>Set the time interval in seconds at which all managed device's agents should report connection status back to ASUS Control Center.</p>  <p>This setting will affect the response times for connection status in System Overview page, if a device's report time exceeds the response threshold time, the device will be seen as offline.</p>

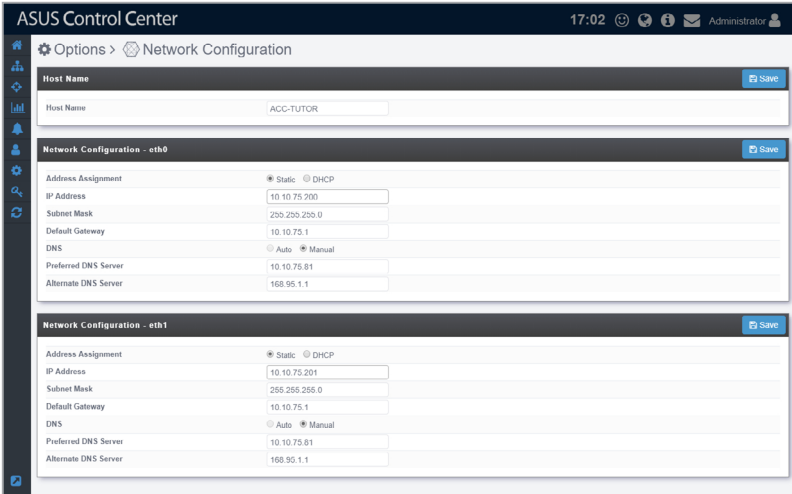
Agent Configuration

Hardware sensor interval	<p>Set the time interval in seconds for all managed device's agents to return Hardware Sensor values. The default setting is 30 seconds, which means that every 30 seconds the agents need to report Hardware Sensor values and status back to ASUS Control Center. 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 on the web page within 30 seconds (Web page refresh time could affect the update time).</p>
Utilization time interval	<p>Set the time interval in seconds for all managed device's agents to return Utilization values. The default setting is 30 seconds, which means that every 30 seconds the agents need to report Utilization values and status back to ASUS Control Center. 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 on the web page within 30 seconds (Web page refresh time could affect the update time).</p>
Agent response timer	<p>Set the time interval in seconds for all managed device's agents to query tasks from ASUS Control Center. The default setting is 10 seconds, which means that every 10 seconds the agents need to query ASUS Control Center if there is a task for that device. 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.</p>

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**.







Adjusting the Network configurations

Configure the items in the **Host Name** block and **Network Configuration** block then click on **Save** to save the changes made. For more details on the different configuration options available, please refer to the tables below:

Host Name	
Host Name	<p>The name of the ASUS Control Center main server.</p> <p> You will need to refer to the Host Name set here when manually installing Windows agents to devices.</p>

Network Configuration


Address Assignment	Select 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 address 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.

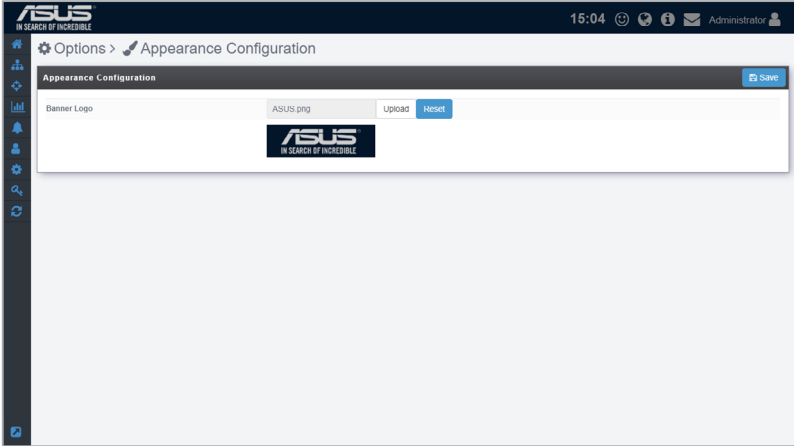


- The amount of **Network Configuration** blocks available will depend on the amount of network cards available.
- You will be logged out of ASUS Control Center when you save the changes made to the **Network Configuration** block(s). If you changed the IP address, you will need to enter the new IP address 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**.

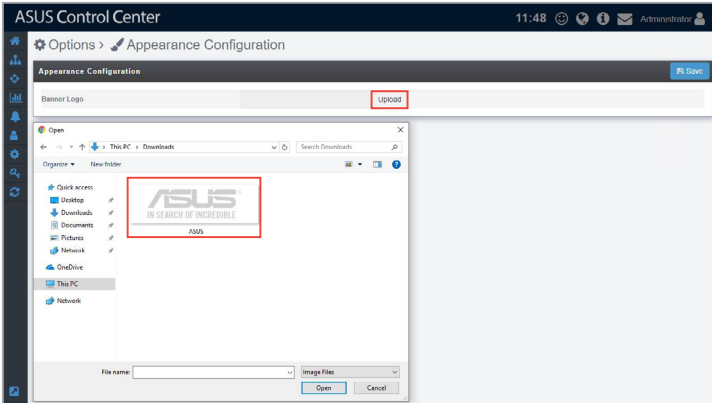


Setting a custom banner logo

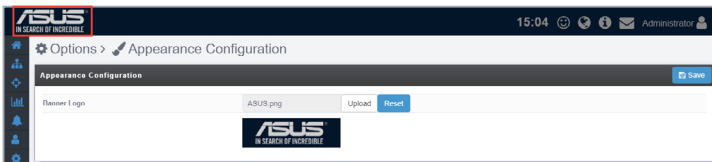
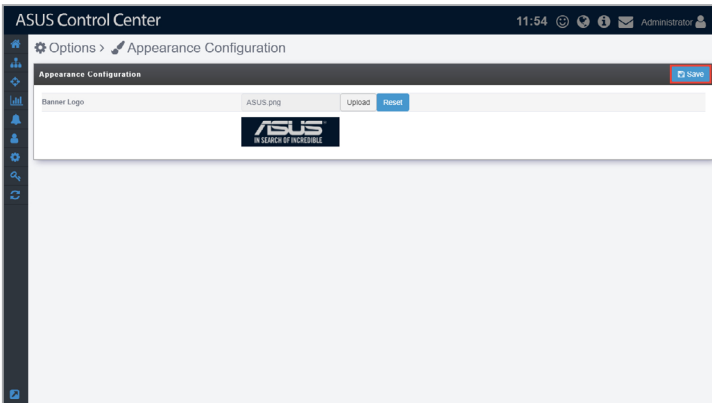
1. Click on **Upload**, then select your new banner logo.



The height dimension of the logo image file should be 56 pixels.

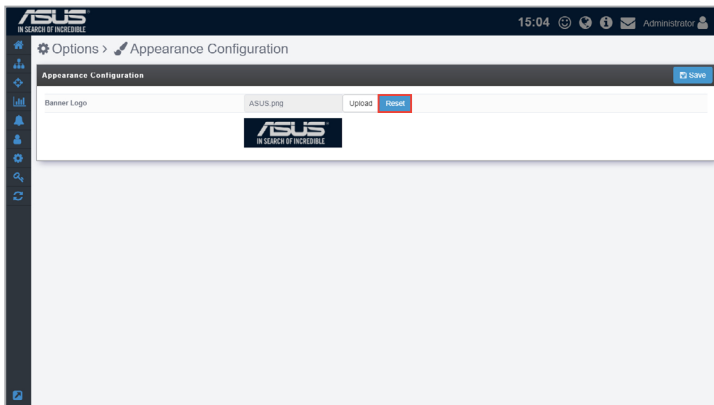


2. Once you have finished uploading the new banner logo, click on **Save**.

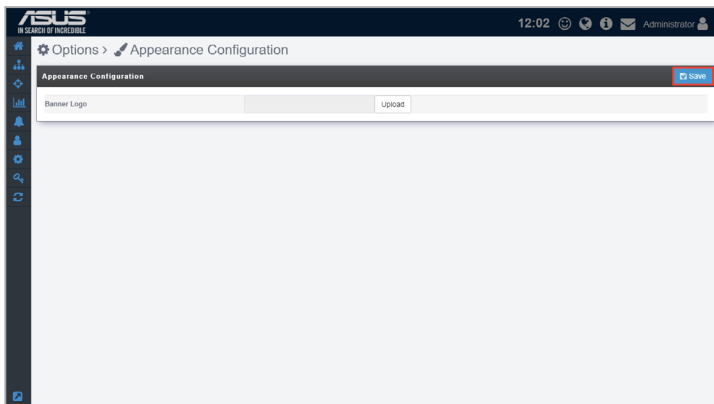


Resetting the banner logo

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

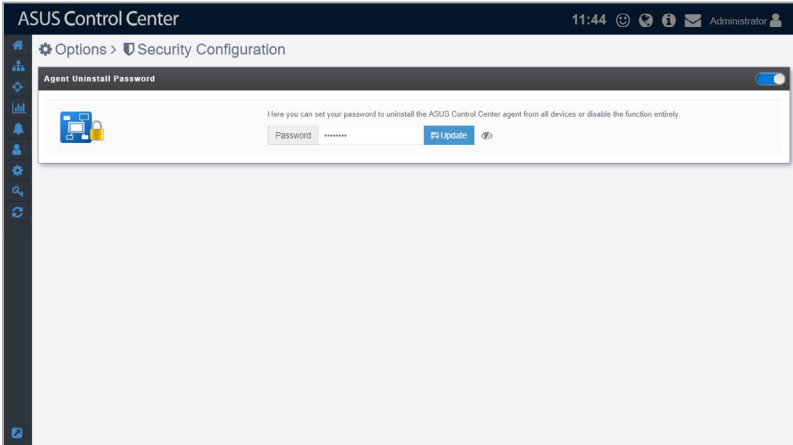


This function is only available for Windows® OS managed devices.

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.

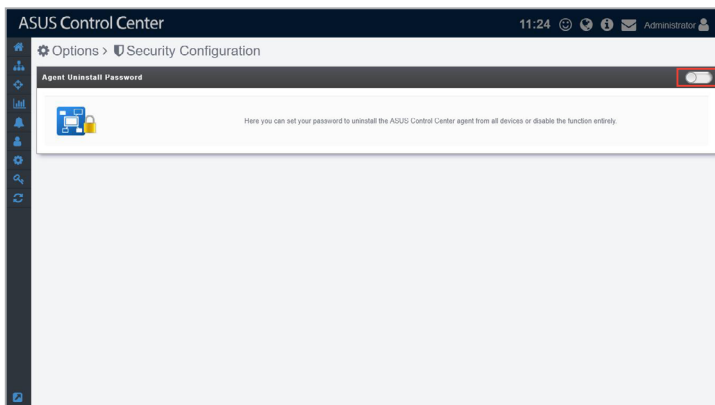
This password is separate from the agent uninstall password on individual devices (**Device Information > Configuration**), and setting this password will not override the individual agent uninstall passwords.

To access **Security Configuration**, click  in the left menu, then click on **Security Configuration**.

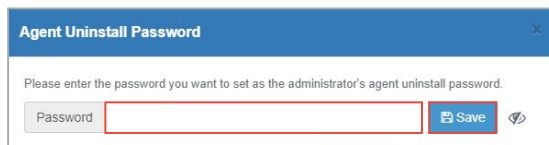


Setting a new Password

1. Click on the button to bring up the pop-up window to set the Administrator's Agent Uninstall Password.

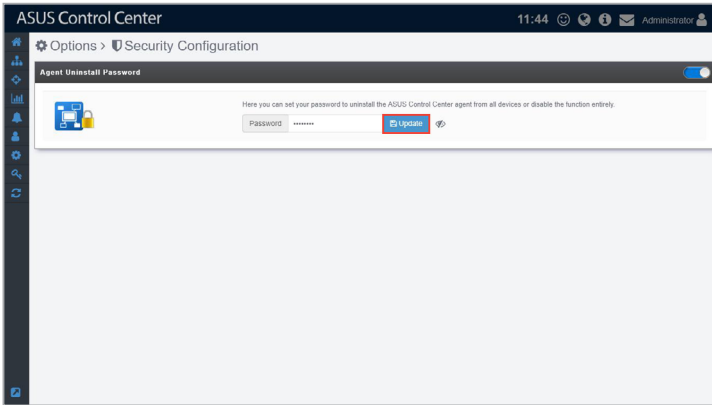


2. Enter the password you wish to set as the Administrator's Agent Uninstall Password, then click **Save** to set the new password.

A pop-up window titled 'Agent Uninstall Password' with a close button in the top right corner. The window contains the text: 'Please enter the password you want to set as the administrator's agent uninstall password.' Below this text is a text input field labeled 'Password' and a blue 'Save' button with a lock icon to its right. A red rectangular box highlights the 'Save' button.

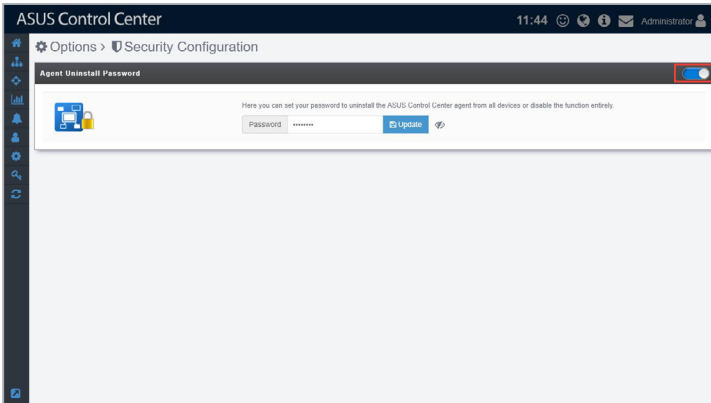
Editing the Password

Click on the **Update** button, then re-enter your new password and click on **Save** to save your new password.



Disabling the Password

Click on the button located at the top right to disable the Administrator's Agent Uninstall Password.




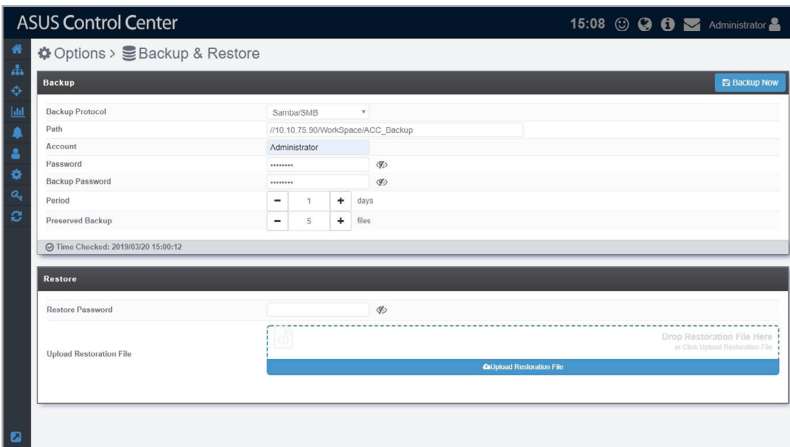
8.5 Backup & Restore



This function is only available on exclusive ASUS systems for ACC (ACC Physical Appliance). Please contact an ASUS representative for more information.

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 appliance.

To access **Backup & Restore**, click  in the left menu, then click on **Backup & Restore**.



The screenshot shows the ASUS Control Center interface. At the top, it says "ASUS Control Center" and "15:08" with user "Administrator". The breadcrumb is "Options > Backup & Restore".

Backup section:

- Backup Protocol: Samba/SMB
- Path: //10.10.75.90/Workspace/ACC_Backup
- Account: Administrator
- Password: [masked]
- Backup Password: [masked]
- Period: 1 days
- Preserved Backup: 5 files

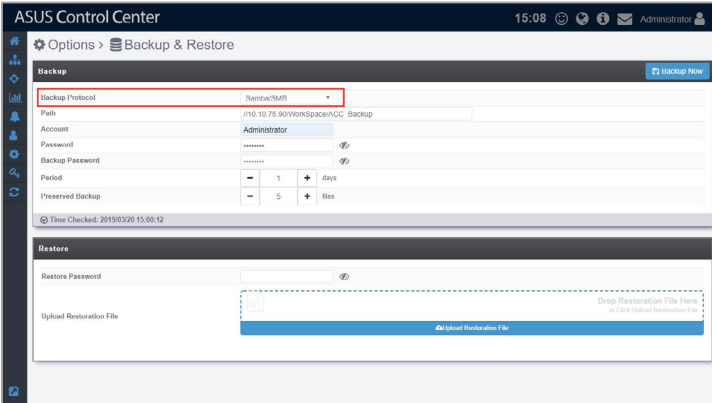
Time Checked: 2019/03/20 15:00:12

Restore section:

- Restore Password: [masked]
- Upload Restoration File: [Drop Restoration File Here or Click Upload Restoration File]

Setting the periodic backup

1. Select a Backup Protocol (currently only supports Samba / SMB protocols).



If you wish to back up your ACC to a Linux OS device's SMB folder, do the following:

- **Close SELinux**
 - a. For RHEL, CentOS, Scientific Linux
 1. Open `/etc/sysconfig/selinux`.
 2. Set `SELINUX=enforcing` to `SELINUX=disabled`.
 - b. For Debian, Ubuntu

SELinux is not installed by default in Debian and Ubuntu.
- **Adding to the Firewall whitelist**
 - a. For RHEL, CentOS, Scientific Linux
 - If you are using `iptables`:
 1. Input the following command to allow 137, 138, and 139 ports:

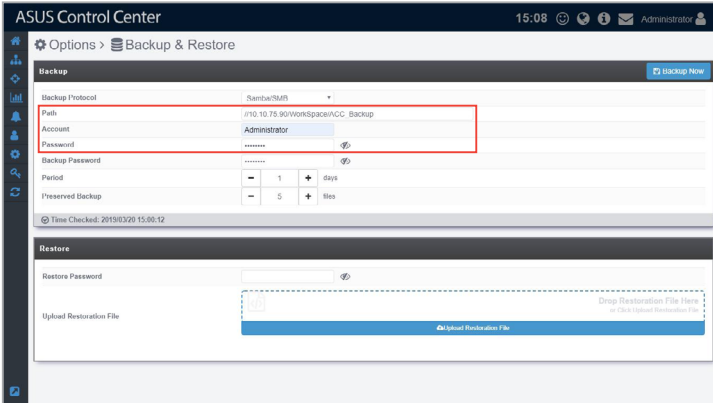
```
-A INPUT -m state --state NEW -m udp -p udp --dport 137 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 138 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT
```

2. Restart the service for the changes to take effect by using the following command: `systemctl restart iptables.`
- If you are using **firewall**:
Enter the following commands to add Samba access privileges:
`firewall-cmd -permanent -zone=public --add-service=samba,`
 - b. For Debian, Ubuntu
If you are using **ufw**, the system has already added `nf_conntrack_netbios_ns` to `IPT_MODULES` under `/etc/default/ufw` by default, so access should already be allowed.
- **Enable write permissions for the destination folder**
The “Write” permission should be enabled for “other(O)” in the folder you wish to back up to. You can use the following command:
`chmod -R 755 /home/acc/backup.`
 - **Modify the Samba configuration file**
 1. Open `/etc/samba/smb.conf`.
 2. Set the **security** variable in **Global Setting** to “user”.
 3. Set the **writable** variable in **Share Definitions** to “yes”.

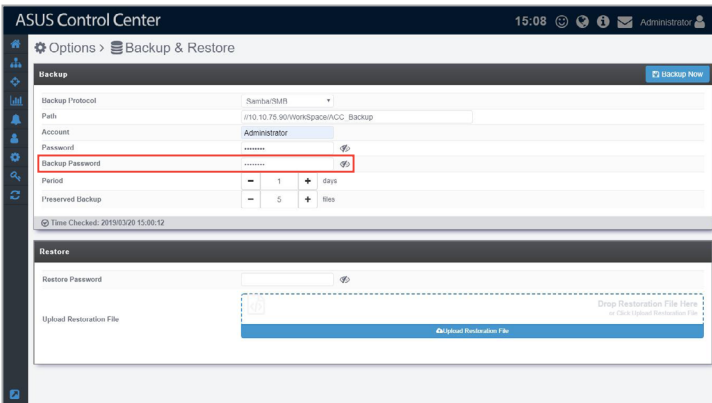
2. Enter the folder path of a shared folder, and the administrator account and password of the shared folder device into the **Path**, **Account**, and **Password** fields.



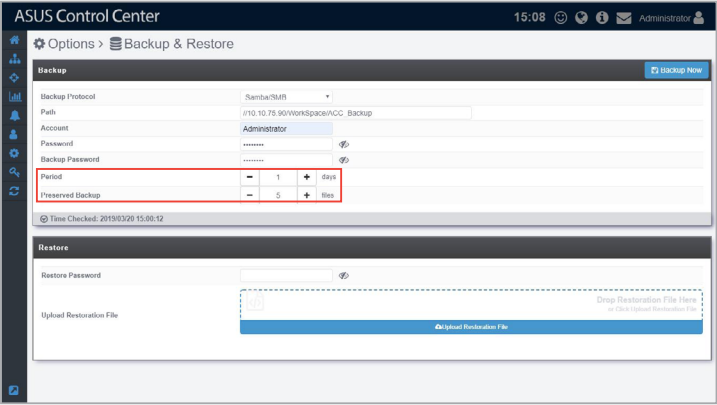
- The folder should be set as a shared folder and discoverable by the system you wish to back up, and should have read and write permissions enabled.
- Take note of the syntax of the path. Ensure to use the correct syntax of your selected protocol from the previous step.



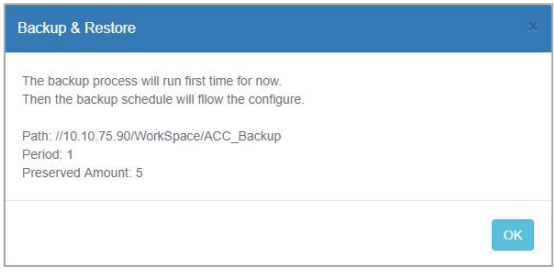
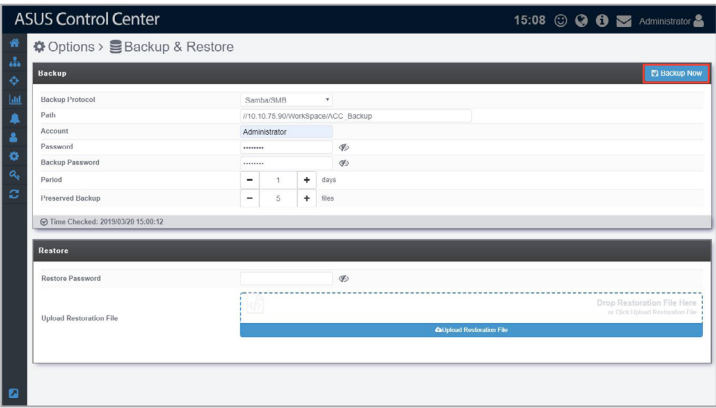
3. Enter a backup password, this password is for when you use the **Restore** function.



4. 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.

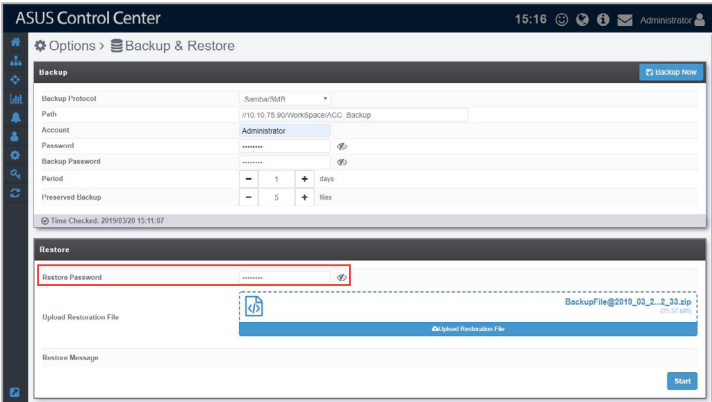


5. Click on **Backup Now** once you have finished, to save the settings made and also prompt the first backup.

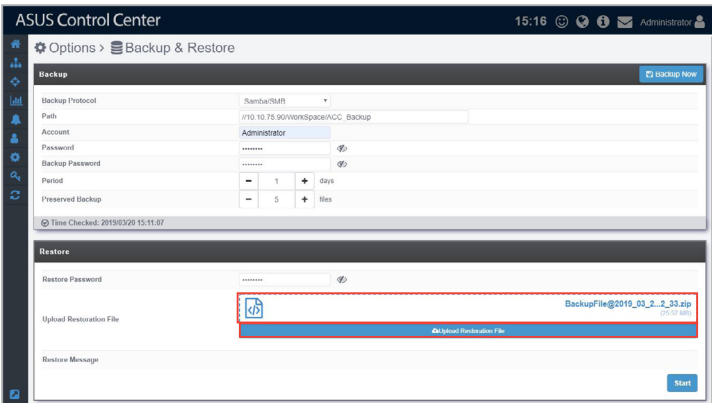


Restoring the backup file

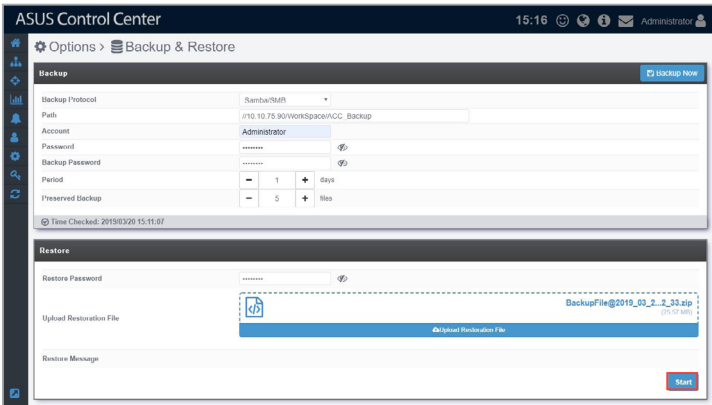
1. Enter the **Backup Password** previously set when setting the periodic backup into the **Restore Password** field.



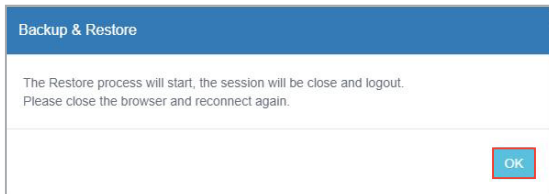
2. Drag a backup file you wish to restore into the **Upload Restoration File** field, or click on **Upload Restoration File** and select the backup file you wish to use to restore.



3. Enter a **Restore Message** if you wish to add a message, then click on **Start** to begin the backup restoration.




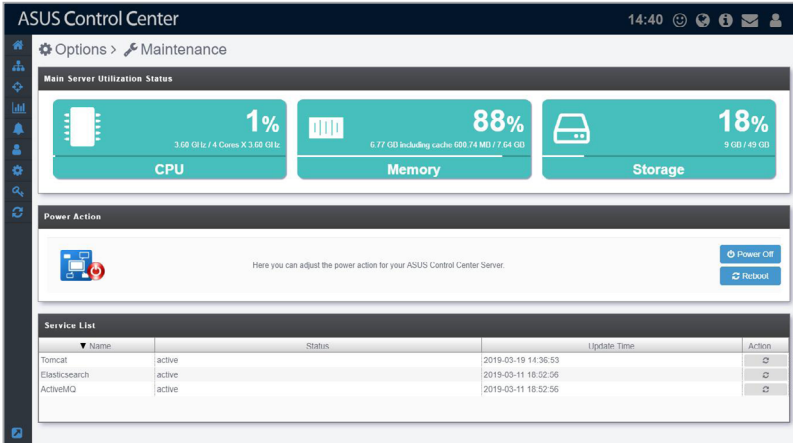
The session will expire and you will be logged out of ACC when the restoration begins, please restart the browser and login again once the restoration is complete.



8.6 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**.



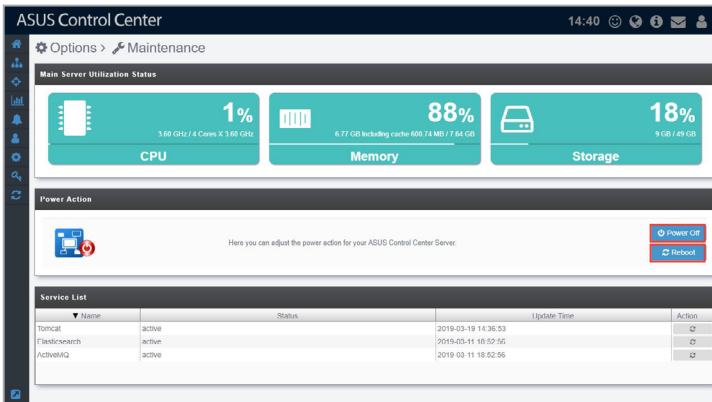
The screenshot displays the ASUS Control Center interface for the Maintenance section. The top navigation bar shows 'Options > Maintenance' and the time '14:40'. The main content area is divided into three sections:

- Main Server Utilization Status:** Three cards showing CPU usage at 1% (3.60 GHz / 4 Cores X 3.10 GHz), Memory usage at 88% (6.77 GB including cache 600.74 MB / 7.64 GB), and Storage usage at 18% (9 GB / 49 GB).
- Power Action:** A section with a power icon and text 'Here you can adjust the power action for your ASUS Control Center Server.' It includes 'Power Off' and 'Reboot' buttons.
- Service List:** A table listing active services.

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	

Configuring the power option of Hypervisors

1. Click on **Power Off** or **Reboot** to power off or reboot the hypervisor.



This screenshot is identical to the one above, showing the ASUS Control Center Maintenance page with server utilization statistics, power action buttons, and a service list table.

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 **Chapter 7 Account Management**.

Administrator's Password

Please enter the administrator's password to authenticate your power action.

Password:

Confirm

Restarting the Services

Click on the restart button next to the service you wish to restart.

The screenshot shows the ASUS Control Center interface. At the top, it displays 'ASUS Control Center' and the time '14:40'. Below this, there are navigation options for 'Options' and 'Maintenance'. The 'Main Server Utilization Status' section shows three metrics: CPU at 1% (3.68 GHz / 4 Cores X 3.68 GHz), Memory at 88% (6.77 GB including cache / 100.24 MB / 7.64 GB), and Storage at 18% (9 GB / 49 GB). The 'Power Action' section contains buttons for 'Power Off' and 'Reboot'. The 'Service List' table is shown below, with a red box highlighting the 'Action' column.

Name	Status	Update Time	Action
Tomcat	active	2019-03-19 14:36:53	⏏
findchsearch	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

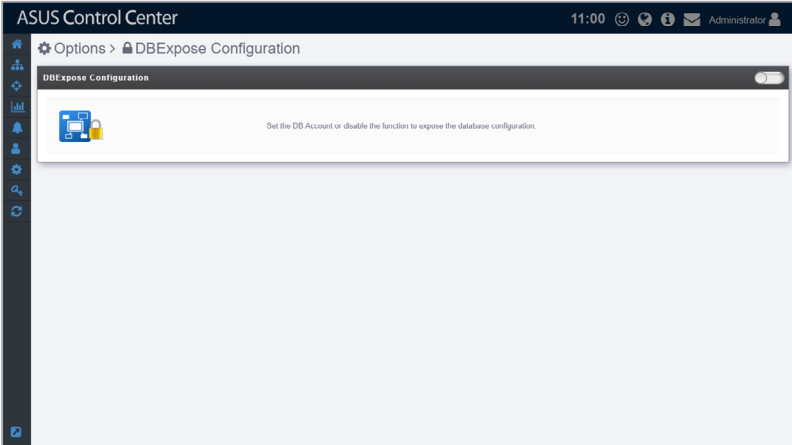
Restart successfully, please wait a moment and refresh website.

OK

8.7 DBExpose Configuration

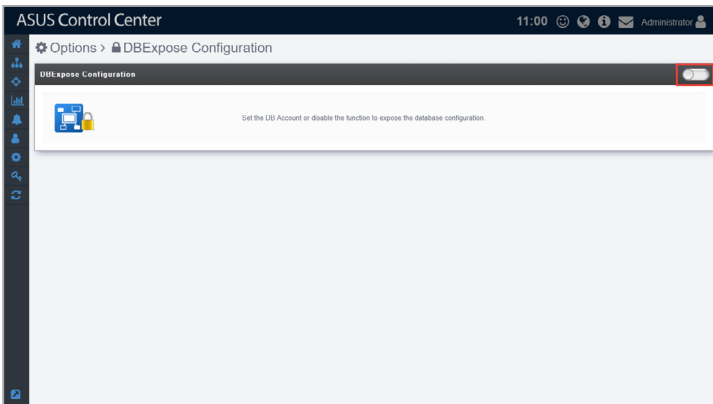
The **DBExpose Configuration** allows you to set an account and password which allows users to use third-party software, such as MySQL Workbench to access data on ASUS Control Center, such as device information or metadata. This information is read-only and cannot be edited.

To access **DBExpose Configuration**, click  in the left menu, then click on **DBExpose Configuration**.

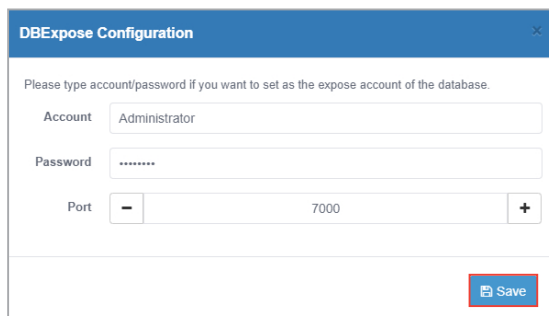


To set the DBExpose account and password

1. Click on the slide button on the top right of the main screen.



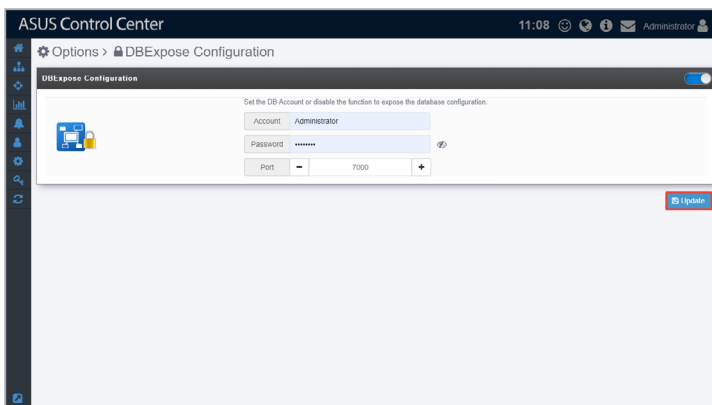
2. Enter an account and password, then enter a port (between 7000-7999) which is not being used. Once you have finished entered the required fields, click on **Save**.



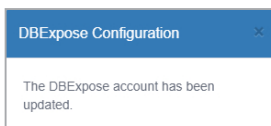
The screenshot shows a dialog box titled "DBExpose Configuration" with a close button (X) in the top right corner. Below the title bar, there is a text prompt: "Please type account/password if you want to set as the expose account of the database." The form contains three input fields: "Account" with the text "Administrator", "Password" with masked characters "*****", and "Port" with a numeric spinner set to "7000". A "Save" button is located in the bottom right corner of the dialog.

To edit the DBExpose account information

Edit the account, password, and port information then click on **Update** to save the changes made.



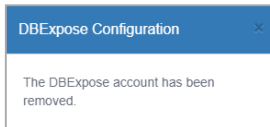
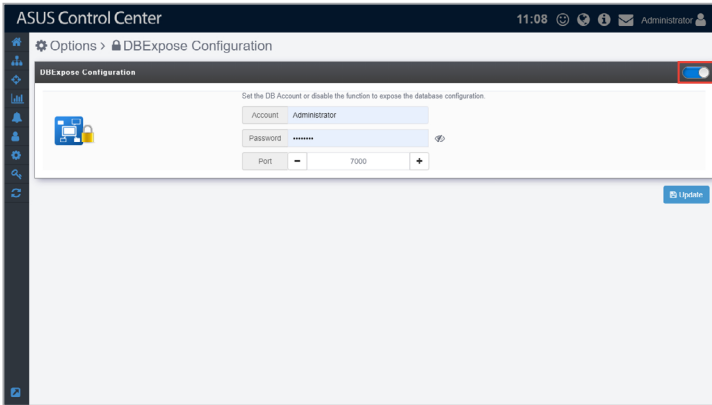
The screenshot shows the ASUS Control Center interface. The top navigation bar includes "ASUS Control Center", the time "11:08", and the user "Administrator". The main content area is titled "Options > DBExpose Configuration". Below this, there is a sub-section "DBExpose Configuration" with a toggle switch that is turned on. The sub-section contains the same form as the previous screenshot, with fields for "Account" (Administrator), "Password" (*****), and "Port" (7000). An "Update" button is located in the bottom right corner of the sub-section.



The screenshot shows a small dialog box titled "DBExpose Configuration" with a close button (X) in the top right corner. The message inside the dialog reads: "The DBExpose account has been updated."

To delete the DBExpose account information

Click on the slide button on the top right to disable and delete the DBExposure Configuration settings.



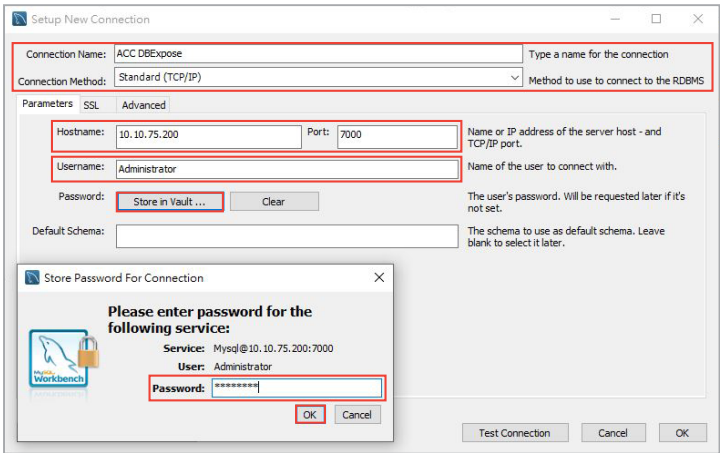
Using a third-party software to access ASUS Control Center



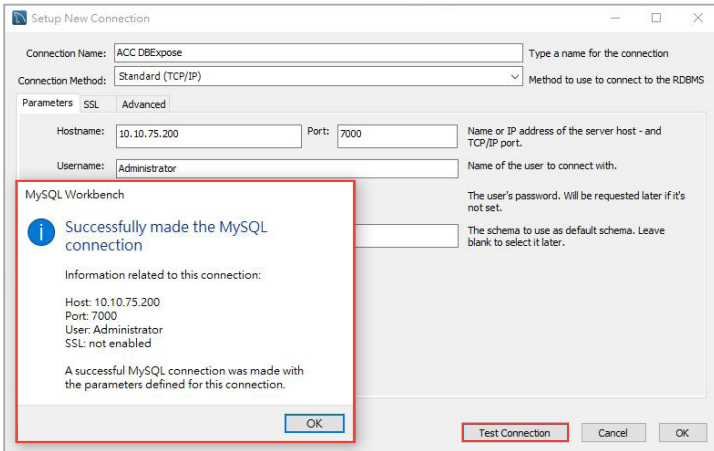
The example in this section is for reference only.

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**.



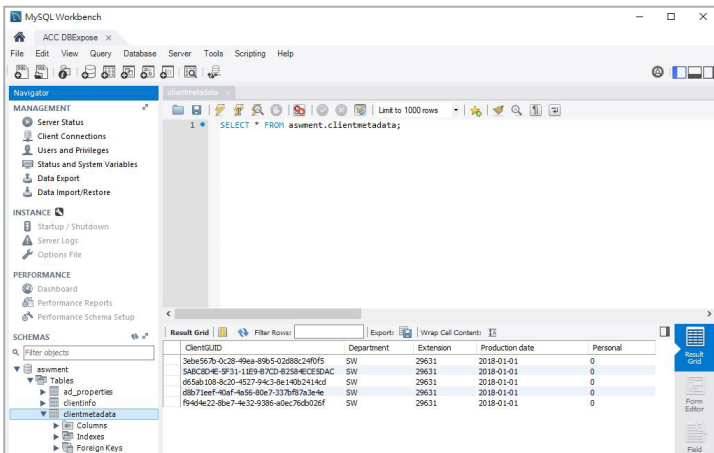
- Click on **Test Connection** to test if the connection to ASUS Control Center was successfully created.



- Save the connection settings, now when using MySQL Workbench, you should be able to access some of the data on ASUS Control Center.



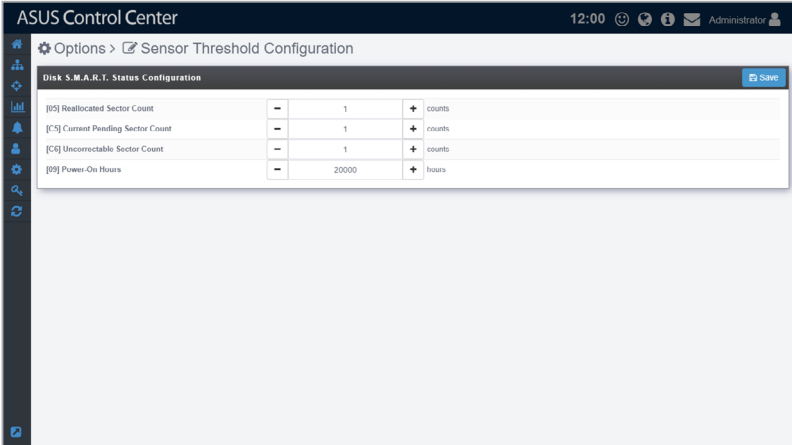
The screenshot below is an example of accessing the metadata of ASUS Control Center.



8.8 Sensor Threshold Configuration

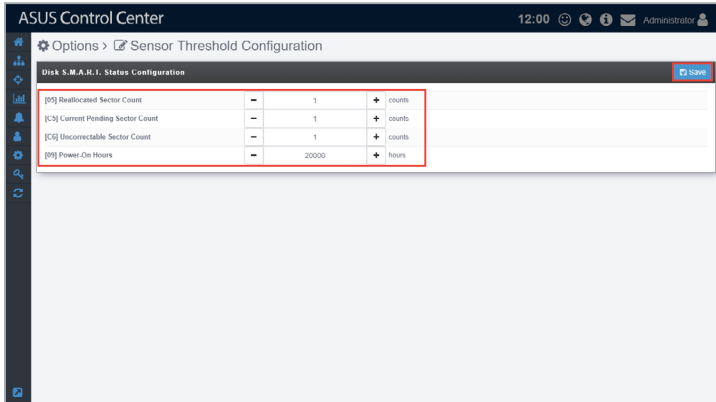
The **Sensor Threshold Configuration** allows you to centrally configure the threshold values of all managed devices, providing you with an effortless method of setting threshold values of all managed devices, instead of having to configure each device's threshold values individually.

To access **Sensor Threshold Configuration**, click  in the left menu, then click on **Sensor Threshold**.



Adjusting the Disk S.M.A.R.T. status configurations

Adjust the disk S.M.A.R.T. status configurations, then click on Save to save the changes made and apply the changes made to all managed devices.



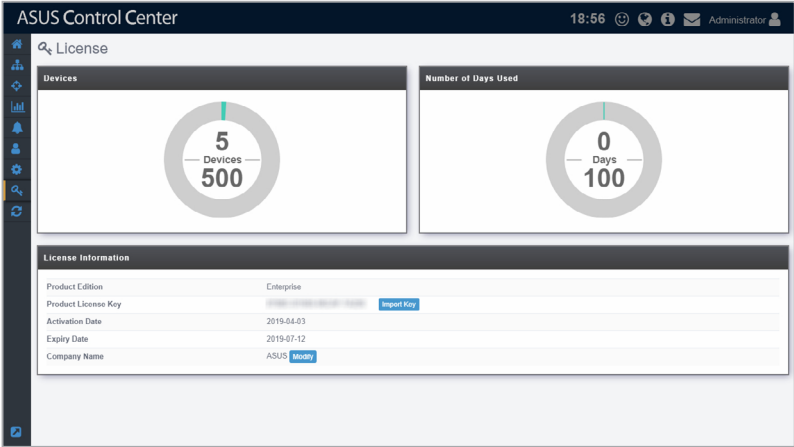
Chapter 9

This chapter describes the license settings.

9.1 License Information

The **License** page displays the license information of your ASUS Control Center, this includes your license key, activation date, expiry date and edition, and also allows you to 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.



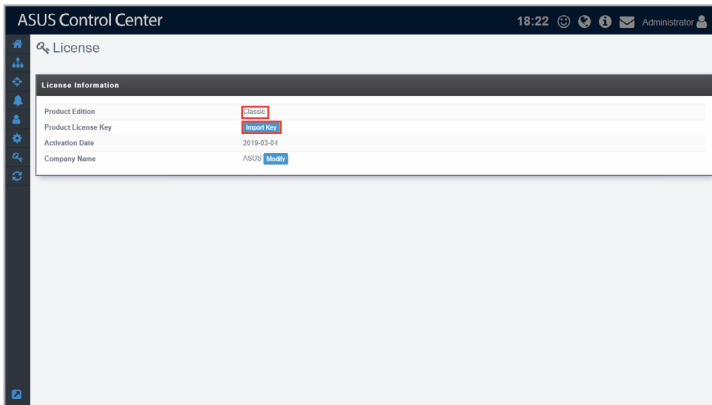
Importing a License key

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.

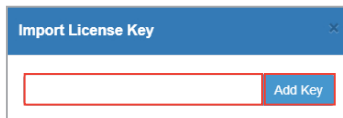


A working Internet connection is required when verifying the upgrade License key.

1. Click on **Import Key**.

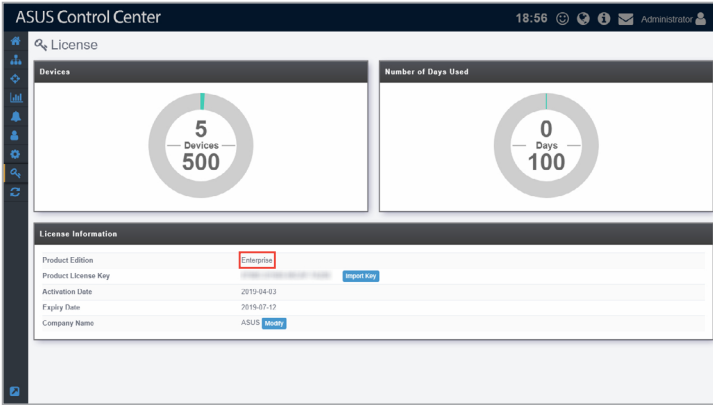


2. Enter your license key and click **Add Key**.



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, you should see the details of your license displayed now.



Chapter 10

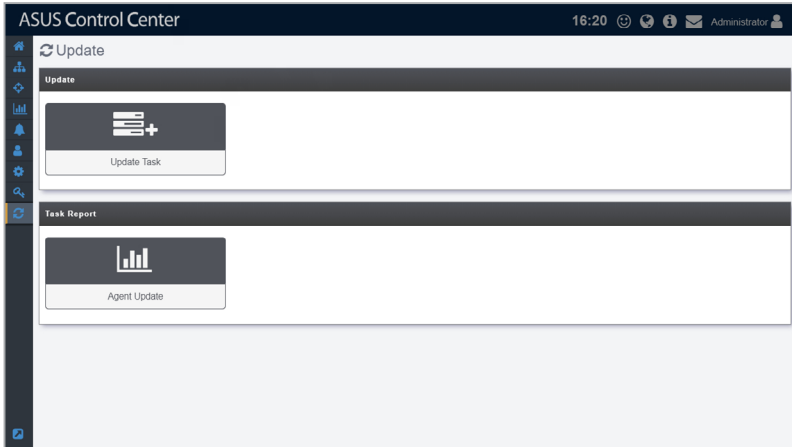
This chapter describes the main server and agent update configurations.

Update

10.1 Update

Update will allow you to update the Windows and Linux agents on managed devices, or update the ASUS Control Center main server, and also allow you to view the Agent Update Report for information on the update status.

To access **Update**, click  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 **2.1.4 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 **2.1.3 Options**.

10.1.1 Update Task

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**.




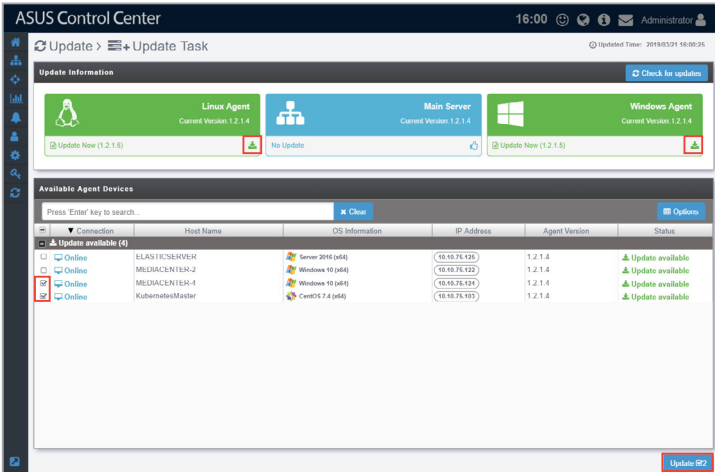
- Ensure to add *asuscontrolcenter.asus.com/** to your firewall exceptions list to enable update checks.
- Ensure you have a stable Internet connection.

The screenshot displays the 'Update Task' section of the ASUS Control Center. At the top, there are three cards for 'Linux Agent', 'Main Server', and 'Windows Agent', each showing 'Current Version 1.2.1.4' and 'No Update'. A red box highlights the 'Check for updates' button in the top right corner. Below this is a table titled 'Available Agent Devices' with a search bar and a 'Clear' button. The table has columns for Connection, Host Name, OS Information, IP Address, Agent Version, and Status. The table lists four devices, all with 'Online' status and 'Latest Version' (1.2.1.4).

Connection	Host Name	OS Information	IP Address	Agent Version	Status
Online	PLASTICSERVER	Server 2016 (x64)	10.10.75.125	1.2.1.4	Latest Version
Online	MEDIACENTER-184-2	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	KubomctoolMaztor	CentOS 7 (x86)	10.10.75.102	1.2.1.4	Latest Version

Updating Windows and Linux agents

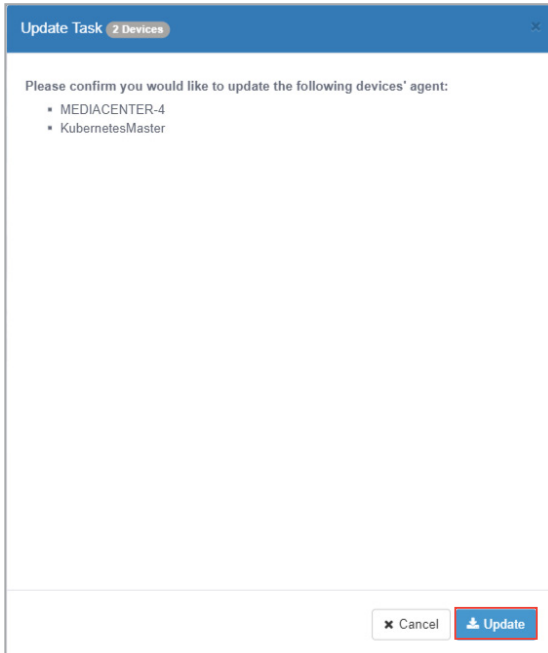
- 1. When an update is available for Linux and/or Windows Agents it will be displayed under **Update Information**, and the **Linux Agent** and/or **Windows Agent** block will be displayed in green.
- 2. Click on  in the **Linux Agent** and/or **Windows Agent** block to download the agent. Once the download is complete, the **Linux Agent** and/or **Windows Agent** block will be displayed in blue.
- 3. Select the device(s) you wish to update agents for in the **Available Agent Devices** list.
- 4. Click on **Update**.



5. Click **Update** on the confirmation pop-up window to start the update process.



You do not need to uninstall the agents on the selected devices before updating.




- 6. After the agent updates have been completed, you will be redirected to the Agent Update Report screen.

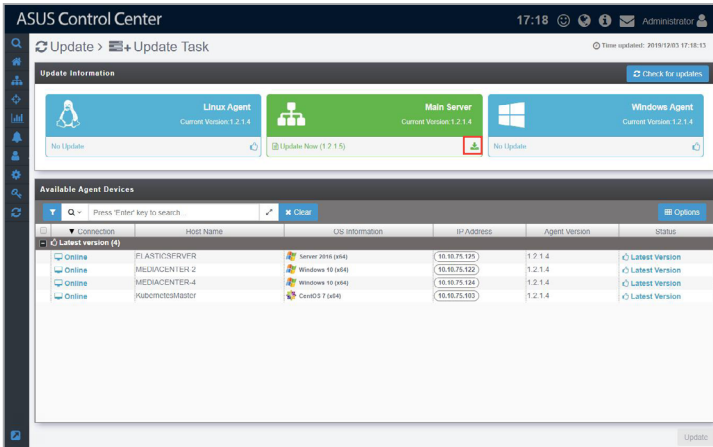



For more details on the Agent Update Report, refer to **10.1.2 Agent Update Report**.

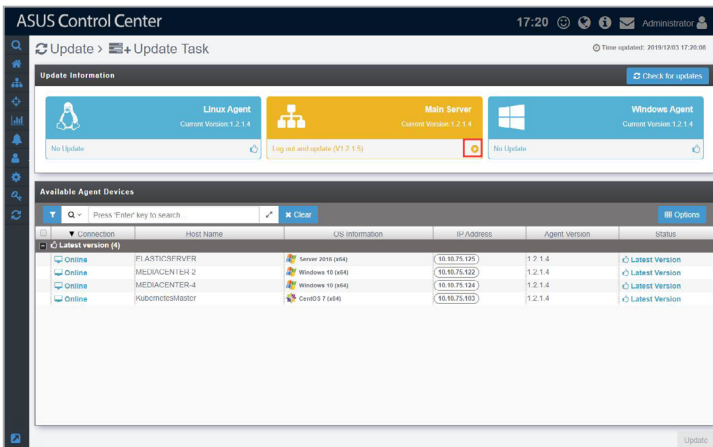
Host Name	OS	IP	Status	Old Version	Message	Creation Time	Update Time
MEDIACENTER 4	Windows 10 (x64)	10.10.75.124	Success	1.2.1.4	Agent Updated	2019-03-21 16:14	2019-03-21 16:15
KubernetesMaster	CentOS 7.4 (x64)	10.10.75.103	Success	1.2.1.4	Agent Updated	2019-03-21 16:14	2019-03-21 16:15

Updating ASUS Control Center main server

1. When an update is available for the main server, it will be displayed under **Update Information** and the **Main Server** block will be displayed in green. Click on  in the **Main Server** block to download the update files.



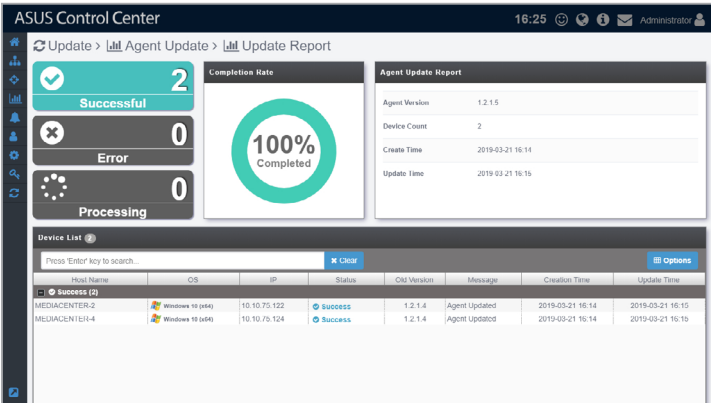
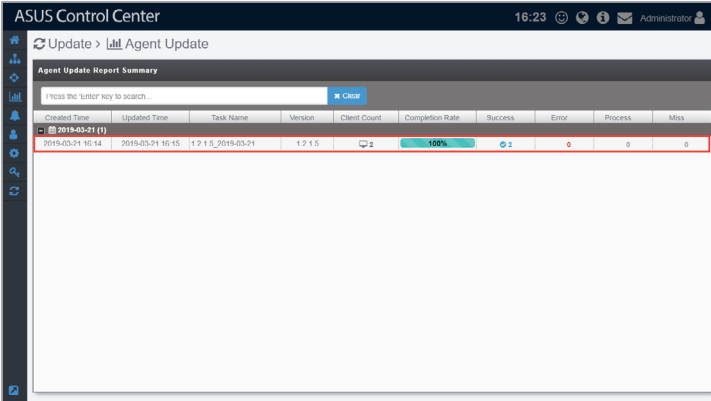
2. Once the update files are successfully downloaded, the **Main Server** block should be displayed in orange. Now click on  to update the ASUS Control Center main server. You will also be logged out of ASUS Control Center when the main server is updating.



3. Log into ASUS Control Center again after the update is completed.

10.1.2 Agent Update Report

The Agent Update Report will display information of each time you update the deployed Windows and Linux agents. Each item showed on the **Agent Update Report** represents a single batch of agent updates; clicking on each item will allow you to view information on the devices whose agents were updated in that batch.



Appendix

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

Appendix

System Requirements

Hardware Host Server Requirements

Virtual machine hypervisors		Oracle VirtualBox 5.1.x 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)	100 GB disk space
	Hypervisor recommended	Virtual Box, VMware
Minimum VM requirement (50 clients capability)	vCPU (Cores)	2 cores
	Memory (GB)	8 GB memory
	Disk (GB)	100 GB disk space
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 capabilities above 500 clients.

Managed Clients Requirements

Supported client OS	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows 7 Windows 8.1 Windows 10 Windows Embedded 7 RedHat 6.4~7.4 CenOS 6.4~7.4 Scientific Linux 6.4~7.4
Requirement on Client Systems	<u>Windows</u> .NET Framework 3.5 <u>Linux</u> sysstat, smartmontools, wireless-tools, ethtool, ipmitool, Open IPMI driver, ASMB

ASUS contact information

ASUSTeK COMPUTER INC.

Address 4F, No. 150, Li-Te Rd., Peitou, Taipei 112, Taiwan
Telephone +886-2-2894-3447
Fax +886-2-2890-7798
Web site <https://www.asus.com>

Technical Support

Telephone +86-21-38429911
Fax +86-21-58668722 ext: 9101
Online Support <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=en>

ASUSTeK COMPUTER INC. (Taiwan)

Address 4F, No. 150, Li-Te Rd., Peitou, Taipei 112, Taiwan
Telephone +886-2-2894-3447
Fax +886-2-2890-7798
Web site <https://www.asus.com/tw/>

Technical Support

Telephone +886-2-2894-3447 (0800-093-456)
Online Support <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=zh-tw>

ASUSTeK COMPUTER INC. (China)

Address No. 5077, Jindu Road, Minhang District, Shanghai, China
Telephone +86-21-5442-1616
Fax +86-21-5442-0099
Web site <https://www.asus.com.cn>

Technical Support

Telephone +86-20-2804-7506 (400-620-6655)
Online Support <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=zh-cn>

ASUS contact information

ASUS COMPUTER INTERNATIONAL (America)

Address 800 Corporate Way, Fremont, CA 94539, USA
Fax +1-510-608-4555
Web site <https://www.asus.com/us/>

Technical Support

Support fax +1-812-284-0883
General support +1-812-282-2787
Online support <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=en-us>

ASUS COMPUTER GmbH (Germany and Austria)

Address Harkort Str. 21-23, 40880 Ratingen, Germany
Fax +49-2102-959911
Web site <https://www.asus.com/de/>

Technical Support

Telephone +49-1805-010923
Support Fax +49-2102-959911
Online support <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=de-de>

