



# **ASUS Control Center Express**

**User Manual**

E15784  
First Edition  
September 2019

**Copyright © 2019 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 .....	vi
------------------------	----

## Chapter 1: Getting Started

<b>1.1</b>	<b>Setting up.....</b>	<b>1-2</b>
1.1.1	Installing ASUS Control Center Express (ACCE) .....	1-2
1.1.2	Logging in to ASUS Control Center Express .....	1-2
1.1.3	Changing the account password.....	1-3
1.1.4	Activating your license key.....	1-4
1.1.5	Changing languages .....	1-4
<b>1.2</b>	<b>Main dashboard overview .....</b>	<b>1-5</b>

## Chapter 2: Dashboard Overview

<b>2.1</b>	<b>System overview .....</b>	<b>2-2</b>
2.1.1	Switching sensor views .....	2-3
2.1.2	Event Log.....	2-3
<b>2.2</b>	<b>Device overview .....</b>	<b>2-4</b>
2.2.1	Filtering client devices.....	2-4
2.2.2	Export device list.....	2-4
2.2.3	Using shortcut functions.....	2-5
<b>2.3</b>	<b>Customizing your dashboard .....</b>	<b>2-7</b>
2.3.1	Customizing the Graphic dashboard view for the first time .....	2-7
2.3.2	Editing the shortcut icons and background .....	2-9
2.3.3	Using the shortcut icons.....	2-9
<b>2.4</b>	<b>Task Scheduler.....</b>	<b>2-10</b>
2.4.1	Task scheduler calendar overview.....	2-10
2.4.2	Setting a new task.....	2-11
2.4.3	Editing a task .....	2-17
2.4.4	Deleting a task .....	2-18

## Chapter 3: Deploy Management

<b>3.1</b>	<b>Deploying agents .....</b>	<b>3-2</b>
3.1.1	Client requirements.....	3-2
3.1.2	Installing Agents manually .....	3-2
3.1.3	Deploying agents through ACC Express .....	3-4
<b>3.2</b>	<b>Removing agents .....</b>	<b>3-11</b>

# Contents

## Chapter 4: Device Information

<b>4.1</b>	<b>Device Information Overview</b> .....	<b>4-2</b>
<b>4.2</b>	<b>Hardware Sensor (software)</b> .....	<b>4-4</b>
	4.2.1 Editing the threshold value.....	4-5
<b>4.3</b>	<b>Utilitization</b> .....	<b>4-6</b>
	4.3.1 Editing the threshold value.....	4-6
<b>4.4</b>	<b>Inventory (Software)</b> .....	<b>4-7</b>
	4.4.1 Disk Information .....	4-7
	4.4.1 Disk Information .....	4-8
<b>4.5</b>	<b>Software</b> .....	<b>4-9</b>
	4.5.1 Application tab .....	4-9
	4.5.2 Processes tab .....	4-10
	4.5.3 Services tab .....	4-10
	4.5.4 Environment tab.....	4-11
<b>4.6</b>	<b>Control (software)</b> .....	<b>4-12</b>
<b>4.7</b>	<b>Event Log</b> .....	<b>4-13</b>
	4.7.1 Monitor tab .....	4-13
	4.7.2 Application tab .....	4-14
	4.7.3 System tab .....	4-15
	4.7.4 Security tab .....	4-16
<b>4.8</b>	<b>Remote Desktop</b> .....	<b>4-17</b>
	4.8.1 General Remote Desktop .....	4-17
	4.8.2 Out-of-band Management Remote Desktop .....	4-18
<b>4.9</b>	<b>USB Redirection</b> .....	<b>4-21</b>
<b>4.10</b>	<b>BIOS</b> .....	<b>4-22</b>
	4.10.1 BIOS Setting .....	4-22
	4.10.2 BIOS Flash Management.....	4-23

## Chapter 5: Management Functions

<b>5.1</b>	<b>Management Control Overview</b> .....	<b>5-2</b>
	5.1.1 Scanning for devices.....	5-2
	5.1.2 Using shortcut functions.....	5-2
	5.1.3 Setting the password for RTL8117 .....	5-3
<b>5.2</b>	<b>Management Control Information Overview</b> .....	<b>5-5</b>
<b>5.3</b>	<b>Hardware Sensor (hardware)</b> .....	<b>5-7</b>

# Contents

<b>5.4</b>	<b>Inventory (hardware)</b> .....	<b>5-7</b>
<b>5.5</b>	<b>Control (hardware)</b> .....	<b>5-8</b>
<b>5.6</b>	<b>Remote Desktop</b> .....	<b>5-9</b>
<b>5.7</b>	<b>USB Redirection</b> .....	<b>5-9</b>
<b>5.8</b>	<b>Smart BIOS</b> .....	<b>5-9</b>
5.8.1	BIOS Flash Management.....	5-9
<b>5.9</b>	<b>Firmware Update</b> .....	<b>5-13</b>
5.9.1	Uploading and updating firmware .....	5-13
<b>5.10</b>	<b>Software Management</b> .....	<b>5-15</b>
5.10.1	Software Dispatch.....	5-15
5.10.2	Software Pool.....	5-17
5.10.3	Software Information.....	5-22
5.10.4	Software Blacklist.....	5-23
<b>5.11</b>	<b>Metadata Management</b> .....	<b>5-25</b>
5.11.1	Adding metadata fields .....	5-25
5.11.2	Removing metadata fields .....	5-27
5.11.3	Updating the metadata manually .....	5-28
5.11.4	Updating the metadata using a batch update .....	5-29

## Chapter 6: Settings Migrator

<b>6.1</b>	<b>Settings Migrator</b> .....	<b>6-2</b>
6.1.1	Importing configurations of ACC CSM server .....	6-2
6.1.2	Deploying ACCE agents to ACC CSM devices .....	6-4

## Chapter 7: Account & General Settings

<b>7.1</b>	<b>Settings menu</b> .....	<b>7-2</b>
7.1.1	SMTP Settings .....	7-2
7.1.2	Rule Management.....	7-3
7.1.3	General Configuration.....	7-10
7.1.4	License.....	7-14
<b>7.2</b>	<b>Account menu</b> .....	<b>7-19</b>
7.2.1	Account Settings .....	7-19
7.2.1	Role Privilege Management.....	7-23
<b>7.3</b>	<b>QR Code</b> .....	<b>7-26</b>
<b>7.4</b>	<b>Submit Feedback</b> .....	<b>7-26</b>

# About this guide

This user guide contains the information you need when using and configuring ASUS Control Center Express (ACCE).

## How this guide is organized

This guide contains the following parts:

**1. Chapter 1: Getting Started**

This chapter provides a quick overview of ASUS Control Center Express, and how to install and set it up.

**2. Chapter 2: Dashboard Overview**

This chapter describes the functions available on the main dashboard.

**3. Chapter 3: Deploy Management**

This chapter describes how to deploy ASUS Control Center agents and remove agents through Microsoft® Active Directory or manually.

**4. Chapter 4: Device Information**

This chapter describes the device information and software controlled options for managing the device.

**5. Chapter 5: Management Functions**

This chapter describes the metadata management, software management, and hardware based management functions.

**6. Chapter 6: Settings Migrator**

This chapter describes how to import configurations of your ACC CSM to ASUS Control Center Express, and also allow you to deploy ASUS Control Center Express agents to devices managed by ACC CSM.

**7. Chapter 7: Account & General Settings**

This chapter describes the User and ASUS Control Center Express settings.

## Conventions

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



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



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



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



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

## Typography

### **Bold text**

Indicates a menu or an item to select.

### *Italics*

Used to emphasize a word or a phrase.

### <Key>

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

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

### <Key1>+<Key2>+<Key3>

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

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

### Command

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

Example: At the 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 a quick overview of ASUS Control Center Express, and how to install and set it up.

# Getting Started

# 1.1 Setting up


## 1.1.1 Installing ASUS Control Center Express (ACCE)

1. Please visit the product website of your ASUS product to download the ASUS Control Center Express installer.
2. Launch the installer, then follow the steps to install ASUS Control Center Express to your system.



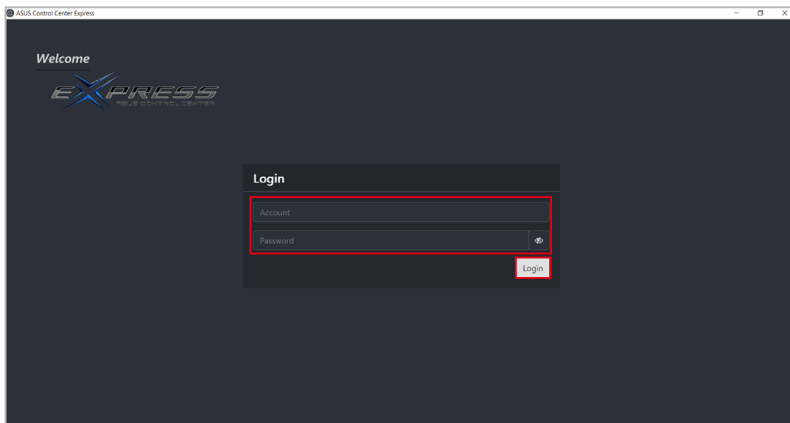
- If there is an older version of ASUS Control Center Express already installed on your system and you wish to clear the original configurations of the older version, you may check the **Clear original configuration** option during the installation process to remove the configuration settings of the older version of ASUS Control Center Express.
- We DO NOT recommend clearing the configuration settings of older versions of ASUS Control Center Express unless necessary.

## 1.1.2 Logging in to ASUS Control Center Express

1. Launch the ASUS Control Center Express by double clicking the **ASUS Control Center Express.exe** application .
2. Enter your **Account** and **Password**. Click **Login** to enter the ASUS Control Center Express main menu.



- The default account is **administrator**, and the default password is **admin**. Refer to the **Changing the account and password** section if you wish to change the default account and password.
- The account and password is case sensitive.




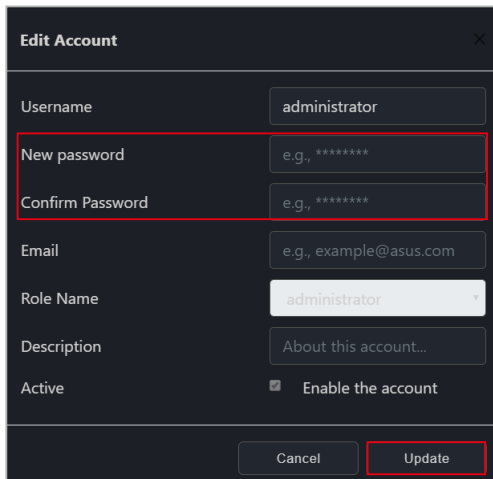
## 1.1.3 Changing the account password

1. Log in with the default account and password.



- The default account is **administrator**, and the default password is **admin**.
- The account and password is case sensitive.

2. Click on the  icon located at the top right menu bar, then click on **Settings**.
3. Click on the account to enter a new password, then click on **Update** to save the changes made.



The screenshot shows a dark-themed 'Edit Account' dialog box with a close button (X) in the top right corner. The form contains the following fields and options:


- Username:** administrator
- New password:** e.g., \*\*\*\*\*
- Confirm Password:** e.g., \*\*\*\*\*
- Email:** e.g., example@asus.com
- Role Name:** administrator
- Description:** About this account...
- Active:**  Enable the account

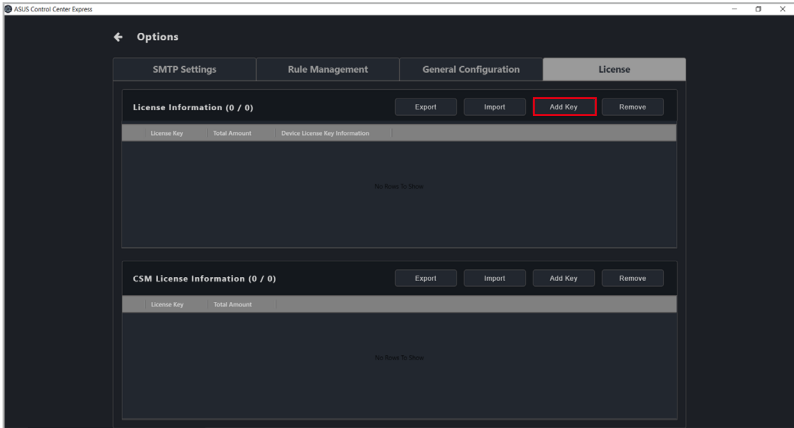
At the bottom of the dialog, there are two buttons: 'Cancel' and 'Update'. The 'Update' button is highlighted with a red border.

## 1.1.4 Activating your license key

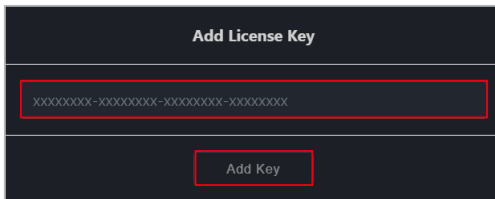


- Each client device you deploy an agent to will require a license key.
- For more details on License Keys please refer to **7.1.4 License Key**.


1. Locate the License Key on the ASUS Control Center Express card bundled in your motherboard's giftbox.
2. Click on the  icon, then select the **License** tab.
3. Click on **Add Key**.




4. Key in the license key and then click on **Add Key** to register a license for a single device on ASUS Control Center Express.



## 1.1.5 Changing languages

You may change the language of the ASUS Control Center Express to a preferred language by clicking on the  icon, then select a language from the drop down list.

# 1.2 Main dashboard overview

You can toggle between Classic and Graphic dashboard views by clicking on . A brief overview of both dashboards of ASUS Control Center Express is displayed as below:



The screenshots in this section are for reference only.

## Classic dashboard

**Annotations for Classic dashboard:**

- Banner logo
- System overview
- Metadata Management
- Management Control
- Switch View
- Deploy Management
- Options
- Language settings
- Account information
- Devices overview

Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization	Model Name	BIOS Version	BIOS Release Date	WatchDog
Offline	DESKTOP-86P7980	Windows	192.168.0.15	Normal	Normal	VCGS-C1	0807	06/12/2019	ENABLE
Offline	DESKTOP-727189M	Windows	192.168.0.16	Normal	Normal	VCGS-C1	0203	01/29/2018	N/A
Online	DESKTOP-VKZGDRP	Windows	192.168.0.10	Normal	Normal	Pro WG K07043C4	0803	08/01/2019	FAIL: Guard


## Graphic dashboard

**Annotations for Graphic dashboard:**

- System overview
- Edit
- Zoom in
- Zoom out
- Reset Zoom
- Client device shortcut icon
- Background area

## Menu items

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

Top menu bar items		Description
<b>System Overview</b>		Displays activity alerts and event logs to monitor server components in real time
<b>Switch View</b>		Toggle between the Classic dashboard and Graphics dashboard UI
<b>Management Control</b>		Provides functions which enable you to manage deployed devices, even when the client device is not in an OS environment. Out-of-band management is also featured if your motherboard supports a Remote Management Controller (RTL8117 LAN IC)
<b>Metadata Management</b>		Customize device metadata
<b>Deployment Management</b>		Remotely deploy agents, or install agents manually for effective monitoring
<b>Settings</b>	<b>SMTP Settings</b>	Configure SMTP Server settings to send notifications for server alert events
	<b>Rule Management</b>	Setting notification rules for the administrator
	<b>General Configuration</b>	Set the refreshment interval of main server and agent, as well as configure the banner logo
	<b>License</b>	Import or remove the product key(s) for ASUS Control Center Express
<b>Language</b>		Select the language for ASUS Control Center Express
<b>Account</b>	<b>Settings</b>	Manage and edit accounts, or create and edit permissions for roles
	<b>QR Code</b>	<div style="display: flex; align-items: center;">  <div> <p>Scan the QR code to access the web version of ASUS Control Center Express</p> <p>The device you use to scan the QR code should be in the same network as the ASUS Control Center Express server.</p> </div> </div>
	<b>Feedback</b>	Provide feedback to the developer team
	<b>Settings Migrator</b>	Import ACC CSM server settings and data and deploy ASUS Control Center Express agents to client devices managed by the ACC CSM server
	<b>Logout</b>	Log out of ASUS Control Center Express

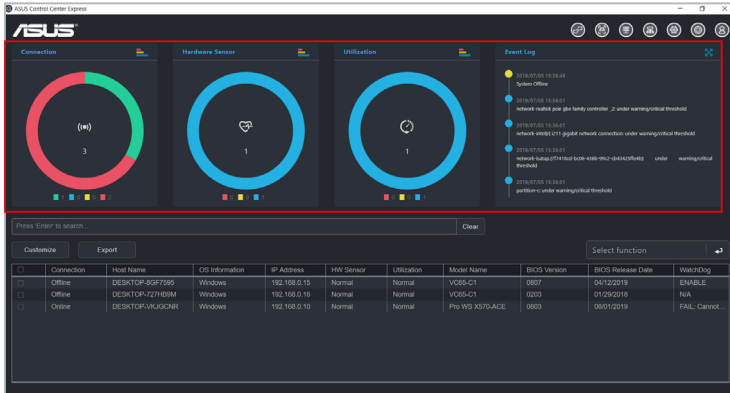
# Chapter 2

This chapter describes the functions available on the main dashboard.

# Dashboard Overview

## 2.1 System overview

The System Overview allows you to view activity alerts and event logs to monitor client devices in real time.



### Connection

This graph displays a summary of the connection status of all client devices.

Color	Status
Green	Online
Blue	Standby
	Maintain
Red	Offline

### Hardware Sensor

This graph displays a summary of the hardware status of all client devices.

Color	Status
Red	Critical
Orange	Warning
Blue	Normal

### Utilization

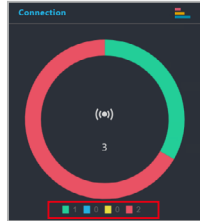
This graph displays a summary of the utilization status of all client devices.

Color	Status
Red	Critical
Orange	Warning
Blue	Normal

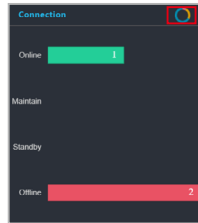
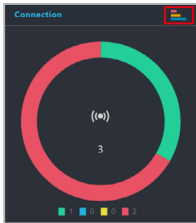


## 2.1.1 Switching sensor views

You can customize the information shown on the **Connection**, **Hardware Sensor**, and **Utilization** graphs by clicking on the graph keys to display or hide a specific group.



You can also click on the top right corner of each graph to switch between pie graph and bar graph views.



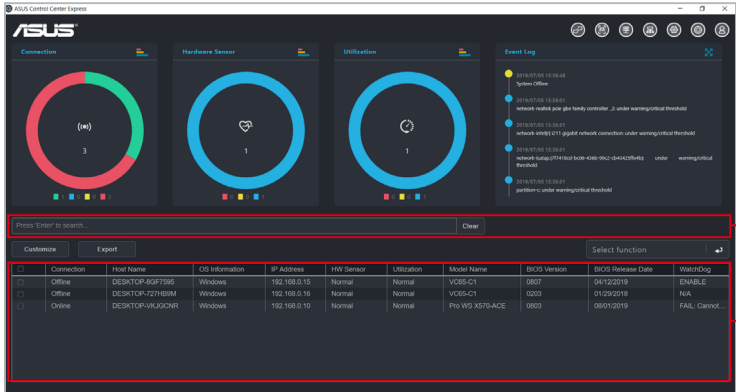
## 2.1.2 Event Log

The Event Log displays the status of all client devices in real time, allowing you to keep track of the status changes of your client devices at a quick glance. You can also click on the top right corner of the Event Log block to expand the Event Log to view a detailed list of the event items.

IP	Date & Time	Level Type	Message	Owner
	2019/07/05 15:3040	warning	System Offline	
	2019/07/05 15:3051	normal	system memory under warning!...	
	2019/07/05 15:3051	normal	performance under warning!...	
	2019/07/05 15:3051	normal	network usage (11717) is too high...	
	2019/07/05 15:3051	normal	network usage (11717) is too high...	
	2019/07/05 15:3051	normal	network usage (11717) is too high...	
	2019/07/05 15:3051	normal	System Online	
	2019/07/05 15:3054	warning	System Offline	
	2019/07/05 15:3055	normal	System Online	

## 2.2 Device overview

The Device overview lists all your client devices and also allows you to search for client devices using keywords, export the list of client devices, or perform actions on selected client devices using the function shortcut.



The screenshot shows the ASUS X300 Control Center Express dashboard. It features three circular gauges for Connection (3), Hardware Sensor (1), and Utilization (1). Below these is a search bar with a 'Clear' button. A table lists client devices with columns for Connection, Host Name, OS Information, IP Address, HW Sensor, Utilization, Model Name, BIOS Version, BIOS Release Date, and Win10Log. The table contains three rows of device data. A 'Search bar' label points to the search input, and a 'Devices list' label points to the table.

	Connection	Host Name	OS Information	IP Address	HW Sensor	Utilization	Model Name	BIOS Version	BIOS Release Date	Win10Log
1	Offline	DESKTOP-80F7896	Windows	192.168.0.16	Normal	Normal	V056-C1	0203	01/29/2018	ENABLE
2	Offline	DESKTOP-727480M	Windows	192.168.0.16	Normal	Normal	V056-C1	0203	01/29/2018	N/A
3	Online	DESKTOP-VUJCCNR	Windows	192.168.0.10	Normal	Normal	Pro WS X370ACE	0203	06/01/2019	FAIL_Cannot...

### 2.2.1 Filtering client devices




To clear the filter and view all devices, click on **Clear** in the Search bar.

- **To filter the devices using the Search bar:**

Enter a keyword into the Search bar then press <Enter> to search for devices with details matching the search criteria.

- **To filter the devices using Devices list:**

1. Hover over the column you wish to use as your filter criteria in the Devices list.
2. Click on , then select the filter rule and enter the keyword to search.



- To view more column items in the Devices list, click on **Customize**, then check the metadata item you wish to display and click on **Save**.
- Click on the name of a column header to sort the filter results alphabetically, in ascending or descending order.

### 2.2.2 Export device list

You can export the device list to a .csv file for when you need to backup the devices list.

To Export the device list, click on **Export**, then enter your file name and click **Save** to save the device list as a .csv file.


## 2.2.3 Using shortcut functions

You can perform certain actions or schedule tasks for the client devices.

1. Select the device(s) you would like to perform an action on.
2. Click on **Select function**, and select the function you would like to use. Please refer to the table below for a brief summary of each function.



- For more details on the following functions listed below, please refer to
  - USB Redirection: **4.9 USB Redirection**
  - 8117-Set password: **5.1.3 Setting the password for RTL8117**
  - Firmware Update: **5.10 Firmware Update**
  - Task Scheduler: **2.4 Task Scheduler**
  - Software Management: **5.10 Software Management**
  - Smart BIOS: **4.10 BIOS**
- **8117-Control** functions are only available on client devices connected using a management LAN port which supports RTL 8117 LAN IC.
- Some functions may require you to restart the client device for the changes to take effect.

<b>Remote Control</b>	<b>Restart Computer</b>	Restart the selected device(s)
	<b>Power Off</b>	Power off the selected device(s)
	<b>Power On</b>	Power on the selected device(s)
<b>8117-Control</b>	<b>8117-Restart Computer</b>	Restart the selected device(s)
	<b>8117-Force Power OFF</b>	Force a 4 second power off of the selected device(s)
	<b>8117-Power OFF</b>	Power off the selected device(s)
	<b>8117-Power ON</b>	Power on the selected device(s)
	<b>8117-WatchDog Enable</b>	Enable WatchDog for selected device(s)
	<b>8117-WatchDog Disable</b>	Disable WatchDog for selected device(s)
	<b>8117-Clear CMOS</b>	Clear CMOS for selected device(s)
	<b>USB Redirection</b>	Allow access of a USB device from within a remote desktop or application
	<b>8117-Set password</b>	Set an encryption password for RTL8117
	<b>Restart Service</b>	Restart the RTL8117 service on selected device(s)
	<b>8117-KVM Enable</b>	Enable KVM for selected device(s)
	<b>8117-KVM Disable</b>	Disable KVM for selected device(s)
	<b>Firmware Update</b>	Update the RTL8117 firmware
	 <p>Firmware Update will be disabled if 8117-KVM is Enabled.</p>	


(continued on the next page)

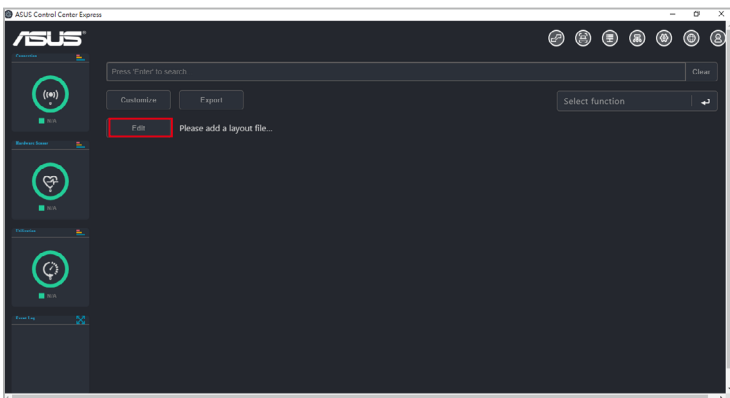
<b>Security</b>	<b>Enable Regedit</b>	Enable Windows Registry Editor
	<b>Disable Regedit</b>	Disable Windows Registry Editor
	<b>Enable USB</b>	Enable the USB ports on the device(s)
	<b>Disable USB</b>	Disable the USB ports on the device(s)
	<b>USB Read Only</b>	Set the USB ports to Read Only privileges
<b>Task Scheduler</b>		Schedule tasks for the device(s)
<b>Software Management</b>	<b>Software Dispatch</b>	Dispatch software and scripts to the selected device(s)
	<b>Software Information</b>	View or configure applications, processes or services on the selected device(s)
	<b>Software Blacklist</b>	View or add blacklisted software
<b>Smart BIOS</b>		Flash the BIOS of the selected device(s)

## 2.3 Customizing your dashboard

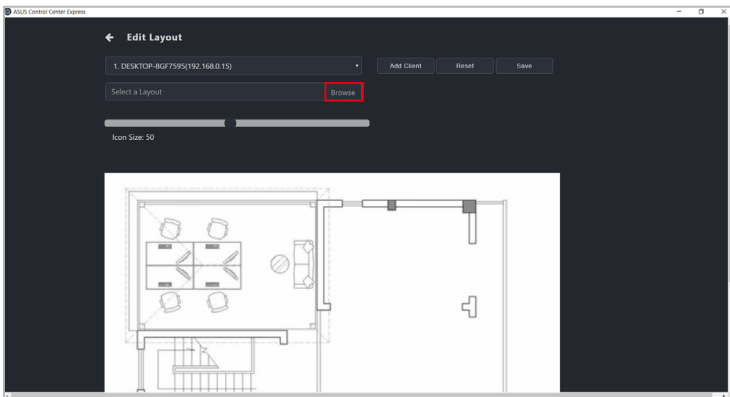
You can toggle between the Classic dashboard view or Graphic dashboard view. The Graphic dashboard view allows you to upload a layout image (such as the office floor) and place shortcut icons of client devices onto their respective places on the layout.

### 2.3.1 Customizing the Graphic dashboard view for the first time

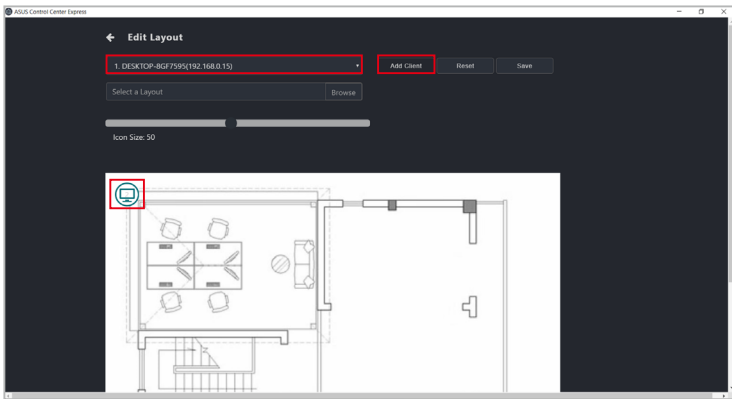
1. Click on  to toggle to the Graphic dashboard view.
2. Click on **Edit** to add a layout file.



3. Click on **Browse** to select and upload an image file you would like to use as the layout image.



4. Select which client device you would like to add as a shortcut icon by selecting the device from the drop down list, then clicking on **Add Client**. The shortcut icon should appear in the background area.

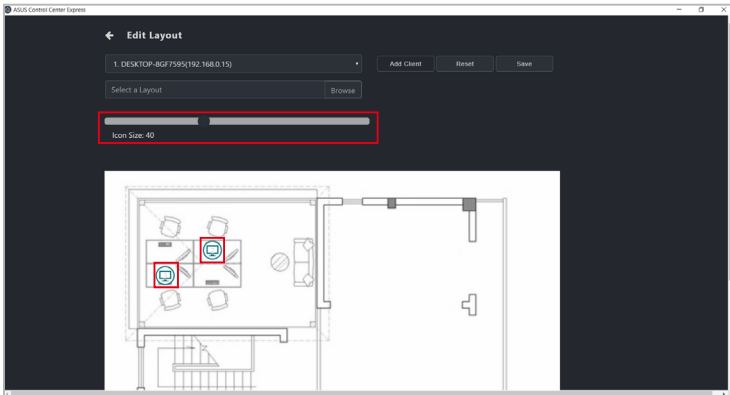


5. Repeat step 4 to add multiple client device shortcut icons.




To remove all shortcut icons click on **Reset**.

6. You may adjust the positions of the shortcut icons by clicking and dragging the shortcut icon to your preferred location, or adjust the size of the shortcut icons using the **Icon Size** scroll bar.



7. Click on **Save** once you have finished customizing, you will be directed back to the Graphic dashboard view.

## 2.3.2 Editing the shortcut icons and background

Click on  to edit the shortcut icons and background, please refer to steps 3 to 7 of the **Customizing the Graphic dashboard view for the first time** section to edit the background and shortcut icons.

## 2.3.3 Using the shortcut icons

- **Hover over shortcut icon:**  
Hover over a shortcut icon to view the details of the client. You may customize the information shown by clicking on **Customize** and checking or unchecking the metadata item you wish to display or hide, then click on **Save**.
- **Single click on shortcut icon:**  
A single click on the shortcut icon will select the icon, for when you wish to use a function on a client device or multiple devices.



---

For more details on the functions, please refer to **Chapter 4 Device Information** and **Chapter 5 Management Functions**.

---

- **Double click on shortcut icon:**  
Double clicking on a shortcut icon will redirect you to the Device information screen.



---

For more information on the Device Information screen please refer to **Chapter 4 Device Information**.

---

- **Shortcut icon status:**  
The shortcut icon will change or change colors depending on the status



: Offline



: Online



: Device online, hardware sensor and utilization status in normal state



: Device online, hardware sensor and utilization status in warning state



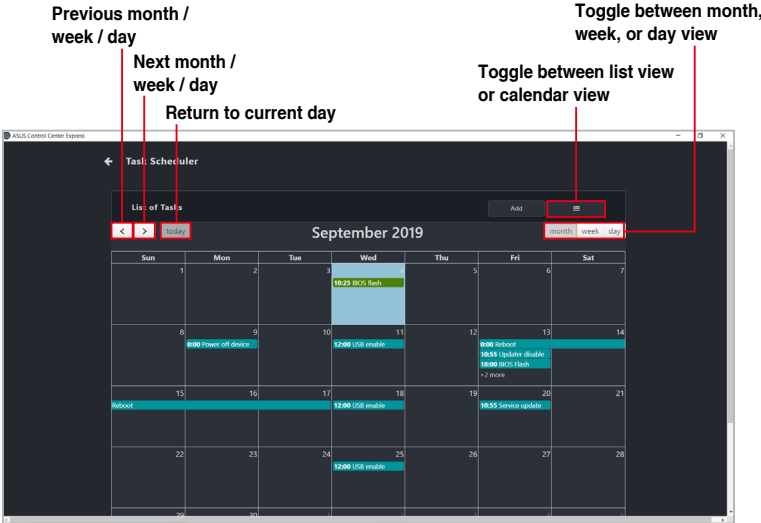
: Device online, hardware sensor and utilization status in critical state

# 2.4 Task Scheduler

You can set scheduled tasks for client devices to perform on set dates, or manage already schedule

## 2.4.1 Task scheduler calendar overview

You can view the tasks already set on the task scheduler calendar.

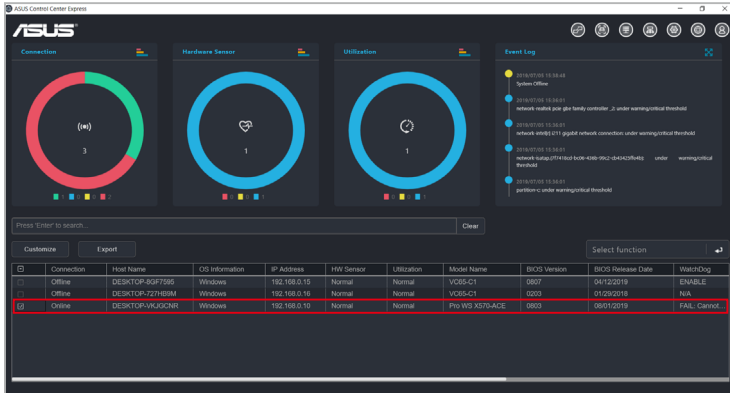




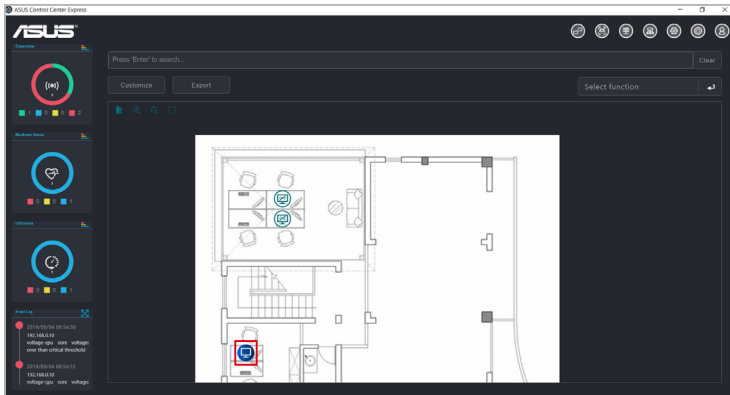
## 2.4.2 Setting a new task

1. Select the devices you would like to set a new scheduled task for.

### Classic dashboard

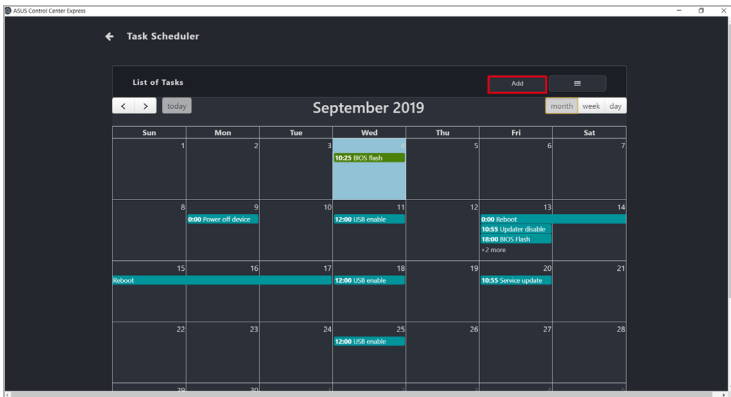


### Graphic dashboard



2. Click on **Select function**, then select **Task Scheduler** from the drop down menu.

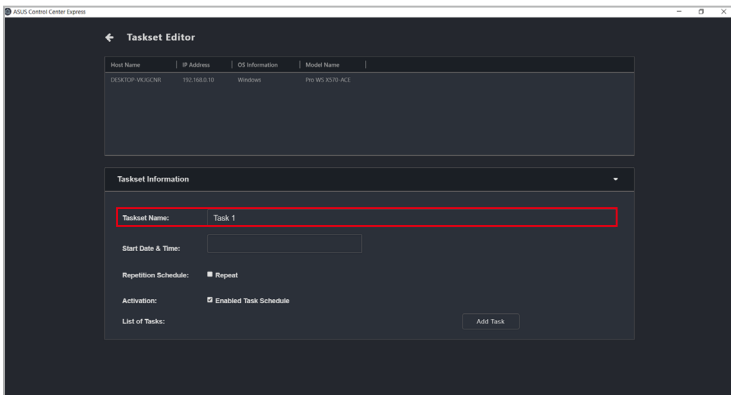
3. Click on **Add**.



4. Enter the Taskset name.



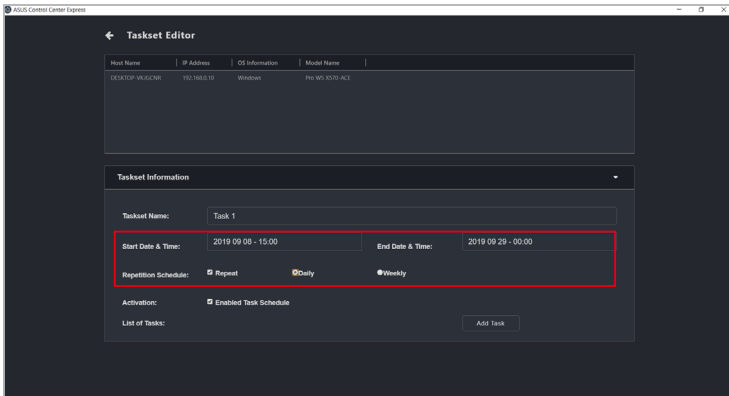
The Taskset name cannot be changed after you have created the task.



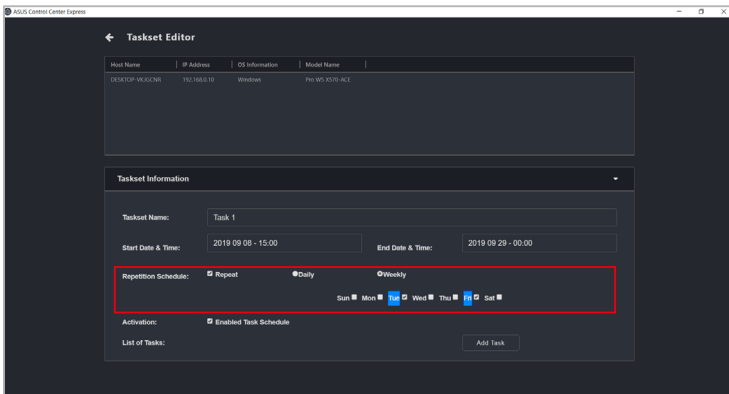
5. Select a **Start Date & Time**. If you want the task to repeat for a set period of time, check **Repeat**, then select the **End Date & Time**.



The **End Date & Time** field will only appear when you check **Repeat**.



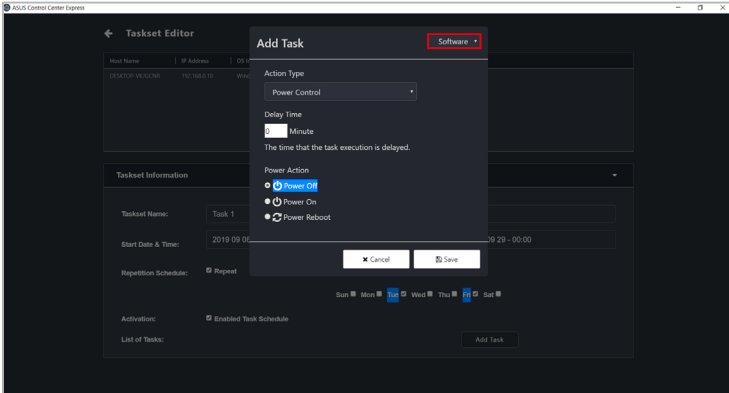
6. (optional) If you checked **Repeat** in the previous step, select if you want the task to repeat **Daily** or **Weekly**. Selecting **Weekly** will allow you to choose the day you wish to repeat the task each week.



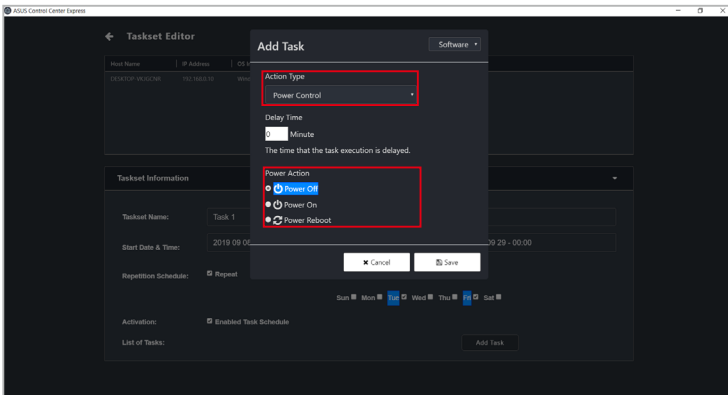
7. Click on **Add Task** and select **Software** for software based functions or **Hardware** for management functions.



**Hardware** functions are only available on client devices connected using a management LAN port which supports RTL 8117 LAN IC.



8. Select an **Action Type** from the drop down menu. You may refer to the table on the next page for a brief overview of the **Action Type** options.

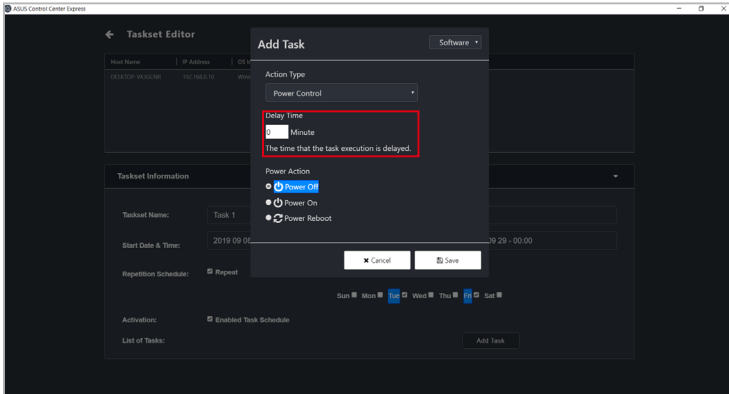


Action Category	Action type	Action options	Description	
Software	Power Control	Power Off	Power off device	
		Power On	Power on device	
		Power Reboot	Restart device	
	Service Control	Service Name	Enter the name of the service	
		Start	Start the service	
		Stop	Stop the service	
		Restart	Restart the service	
	Software Dispatch	Package Name	Select a software package from the Software Pool	
	Security Control	Registry Tool	Enable	Enable Windows Registry Editor
			Disable	Disable Windows Registry Editor
USB Control		Enable	Enable the USB ports	
		Disable	Disable the USB ports	
	Read Only	Set the USB to Read Only privileges		
BIOS Cache	BIOS Cache List	Select a BIOS file from the BIOS cache list		
Hardware	Power Control	Power Off	Power off device	
		Force Power Off	Force power off device	
		Power On	Power on device	
		Power Reboot	Restart device	
	Enable / Disable WatchDog	Heartbeat Interval	Set the heartbeat interval	
		Enable	Enable Watchdog	
		Disable	Disable Watchdog	
	Clear CMOS	-	Clear the CMOS of device	
Enable / Disable KVM	Enable	Enable KVM		
	Disable	Disable KVM		

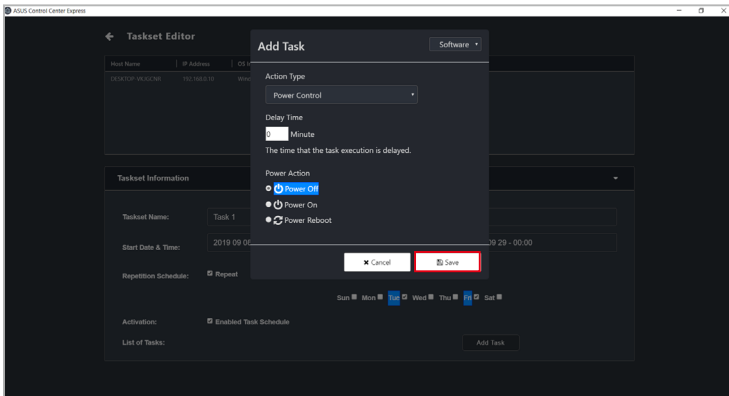
9. Enter the **Delay Time** (in minutes). The delay time determines the amount of time this task should wait before executing this task once the previous task has finished.



When scheduling multiple tasks, ensure that each task has a delay time set to ensure the tasks are executed properly.



10. Click on **Save** to save this task

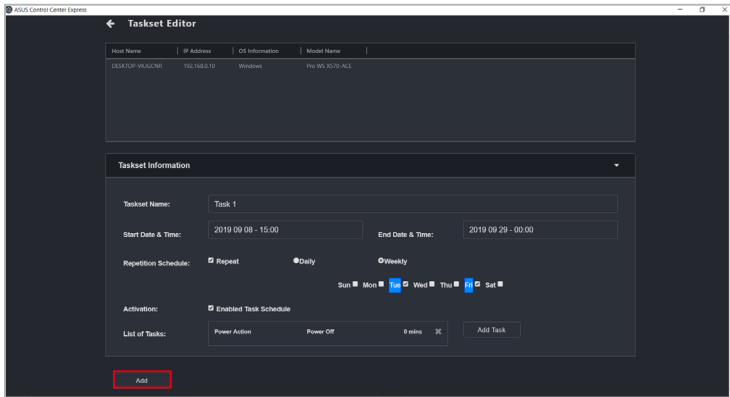


11. Repeat steps 7 to 10 to add more tasks, the tasks added will appear in the **List of Tasks**.



To delete a task, click on the **X** next to the task in the **List of Tasks**.

- Once you have finished, click on **Add** to add the new scheduled task to the task scheduler calendar.



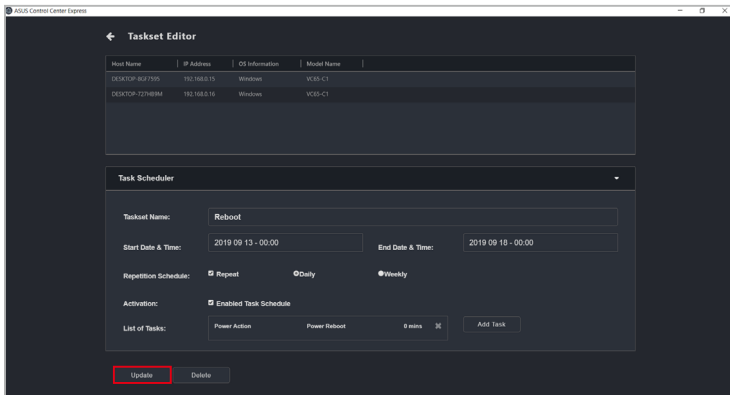
### 2.4.3 Editing a task

- Click on the scheduled task you would like to edit on the task scheduler calendar.
- You can edit the **Start Date & Time, End Date & Time, Repetition Schedule, Activation, and List of tasks.**



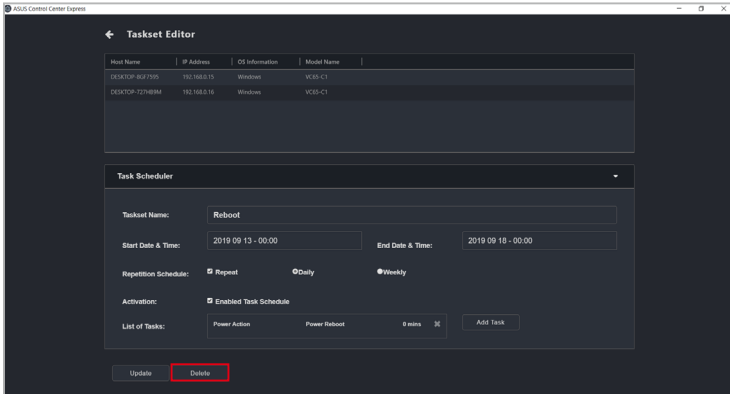
To delete a task, click on the **X** next to the task in the **List of Tasks**.

- Once you have finished editing the scheduled task, click on **Update**.



## 2.4.4 Deleting a task

1. Click on the scheduled task you would like to delete on the task scheduler calendar.
2. Click on **Delete** to delete the scheduled task.






# Chapter 3

This chapter describes how to deploy ASUS Control Center agents and remove agents through Microsoft® Active Directory or manually.

# Deploy Management

## 3.1 Deploying agents

Install new agents on devices and add them to the ASUS Control Center Express server for convenient management, monitor and control.

To access **Agent Management**, click on  located at the top right menu bar.



Ensure to register the License keys before deploying agents to client devices. For more information on registering license keys, please refer to **7.1.4 License Key**.



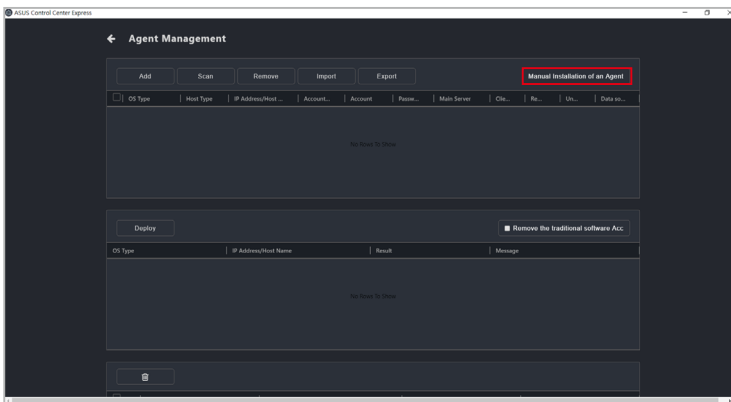
The screenshots in this section are for reference only.

### 3.1.1 Client requirements

<b>Supported client OS</b>	Windows® 10 PRO or later version
<b>Account settings</b>	Administrator account and password enabled

### 3.1.2 Installing Agents manually

1. Click on **Manual Installation of an Agent** to start downloading the installation files (Setup.msi).



2. Copy and paste **Setup.msi** to the client you wish to install the agent on using an external storage device such as a USB flash drive.

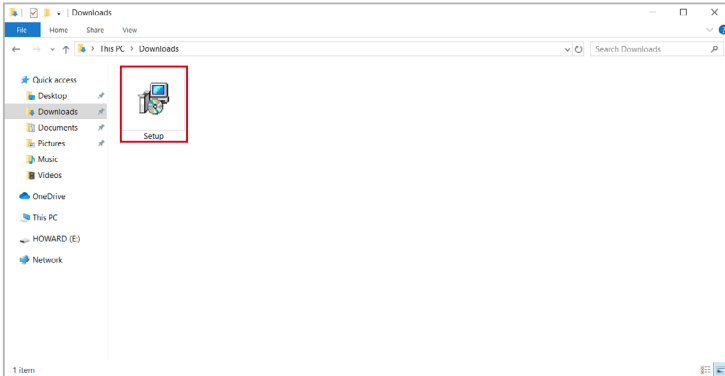
3. On the client device, double click on the **Setup.msi** file to launch the installation.



---

ASUS Control Center Express only supports Windows® 10 PRO or later versions.

---



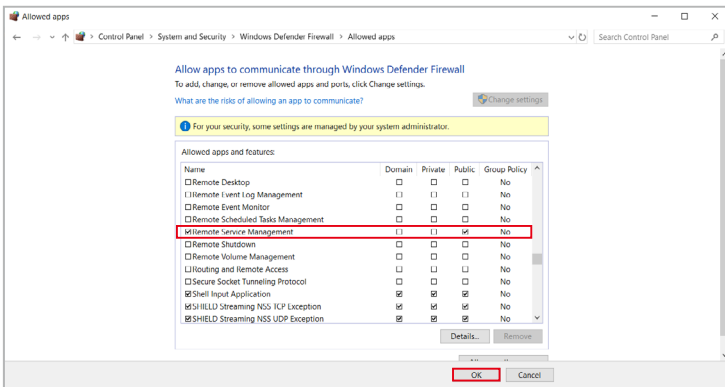
4. Follow the instructions of the installation wizard to install the ASUS Control Center Express agent to the client device.

### 3.1.3 Deploying agents through ACC Express

1. Ensure to disable the firewall on the client device.

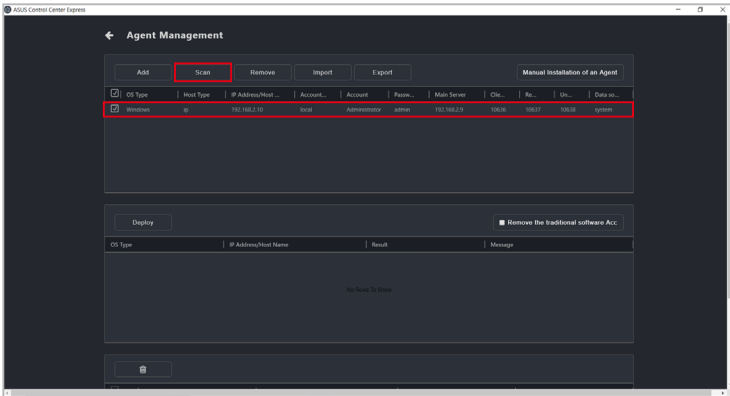


- Ensure the client has sufficient power and a steady connection to prevent packet loss when deploying the agent.
- Ensure the client and ACCE server are in the same network domain.
- ASUS Control Center Express only supports Windows® 10 PRO or later versions.
- To disable the firewall on the client device, please navigate to **Control Panel > System and Security**, then click on **Allow an app through Windows Defender Firewall** under the **Windows Defender Firewall** section. Check the **Remote Service Management** option, then click on **OK**.

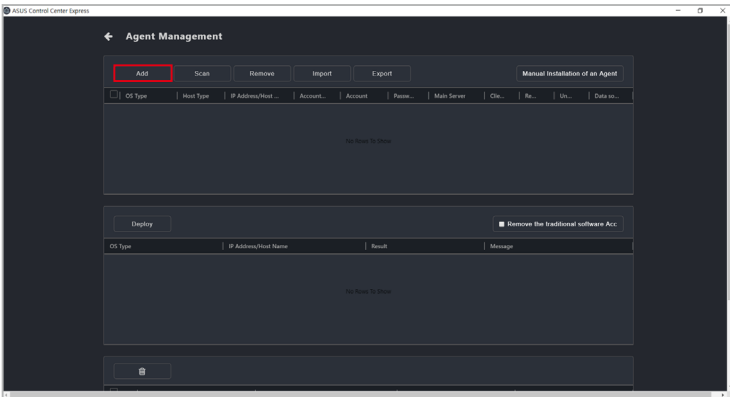


2. You may use the following three methods to scan for or add available client devices:

- **To automatically scan for client devices:**
  - a. Click on **Scan** to start scanning for available client devices. The devices should appear in the scan results block shown below.



- **To manually add a client device to scan results:**
  - a. Click on **Add**.

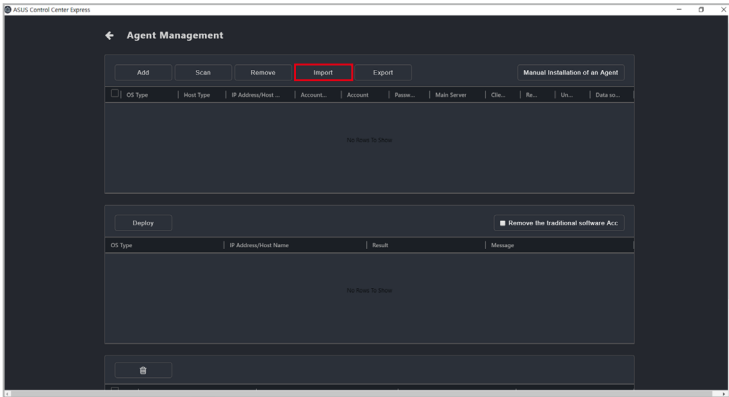


- b. Enter the information of the device you wish to add, then click on **Save**.

<b>Main Server</b>	Enter the IP of the ASUS Control Center Express server
<b>OS Type</b>	Select the OS type of the client
<b>Host Type</b>	Select <b>IP Address</b> to enter the IP address of the client or Select <b>Host name</b> to enter the name of the client
<b>Host Port</b>	Enter the port
<b>Account Type</b>	Select whether the client account is local or domain <b>Local:</b> The agent's administrator privileges only allow you to manage the device the agent is installed on <b>Domain:</b> The agent's administrator privileges allow you to manage all devices in the domain
<b>Domain*</b>	Enter the domain name
<b>Account</b>	Enter the administrator account name of the client
<b>Password</b>	Enter the password for the administrator account of the client
<b>Remote</b>	Enter the port to use when remotely accessing this client
<b>Undeploy</b>	Enter the port to use when removing the agent from this client

\* This field only appears if you selected Domain as the account type.

- **To manually import multiple client devices to scan results:**
  - a. Click on **Import**.



- b. Select the .csv file you would like to import, then click **Open**. The devices listed in the .csv file should appear in the scan results block.



---

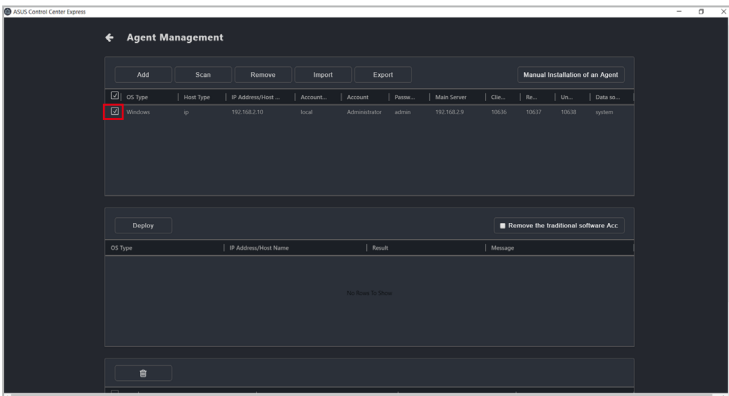
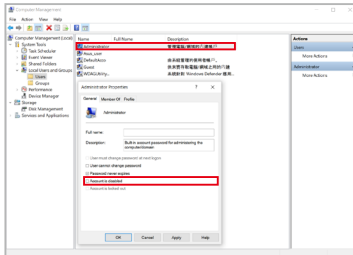
Ensure to use a .csv file you have previously exported by clicking **Export** to ensure you use the correct .csv template. Using a .csv file with the incorrect fields may result in failure when importing the .csv file.

---

### 3. Check the client devices you wish to add agents to.

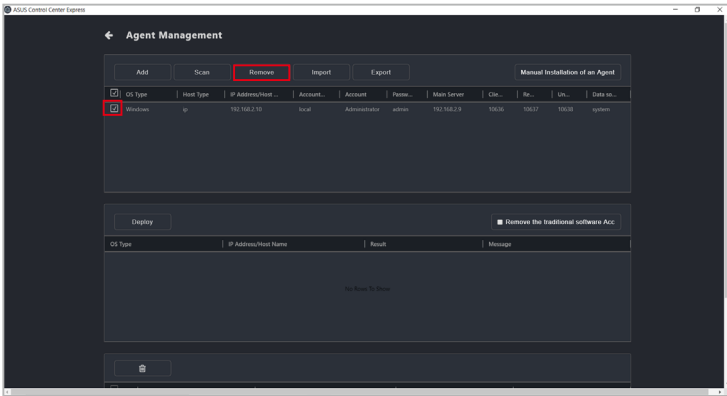


- Ensure to enter an account with administrator privileges and has the password enabled on the client device into the **Account** and **Password** cells. You can edit the **Account** and **Password** fields by double clicking on the device in the scan results.
- Ensure the Administrator account of the client is enabled and has a password set. (Windows disables the Administrator account by default, to enable the account click on the Windows button from the Desktop > **Windows Administrative Tools > Computer Management > System Tools > Local Users and Groups > User > Administrator**, then uncheck the **Account is disabled** field)

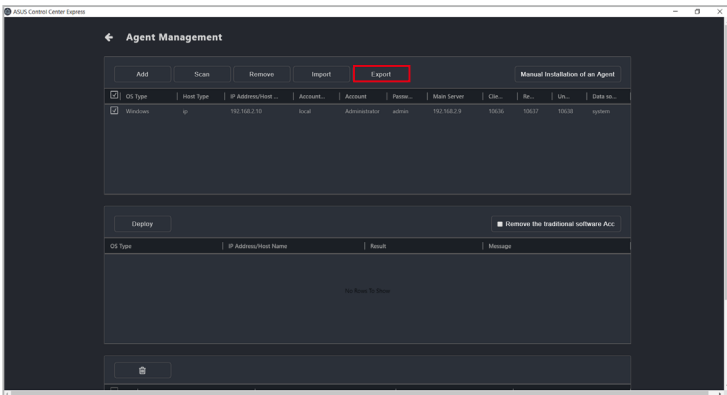




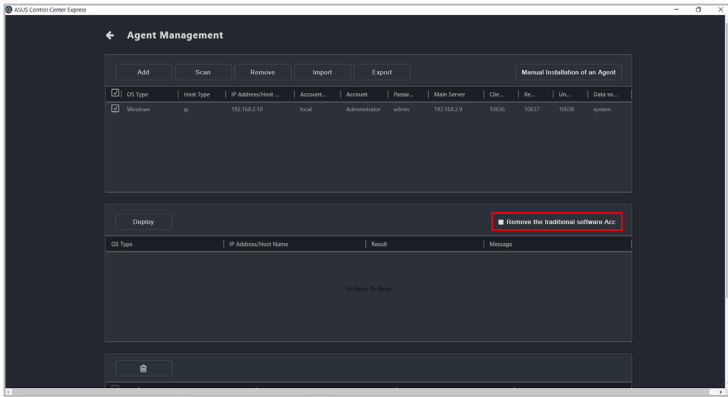
- (optional) If there are devices in the scan results you do not wish to deploy agents to, check the devices then click on **Remove**.



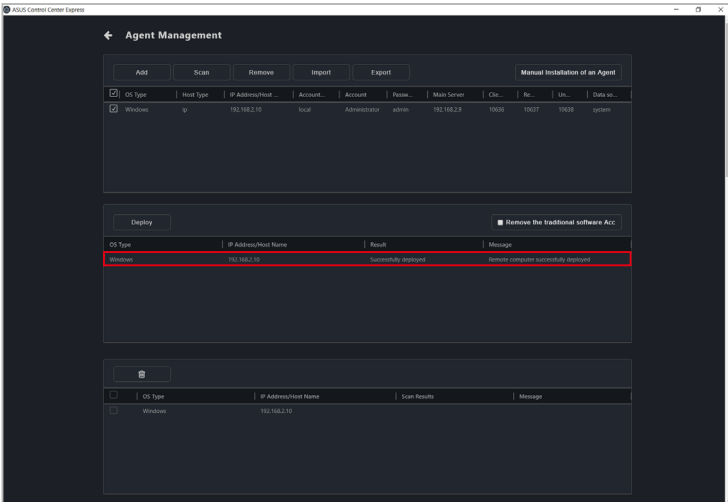
- (optional) You may click on **Export** to export the scan results to a .csv file for future use.



- (optional) Check the **Remove the traditional software Acc** box to remove any previous versions of ASUS Control Center agents installed on the selected client devices when deploying new agents.



- Click on **Deploy** and wait for the agent deployment to be completed. Once the process is completed, you may view the deploy status in the deploy list.



## 3.2 Removing agents

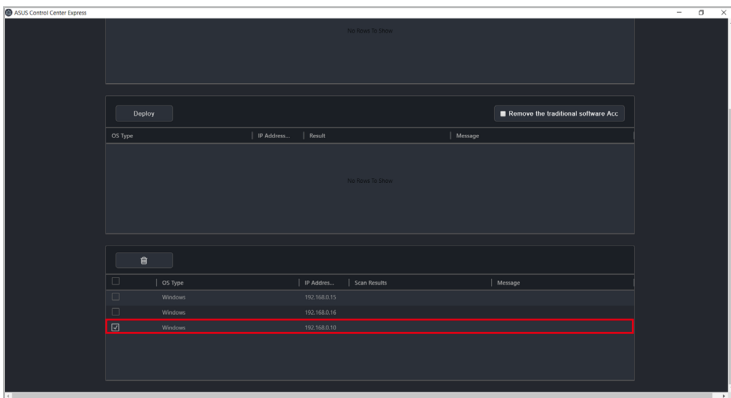



If a client device with an agent already deployed to it has been in for repairs or maintenance, please remove the agent on the client device, then re-deploy an agent to the device. To deploy an agent to a device please refer to **3.1 Deploying agents**.

1. Check the client devices you wish to remove agents from in the deployed block.



The deployed block is located at the bottom of the **Agent Management** or **Settings Migrator** screen.



2. Click on , then click **OK** to remove agents on all selected devices.



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



# Chapter 4

This chapter describes the device information and software controlled options for managing the device.

# Device Information

## 4.1 Device Information Overview

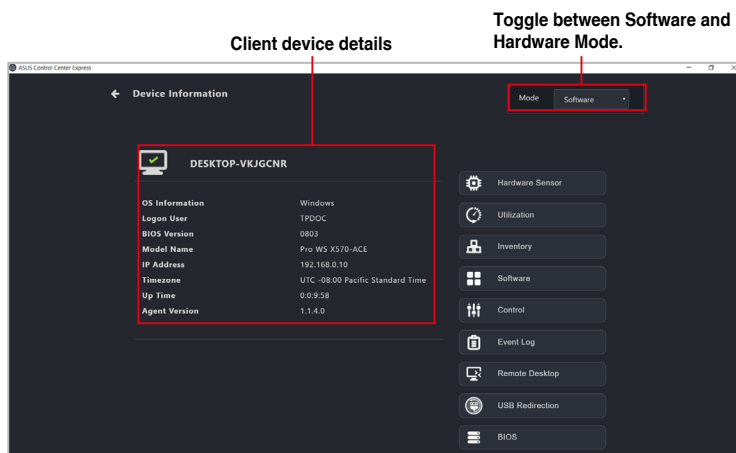
The **Device Information Overview** provides you with detailed information about your selected client device, and also provides you with some software controlled management functions such as power control options.

To access **Device Information** of a client device from the different dashboard views, please refer to the following:

- Classic dashboard view: Click on a client device in the device list.
- Graphic dashboard view: Double click on a client device shortcut icon.



- 
- This chapter is only for the **Software Mode** options, for Hardware Mode options, please refer to **Chapter 5 Management Functions**. **Hardware Mode** (out-of-band management) options are available for client devices connected using a management LAN port which supports RTL 8117 LAN IC.
  - Most options are only available when the client device is online and logged into the OS.
  - Some options are only available when the following requirements are met:
    - Client device is online and logged into the OS
    - Has already had an agent deployed to it
    - Connected using a management LAN port which supports RTL 8117 LAN IC
  - The screenshots in this section are for reference only.
-



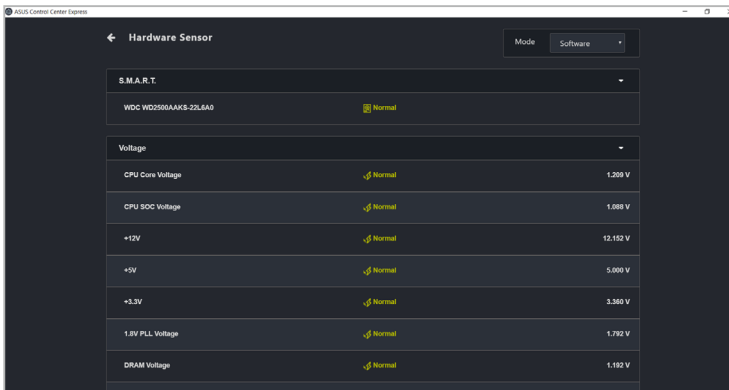
<b>Device Name</b>	Displays the device name.
<b>OS Information</b>	Displays information on the Operating System.
<b>Logon user</b>	Displays the user logged into client device.
<b>BIOS Version</b>	Displays information on the BIOS version.
<b>Model Name</b>	Displays the model name of client device.
<b>IP Address</b>	Displays the IP address of client device.
<b>Time Zone</b>	Displays the time zone client device is located in.
<b>Up Time</b>	Displays the up time of client device.
<b>Agent Version</b>	Displays information on the Agent version.

## 4.2 Hardware Sensor (software)

This item allows you to view S.M.A.R.T attributes or edit the threshold value for items such as voltage, temperature, fans, and graphics card. This item is software controlled and values may differ with the hardware version. Please refer to **5.3 Hardware sensor (hardware)** for more information on **Hardware mode**.



- Some options such as Graphics card may only be available if you have the component installed on your client device.
- This item will not be available if your device is not logged into an OS environment, or is not connected using a management LAN port which supports RTL 8117 LAN IC.



<b>S.M.A.R.T.</b>	Displays disk status, click on this item to show detailed S.M.A.R.T. attribute information.
<b>Voltage</b>	Displays the CPU Core Voltage, and other voltage related items. You may edit the threshold for these items.
<b>Temperature</b>	Displays the CPU status and temperature. You may edit the threshold for these items.
<b>Fans</b>	Displays the status and fan speed of connected fans. You may edit the threshold for these items.
<b>Graphics Card</b>	Displays the fan speed, voltage and temperature of external AMD or NVIDIA graphics card. You may edit the threshold for these items.



## 4.2.1 Editing the threshold value

Some items such as Voltage items, or Fan items allow you to edit the threshold values. Click on the item you wish to edit, then click on **Save** once you are finished editing.



- The threshold options for each item may vary.
- Some items may not have a threshold value you can edit.

CPU Fan

High threshold 7200

Low threshold 200

Monitor Enable ▾

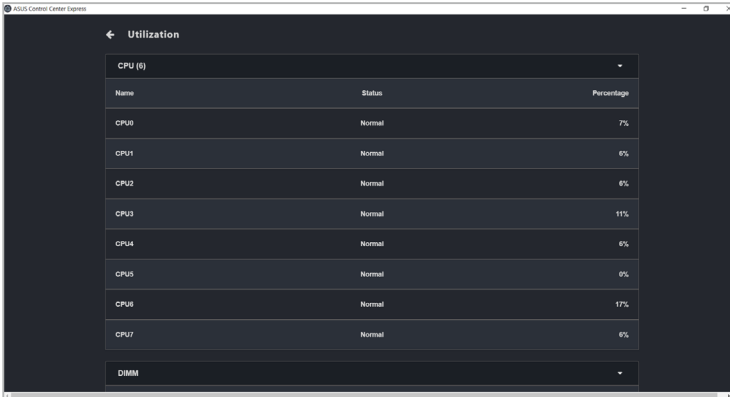
Check zero value Enable ▾

Save Cancel

<b>High threshold</b>	When the value exceeds this threshold value, the sensor will display <b>Warning (Yellow)</b> . When the value exceeds this threshold value by 20%, the sensor will display <b>Critical (Red)</b> .
<b>Low threshold</b>	When the value is below this threshold value, the sensor will display <b>Warning (Yellow)</b> . When the value is below this threshold value by 20%, the sensor will display <b>Critical (Red)</b> .
<b>Monitor</b>	Enable or disable monitoring of this item.
<b>Check zero value</b>	Enable or disable the check for zero value. When <b>enabled</b> , a warning will display if the fan speed for a fan is 0. When <b>disabled</b> , if the fan speed for a fan is 0, it will be recognized as a removed fan (not connected).

## 4.3 Utilitization

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



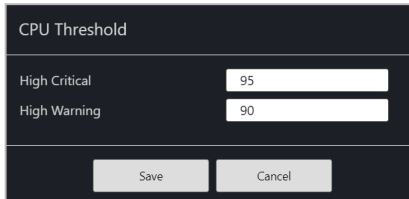
The screenshot shows the 'Utilization' screen in the BIOS. It features a dropdown menu for 'CPU (8)' and a table with columns for 'Name', 'Status', and 'Percentage'. Below the table is a 'DIMM' dropdown menu.

Name	Status	Percentage
CPU0	Normal	7%
CPU1	Normal	6%
CPU2	Normal	6%
CPU3	Normal	11%
CPU4	Normal	6%
CPU5	Normal	0%
CPU6	Normal	17%
CPU7	Normal	6%

<b>CPU</b>	Displays CPU utilization status and usage percentile. You may edit the threshold for these items.
<b>DIMM</b>	Displays memory utilization status and usage percentile. You may edit the threshold for these items.
<b>Partition</b>	Displays disk partition utilization status and usage percentile. You may edit the threshold for these items.
<b>Network</b>	Displays disk network utilization status and usage percentile. You may edit the threshold for these items.

### 4.3.1 Editing the threshold value

Click on the item you wish to edit, then click on **Save** once you are finished editing.



The 'CPU Threshold' dialog box has two input fields: 'High Critical' with the value '95' and 'High Warning' with the value '90'. At the bottom are 'Save' and 'Cancel' buttons.

<b>High Critical</b>	When the value exceeds this threshold value, the sensor will display <b>Critical (Red)</b> .
<b>High Warning</b>	When the value exceeds this threshold value, the sensor will display <b>Warning (Yellow)</b> .

## 4.4 Inventory (Software)

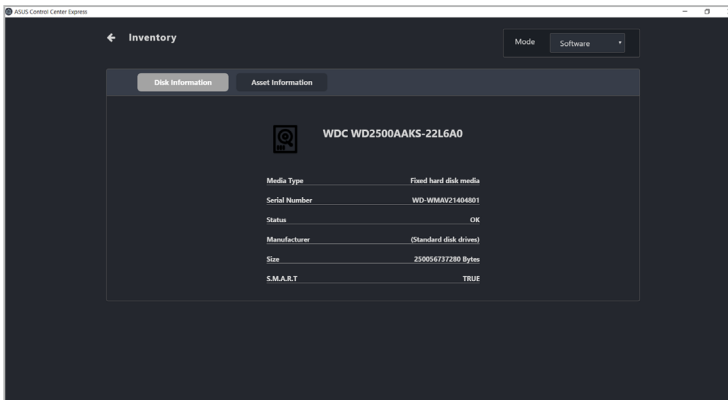


This item will not be available if your device is not logged into an OS environment, or is not connected using a management LAN port which supports RTL 8117 LAN IC.

This item displays more details about the client device and disk. This item is software controlled and values may differ with the hardware version. Please refer to **5.4 Inventory (hardware)** for more information on **Hardware** mode.

### 4.4.1 Disk Information

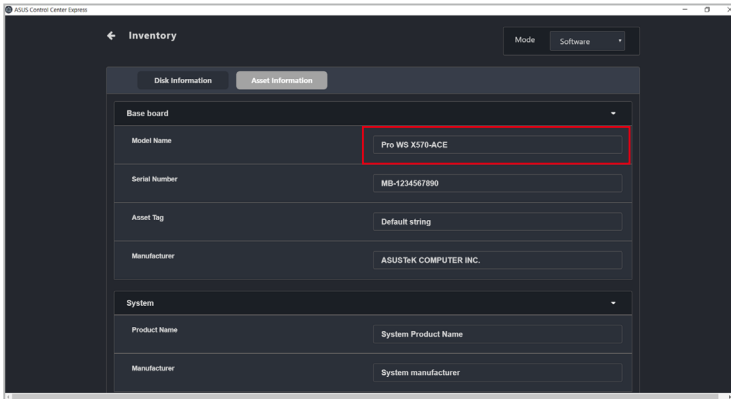
Click on **Disk Information** for more details on the disk.



<b>Disk Name</b>	Displays the disk name.
<b>Media Type</b>	Displays the media type.
<b>Serial Number</b>	Displays the serial number for the disk.
<b>Status</b>	Displays the status of the disk.
<b>Manufacture</b>	Displays the name of the manufacturer of the disk.
<b>Size</b>	Displays the total size of the disk.
<b>S.M.A.R.T.</b>	Displays the S.M.A.R.T. attribute status of the disk.

## 4.4.1 Disk Information

Click on **Asset Information** for more details on the client device. You may also edit items with a gray border.



<b>Baseboard</b>	Displays the model name, serial number, asset tag and manufacturer information on the base motherboard. You may edit these items.
<b>System</b>	Displays the name and manufacturer of the system. You may edit these items.
<b>Memory</b>	Displays the location and size of the memory.
<b>BIOS</b>	Displays the release date, version, and manufacturer information of the BIOS.
<b>Processor</b>	Displays the name, and clock of the processor.
<b>Network Adapter</b>	Displays the name, MAC address, connection status, and adapter type information on the network adapter.
<b>Graphic Card</b>	Displays the name and driver version of the graphic card.
<b>OEM String</b>	Displays the device's SMBIOS TYPE information. You may edit these items.

## 4.5 Software

This item displays details on the software and applications with the **Application**, **Processes**, **Services**, and **Environment** tab.



Some operating system applications, processes, and services cannot be removed, terminated, or stopped.

### 4.5.1 Application tab

The **Application** tab allows you to view information on installed applications on the client device. You may also click on an application then select **Uninstall** to uninstall the application.

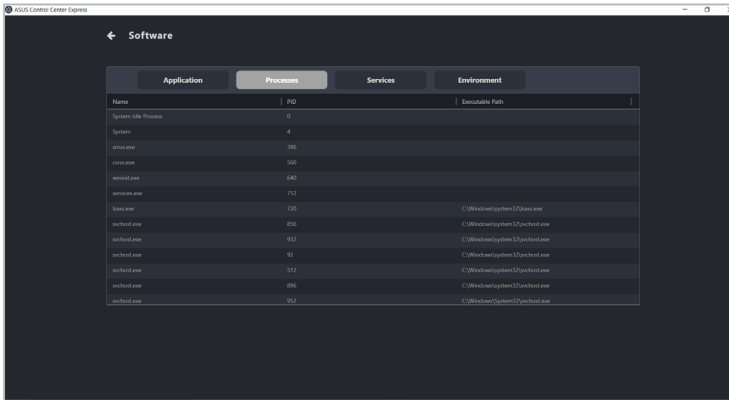


The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.

Name	Version	Publisher	Installation Date
MSVC_Build_Compiler	17.046117	Microsoft Build Tools	20190520
Microsoft .NET Core	16.1.21.024.0005	Microsoft Corporation	20190520
Microsoft Visual C++ 2015 Redistributable (x...	14.0.24712.0	Microsoft Corporation	20190520
Microsoft Visual C++ 2017 Redistributable (x...	14.14.26427.4	Microsoft Corporation	20190519
NVIDIA GeForce Experience 3.16.0.107	3.16.0.107	NVIDIA Corporation	20190503
NVIDIA GeForce Driver 411.66	411.66	NVIDIA Corporation	20190503
NVIDIA HD Audio Driver 1.3.38.16	1.3.38.16	NVIDIA Corporation	20190503
NVIDIA PhysX System Software 9.19.0216	9.19.0216	NVIDIA Corporation	20190519
CEM Application Profile	1.00.0000	Advanced Micro Devices, Inc.	20190519
Realtek DASH Client Service	4.04	Realtek	20190521
Realtek Ethernet Controller AS-9014-0100	70.52.1306.2018	Realtek	20190521
ROG Live Service	1.0.0.0	ASUSTeK COMPUTER INC.	20190520
TeamViewer 14	14.4.7659	TeamViewer	20190521

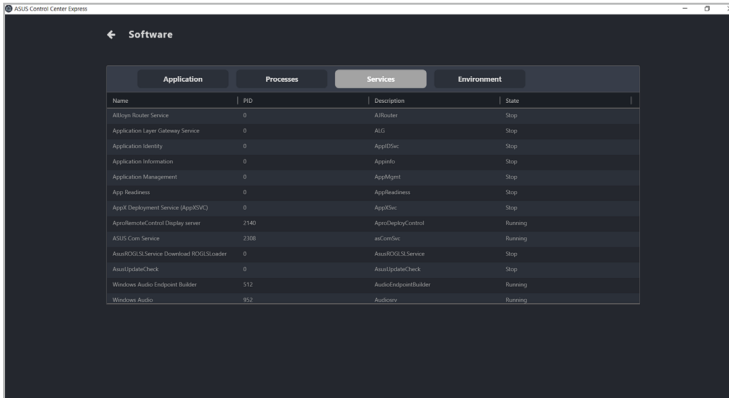
## 4.5.2 Processes tab

The **Processes** tab allows you to view information on active processes. You may also click on a process then select **End Task** to end the process.



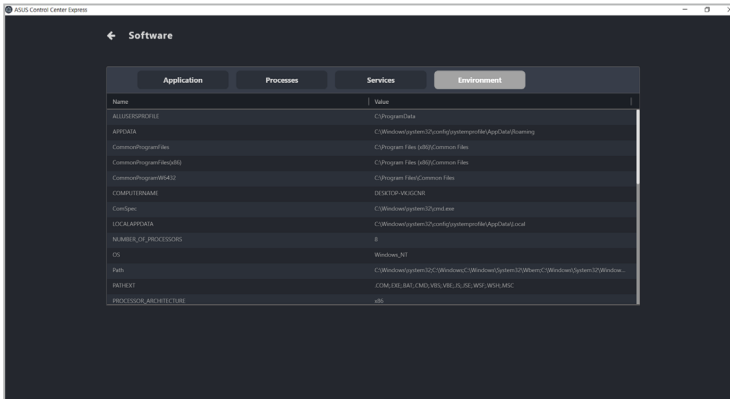
## 4.5.3 Services tab

The **Services** tab allows you to view information on the services available. You may click on a service then choose to start the service by clicking on **Start**, or stop a running process by clicking on **Stop**.



## 4.5.4 Environment tab

The **Environment** tab allows you to view information on the environment variables.



The screenshot shows the 'ASUS Control Center Express' window with the 'Software' section selected. Under 'Software', the 'Environment' tab is active, displaying a table of system environment variables.

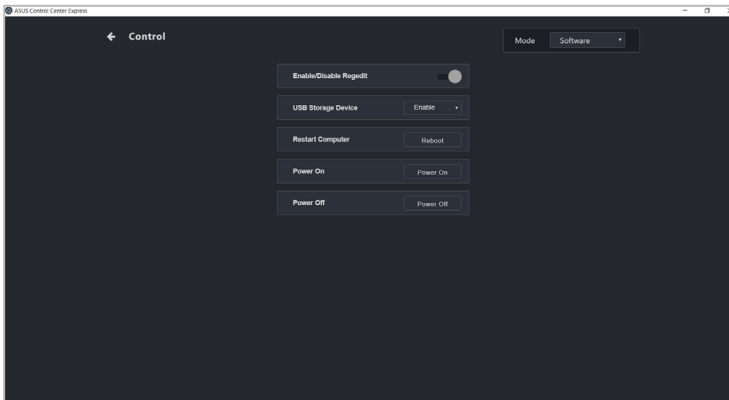
Name	Value
ALLUSERSPROFILE	C:\ProgramData
APPDATA	C:\Windows\System32\config\systemprofile\AppData\Roaming
CommonProgramFiles	C:\Program Files (x86)\Common Files
CommonProgramFiles(x86)	C:\Program Files (x86)\Common Files
CommonProgramFiles(x-ww)	C:\Program Files\Common Files
COMPUTERNAME	DESKTOP-WEUCNE
ComSpec	C:\Windows\System32\cmd.exe
LOCALAPPDATA	C:\Windows\System32\config\systemprofile\AppData\Local
NUMBER_OF_PROCESSORS	8
OS	Windows_NT
Path	C:\Windows\System32\WindowsCommon-System32\Windows\System32\Windows
PATHEXT	COM,EXE,BAT,CMD,VB,VB_SCRIPT,WSF,WSH,MSI
PROCESSOR_ARCHITECTURE	amd64



## 4.6 Control (software)



This item will not be available if your device is not logged into an OS environment, or is not connected using a management LAN port which supports RTL 8117 LAN IC.

This item allows you to configure items such as Regedit, USB Storage Device, and power control options. This item is software controlled and values may differ with the hardware version. Please refer to **5.5 Control (hardware)** for more information on **Hardware** mode.



<b>Enable/Disable Regedit</b>	Enable or disable the Windows Registry Editor. Enabled:  Disabled: 
<b>USB Storage Device</b>	Enable or disable the USB port, or set it to Read Only.
<b>Restart Computer</b>	Restart the client device.
<b>Power On</b>	Power on the client device.
<b>Power Off</b>	Power off the client device.



## 4.7 Event Log

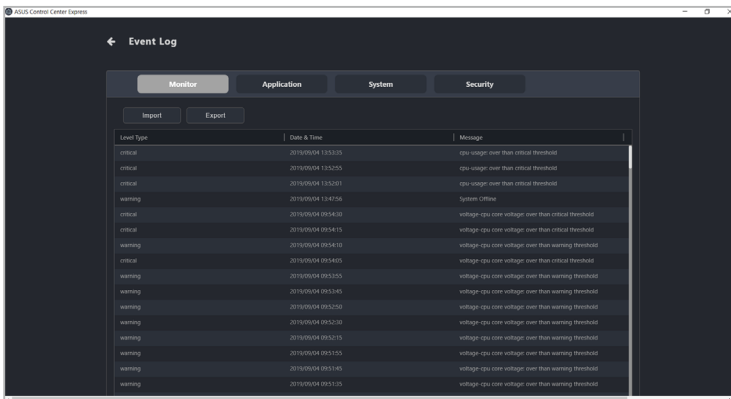
This item displays the event logs for the client devices of ASUS Control Center Express by clicking on the **Monitor**, **Application**, **System**, and **Security** tabs. In each event log tab you may click on an event to view more details about the event.

You may also export the tables to a .csv file, or import an ACC CSM Event Log .csv file:

- To export the table click the **Export** button, enter a filename, then click **Save**.
- To import an ACC CSM Event Log table click the **Import** button, select the ACC CSM Event Log .csv file you wish to import, then click **Open**.

### 4.7.1 Monitor tab

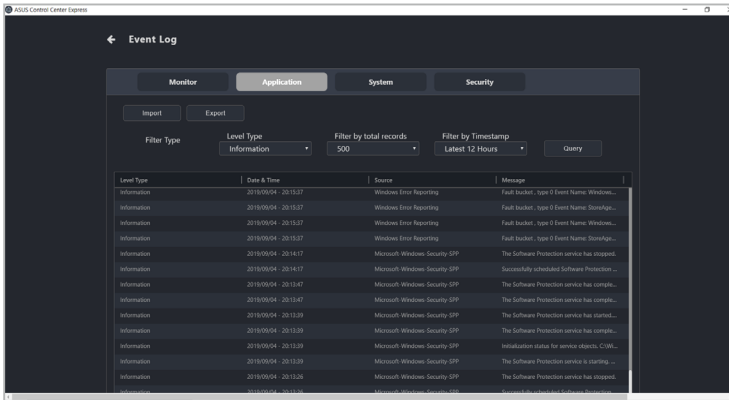
The **Monitor** tab allows you to view the event log of the status changes of client devices detected by the **Connection**, **Hardware**, and **Utilization** sensors.



Event Type	Date & Time	Message
critical	2019/05/04 15:32:25	cpu voltage over than critical threshold
critical	2019/05/04 15:32:25	cpu voltage over than critical threshold
critical	2019/05/04 15:32:25	cpu voltage over than critical threshold
warning	2019/05/04 15:47:56	system offline
critical	2019/05/04 09:14:52	voltage cpu core voltage over than critical threshold
critical	2019/05/04 09:14:52	voltage cpu core voltage over than critical threshold
warning	2019/05/04 09:14:52	voltage cpu core voltage over than warning threshold
critical	2019/05/04 09:14:40	voltage cpu core voltage over than critical threshold
warning	2019/05/04 09:15:45	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:45	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:50	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:50	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:15	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:15	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:45	voltage cpu core voltage over than warning threshold
warning	2019/05/04 09:15:35	voltage cpu core voltage over than warning threshold

## 4.7.2 Application tab

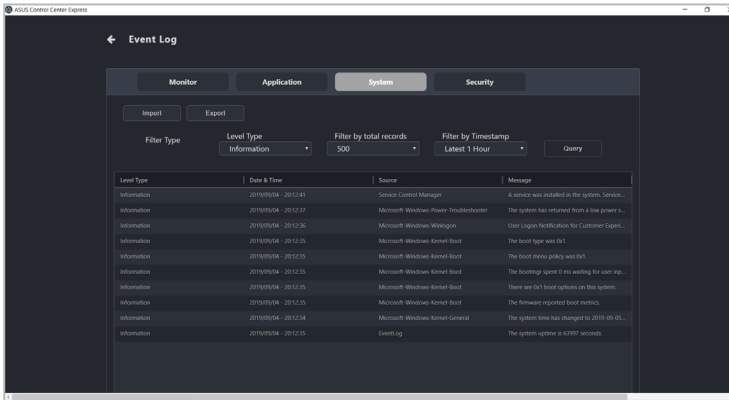
The **Application** tab allows you to filter application related events by selecting your filter criteria from the **Filter Type** block, then clicking **Query**.



<b>Level Type</b>	-	Ignore this filter
	<b>Information</b>	Information level events usually indicate an event which occurred without incident or issue
	<b>Warning</b>	Warning level events indicate potential issues which may not require immediate action
	<b>Error</b>	Error level events indicate loading or operation failures
	<b>Critical</b>	Critical level events indicate the most severe problems and may require immediate action
<b>Filter by total records</b>	Select the amount of events to display, or select - to ignore this filter	
<b>Filter by Timestamp</b>	Select the period of time to filter events, or select - to ignore this filter	

### 4.7.3 System tab

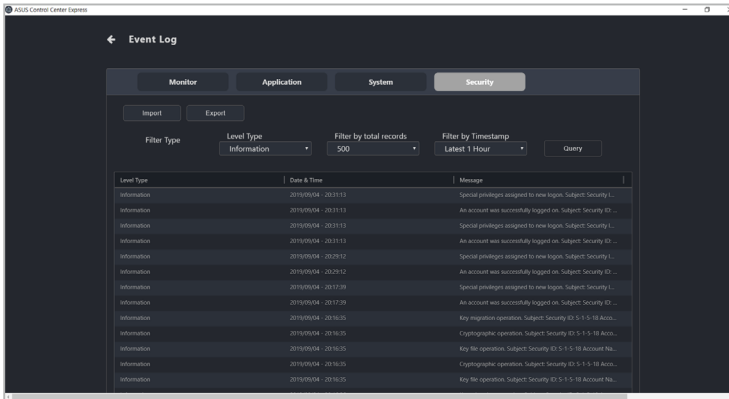
The **System** tab allows you to filter system related events by selecting your filter criteria from the **Filter Type** block, then clicking **Query**.



<b>Level Type</b>	-	Ignore this filter
	<b>Information</b>	Information level events usually indicate an event which occurred without incident or issue
	<b>Warning</b>	Warning level events indicate potential issues which may not require immediate action
	<b>Error</b>	Error level events indicate loading or operation failures
	<b>Critical</b>	Critical level events indicate the most severe problems and may require immediate action
<b>Filter by total records</b>	Select the amount of events to display, or select - to ignore this filter	
<b>Filter by Timestamp</b>	Select the period of time to filter events, or select - to ignore this filter	

## 4.7.4 Security tab

The **Security** tab allows you to filter security related events by selecting your filter criteria from the **Filter Type** block, then clicking **Query**.



<b>Level Type</b>	-	Ignore this filter
	<b>Information</b>	Information level events usually indicate an event which occurred without incident or issue
	<b>Warning</b>	Warning level events indicate potential issues which may not require immediate action
	<b>Error</b>	Error level events indicate loading or operation failures
	<b>Critical</b>	Critical level events indicate the most severe problems and may require immediate action
<b>Filter by total records</b>	Select the amount of events to display, or select - to ignore this filter	
<b>Filter by Timestamp</b>	Select the period of time to filter events, or select - to ignore this filter	

## 4.8 Remote Desktop

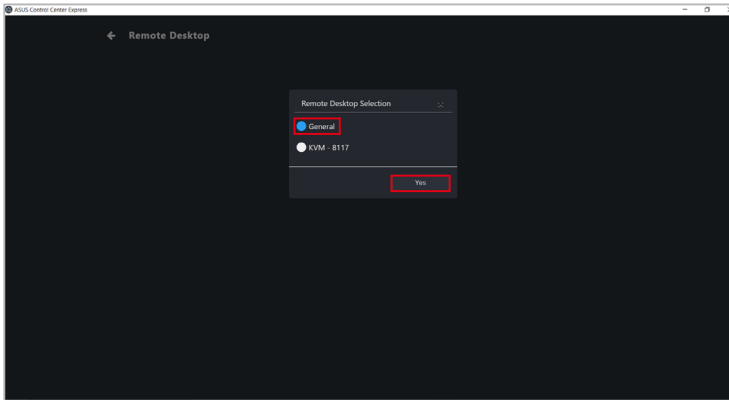
The **Remote Desktop** function provides a flexible interface for device management through the desktop accessed in ASUS Control Center Express.

### 4.8.1 General Remote Desktop

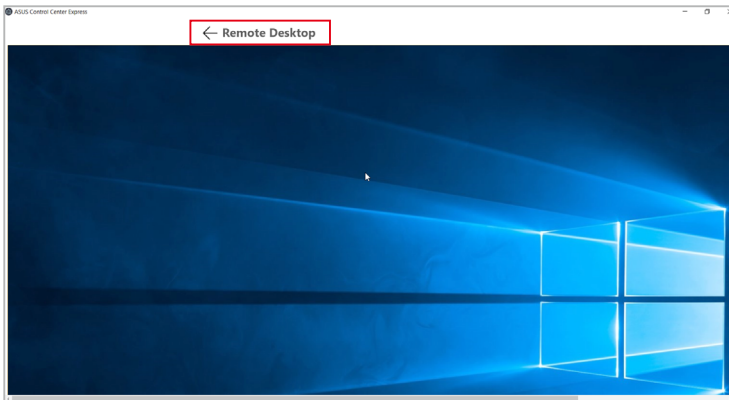
Select **General** and click on **Yes** to remotely control the client device.



The client device should be powered on and logged into an OS environment.



To end the remote control session, scroll to the top of the page, then click on **← Remote Desktop**.



## 4.8.2 Out-of-band Management Remote Desktop

This method of remote desktop will allow you to control your client device even if it is not in an OS environment, such as BIOS.



This remote control method requires the client device to have KVM enabled, and connected using a management LAN port which supports RTL 8117 LAN IC.

### Setting up KVM before using Remote Desktop

Before using the Out-of-band Management Remote Desktop function, ensure you have enabled KVM, and selected a KVM Display Mode.

1. Select the device you would like to use out-of-band management remote desktop in the main dashboard overview, and click **Select function > 8117 Control > 8117 - KVM Enable**.
2. Reboot the client device and enter BIOS setup, then navigate to **Advanced > RTL8117 setting**.



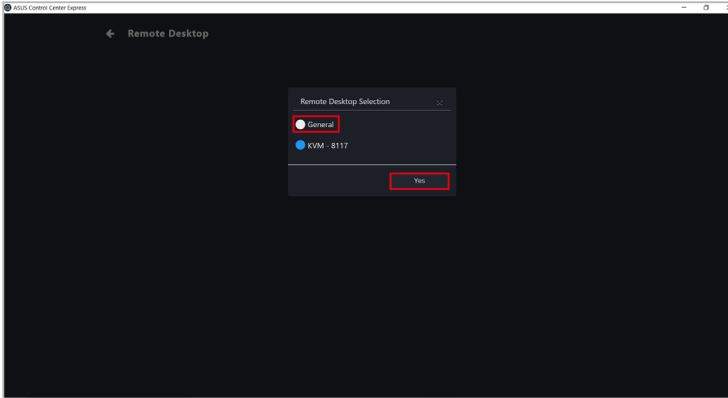
The BIOS settings may differ between client devices. Please refer to your client device's motherboard user manual for more information about navigating the BIOS and BIOS settings.

3. Click on the drop down menu of the **KVM Display Mode** option, and select a display mode from the following configuration options:

<b>Remote Multit-Display</b>	BIOS screen will be mirrored on both server remote desktop and client devices. OS screen will only be displayed on the server remote desktop.
<b>Local Multi-Display</b>	BIOS screen will be mirrored on both server remote desktop and client devices. OS screen will only be displayed on the client device.
<b>Remote Single-Display</b>	BIOS and OS screen will only be displayed on the server remote desktop.
<b>Local Single-Display</b>	BIOS and OS screen will only be displayed on the client device.

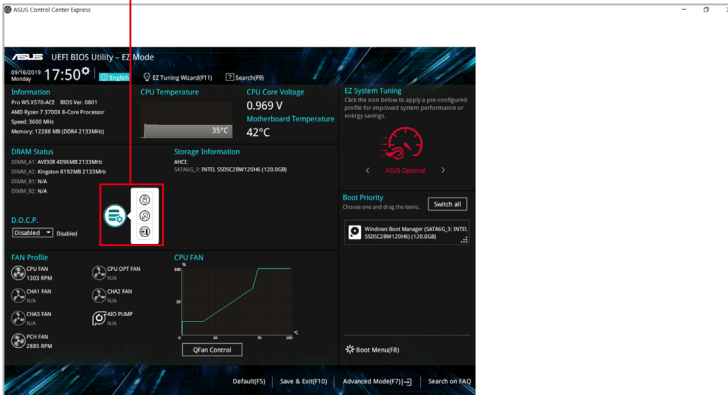
## Using the out-of-band management Remote Desktop


Select **KVM - 8117** and click on **Yes** to remotely control your client device even if it is not in an OS environment.



Clicking on the Function button offers more options for navigating the remote desktop screen.


### Function button



 Leave : Return to the previous options

Display remote mouse cursor : When there is no mouse connected to the client, there may not be a mouse cursor available for the remote screen, click to display a remote mouse cursor on the remote desktop screen.

---


 Leave : Return to the previous options

Switch full screen : Zooms the remote desktop screen to fit within your screen .

Zoom to screen size : Centers the remote desktop screen.

Dynamic zoom size : Zoom in or out by using the horizontal slider.

---

 : End the remote control session



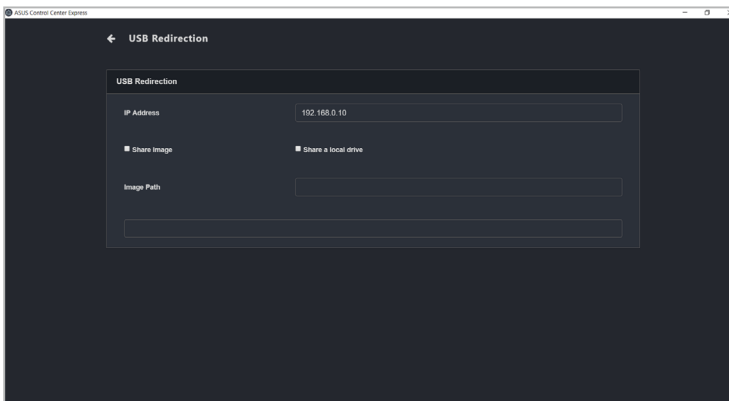
## 4.9 USB Redirection

The **USB Redirection** function allows your client devices to read USB drives connected to your main server. This is useful for situations where you need to boot up the client device using a USB device, or when you need to access a USB connected to the main server from a remote location.



This function is only available when the following requirements are met:

- Client device is online and logged into the OS
- Has already had an agent deployed to it
- Connected using a management LAN port which supports RTL 8117 LAN



<b>IP Address</b>	The ip address of the device the USB device is connected to
<b>Share Image</b>	Copy the path or link to an image file you wish to mount onto the client device
<b>Share a local drive</b>	Allow the client device access to a selected USB storage device connected to the main server device.
<b>Image Path</b>	The path of your redirected USB device or image file

## 4.10 BIOS



This item will have limited functions if your device is not logged into an OS environment, or is not connected using a management LAN port which supports RTL 8117 LAN IC.

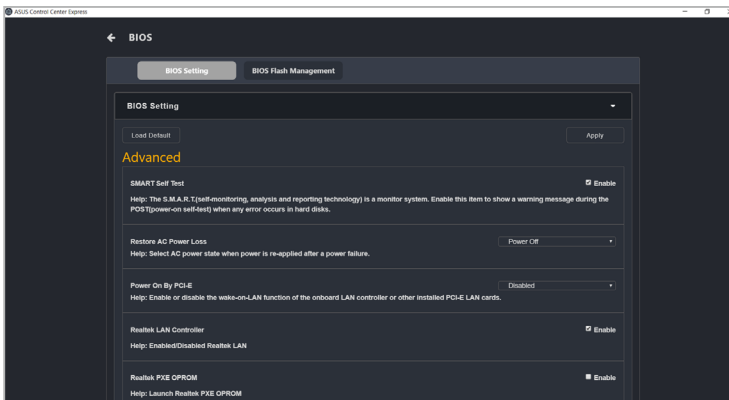
This item will allow you to adjust some BIOS settings such as **Advanced**, **Boot**, **Monitor** and **Security**. It also allows you to update the BIOS of a device by uploading a BIOS file manually or from the BIOS Cache.

### 4.10.1 BIOS Setting

Adjust the BIOS **Advanced**, **Boot**, **Monitor** and **Security** settings of your client device, then click **Apply** to save the changes made, or click **Load Default** to load the default settings.



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



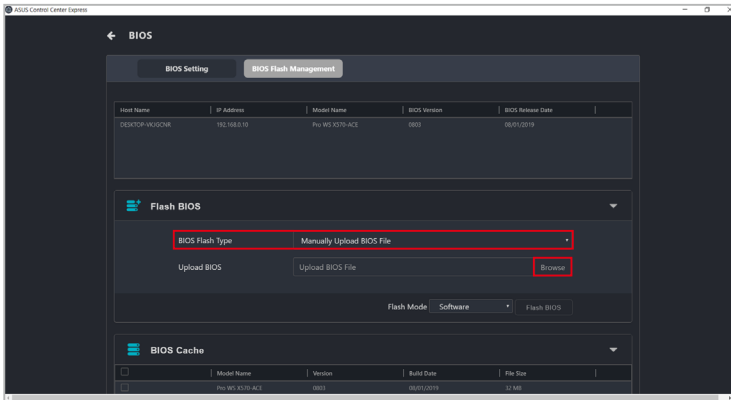
## 4.10.2 BIOS Flash Management

You can flash the BIOS by manually uploading a BIOS file or by selecting a previously flashed BIOS file from the BIOS cache. You may also remove BIOS files from the BIOS cache if needed.

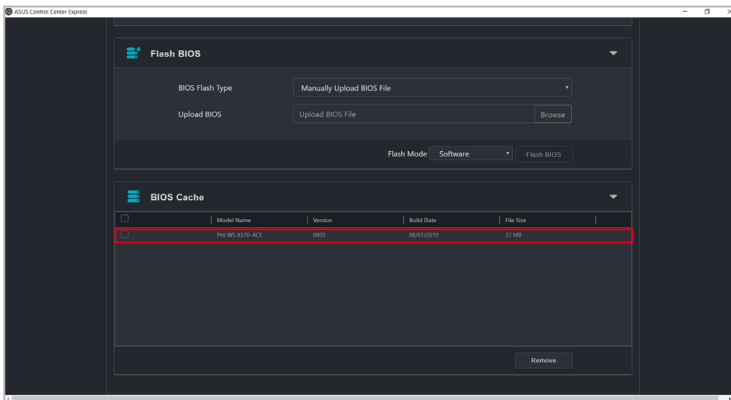
### Flashing BIOS by manually uploading BIOS file

Manually upload a BIOS file to flash the BIOS of the client device. The BIOS file uploaded and flashed with will be added to the BIOS Cache.

1. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.
2. Click on **Browse** to select a BIOS file.



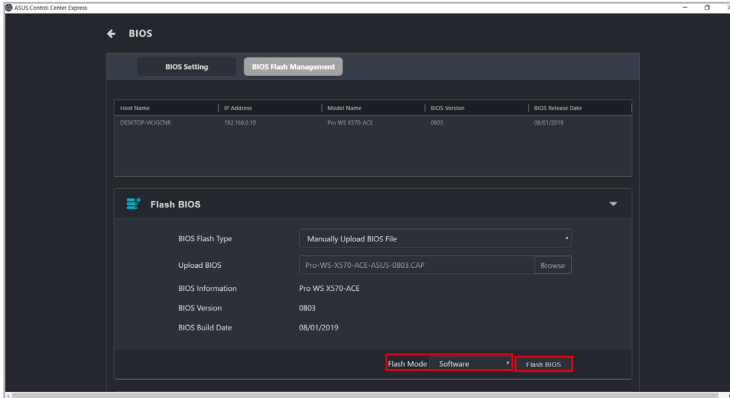
3. Confirm that the BIOS file was successfully uploaded and click **OK**. The uploaded BIOS file will also be added to the **BIOS Cache**.



4. Select your **Flash Mode**, then click on **Flash BIOS**.



Hardware Flash Mode is only available if the client device is connected using a management LAN port which supports RTL 8117 LAN IC.



5. Click **OK** to begin the flash process.

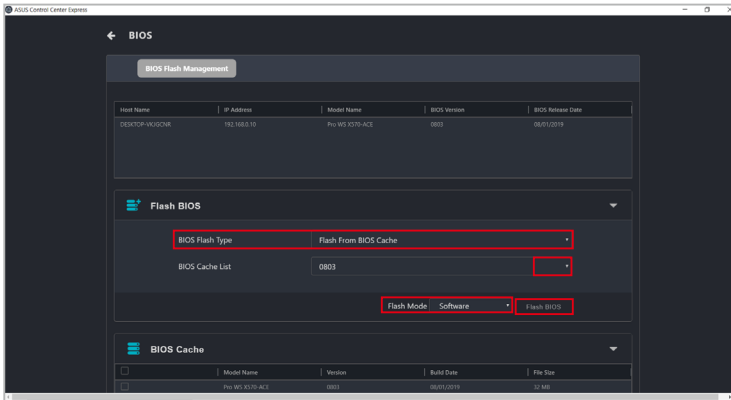
## Flashing BIOS from the BIOS cache

You can select a BIOS file from the BIOS cache.

1. Select **Flash from BIOS Cache** in the **BIOS Flash Type** field.
2. An applicable BIOS file should be automatically selected, if you wish to select another BIOS file, click on the **BIOS Cache List** drop down menu.
3. Select your **Flash Mode**, then click on **Flash BIOS** to begin the BIOS flash process.

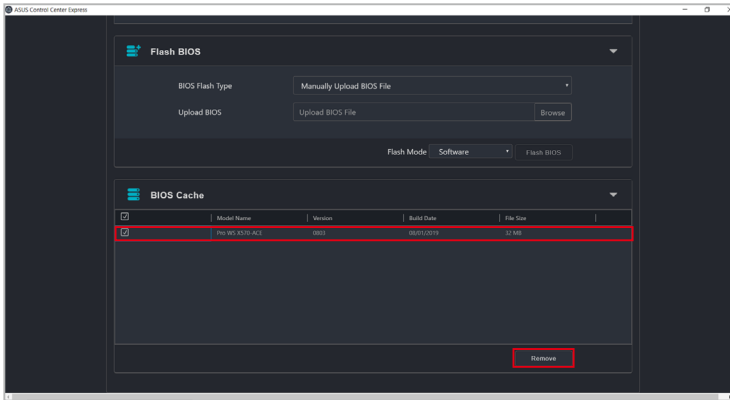


Hardware Flash Mode is only available if the client device is connected using a management LAN port which supports RTL 8117 LAN IC.



## Removing a BIOS file from the BIOS cache

You can view the BIOS files available for the client device in the BIOS Cache block. To remove a BIOS file from the BIOS Cache, check the BIOS file you wish to remove, then click on **Remove**.



# Chapter 5

This chapter describes the metadata management, software management, and hardware based management functions.


# Management Control

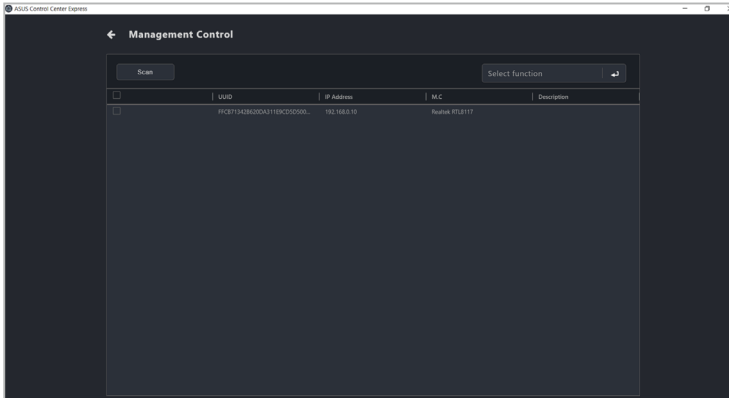


The screenshots in this chapter are for reference only.

## 5.1 Management Control Overview

The Management Control options allow you to manage a client device which is connected via a management LAN port which supports RTL 8117 LAN IC, and also allows out-of-band management.

To access **Management Control**, click on  located at the top right menu bar.



### 5.1.1 Scanning for devices

You can scan for client devices which support the Management Control functions by clicking on **Scan**.


### 5.1.2 Using shortcut functions

1. Select the device(s) you would like to perform an action on.
2. Click on **Select function**, and select the function you would like to use. Please refer to the table on the next page for a brief summary of each function.



- For more details on the following functions listed below, please refer to
  - USB Redirection: **4.9 USB Redirection**
  - 8117-Set password: **5.1.3 Setting the password for RTL8117**
  - 8117-Update Firmware: **5.9 Firmware Update**
  - 8117-Smart BIOS: **4.10 BIOS**
- Some functions may require you to restart the client device for the changes to take effect.



<b>8117-Restart Computer</b>	Restart the selected device(s).
<b>8117-Force Power OFF</b>	Force power off the selected device(s).
<b>8117-Power OFF</b>	Power off the selected device(s).
<b>8117-Power ON</b>	Power on the selected device(s).
<b>8117-Clear CMOS</b>	Clear CMOS for selected device(s).
<b>USB Redirection</b>	Allows access of a USB device from within a remote desktop or application using RTL8117.
<b>8117-Set password</b>	Set an encryption password for RTL8117
<b>Restart Service</b>	Restart the RTL8117 service on selected device(s)
<b>8117-Smart BIOS</b>	Flash the BIOS of the selected device(s) using RTL8117.
<b>8117-Update Firmware</b>	Update the RTL8117 firmware.  Firmware Update will be disabled if 8117-KVM is Enabled.
<b>8117-KVM Enable</b>	Enable KVM for selected device(s).
<b>8117-KVM Disable</b>	Disable KVM for selected device(s).

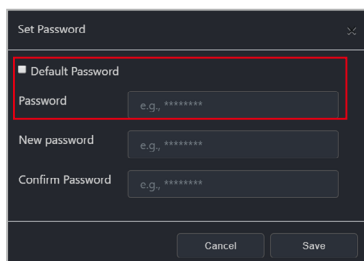
### 5.1.3 Setting the password for RTL8117

You can set an encryption password for RTL8117 using this function.

1. Select the device(s) you would like to set the encryption password for.
2. Click on **Select function > 8117 - Control > 8117 - Set password**.
3. Enter the current password in the **Password** field, or you may check **Default Password** to load a previously set password.



If no RTL8117 password was previously set, checking **Default Password** will load the system's default password.



3. Enter your new password into the **New password** field, and enter it again into the **Confirm Password** field.



The password should be a minimum of 8 characters and should only consist of uppercase characters, lowercase characters, and numbers.

A screenshot of a 'Set Password' dialog box. It has a title bar with a close button. Below the title bar is a checkbox labeled 'Default Password'. There are three input fields: 'Password', 'New password', and 'Confirm Password'. Each field contains the placeholder text 'e.g. \*\*\*\*\*'. A red rectangular box highlights the 'New password' and 'Confirm Password' fields. At the bottom of the dialog are two buttons: 'Cancel' and 'Save'.

4. Click **Save** once you are finished.

A screenshot of the same 'Set Password' dialog box. The 'New password' and 'Confirm Password' fields are no longer highlighted. Instead, the 'Save' button at the bottom right is highlighted with a red rectangular box.

## 5.2 Management Control Information Overview

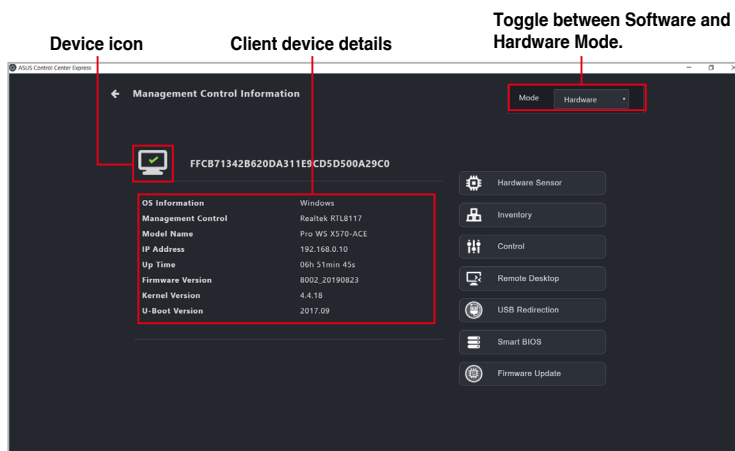
The **Management Control Information** provides you with detailed information about your selected client device, and also provides you with some hardware controlled management functions such as power control options.

To access **Management Control Information** of a client device, please refer to one of the following methods:

- Classic dashboard view: Click on a client device in the device list, then select **Hardware** in the **Mode** dropdown menu.
- Graphic dashboard view: Double click on a client device shortcut icon, then select **Hardware** in the **Mode** dropdown menu.
- Management Control: Click on a client device in the scanned list of the **Management Control** screen.



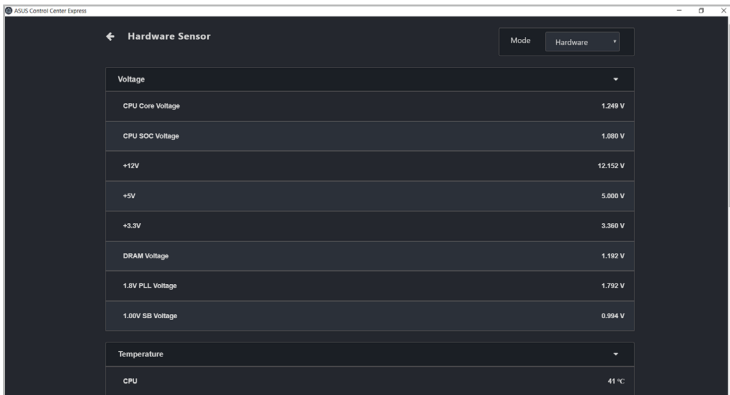
- 
- Some options are only available when the client device is online and logged into the OS.
  - This chapter is only for the **Hardware Mode** options, for **Software Mode** options, please refer to **Chapter 4 Device Information**.
-



<b>Device Name</b>	Displays the device name.
<b>Device icon</b>	Click on the device icon to view the event log of this device.w
<b>OS Information</b>	Displays information on the Operating System.
<b>Management Control</b>	Displays the Management Control LAN IC
<b>Model Name</b>	Displays the model name of client device.
<b>IP Address</b>	Displays the IP address of client device.
<b>Up Time</b>	Displays the up time of client device.
<b>Firmware Version</b>	Displays the firmware version of client device.
<b>Kernel Version</b>	Displays the kernel version of client device.
<b>U-Boot Version</b>	Displays the U-Boot version of client device.

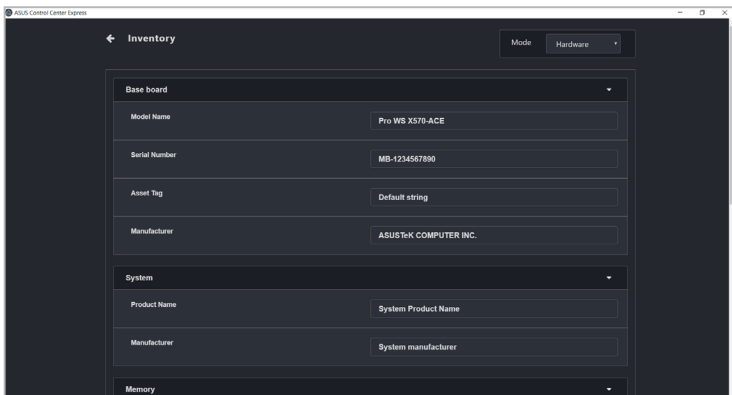
## 5.3 Hardware Sensor (hardware)

This item allows you to view threshold value for items such as voltage, temperature, and fans. This item is hardware controlled and values may differ with the software version. Please refer to **4.2 Hardware sensor (software)** for more information on **Software** mode.



## 5.4 Inventory (hardware)

This item displays more details about the client device. This item is hardware controlled and values may differ with the software version. Please refer to **4.4 Inventory (software)** for more information on **Software** mode.

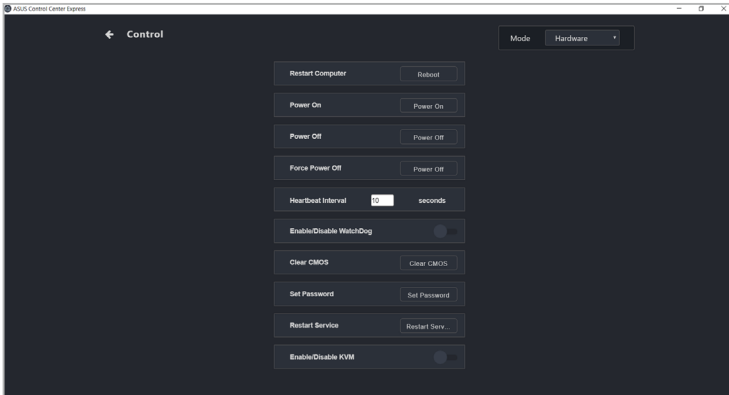



## 5.5 Control (hardware)

This item allows you to configure KVM and Watchdog, clear CMOS, restart services, set an encryption password, and configure power control options. This item is hardware controlled and values may differ with the software version. Please refer to **4.6 Control (software)** for more information on **Software** mode.



Some functions may require you to restart the client device for the changes to take effect.



<b>Restart Computer</b>	Restarts the client device.
<b>Power On</b>	Power on the client device.
<b>Power Off</b>	Power off the client device.
<b>Force Power Off</b>	Forces a power off if your client device may be unresponsive due to an error.
<b>Heartbeat Interval*</b>	Allows you to set the time interval in seconds for which the hardware signals are checked.
<b>Enabled / Disable Watchdog*</b>	Enable or disable the Windows Registry Editor. Enabled: <input type="checkbox"/> Disabled: <input type="checkbox"/>
<b>Clear CMOS</b>	Clears the BIOS setup information for when the client hangs due to overclocking or other errors.  Ensure the client device is completely powered off before clearing CMOS. Power the client device on after the clearing the CMOS.

\* These functions only appear if an agent is already deployed to this device and if you switch from Software Mode to Hardware Mode

(continued on the next page)

<b>Set Password</b>	Set an encryption password.
<b>Restart Service</b>	Restart service.
<b>Enable/Disable KVM</b>	Enable or disable KVM. Enabled: <input checked="" type="checkbox"/> Disabled: <input type="checkbox"/>

## 5.6 Remote Desktop

The **Remote Desktop** function provides a flexible interface for out-of-band device management through the desktop accessed in ASUS Control Center Express. Please refer to **4.8.2 Out-of-band Management Remote Desktop** for more information on using the out-of-band management remote desktop.

## 5.7 USB Redirection

The **USB Redirection** function allows your client devices to read USB drives connected to your main server. This is useful for situations where you need to boot up the client device using a USB device, or when you need to access a USB connected to the main server from a remote location. Please refer to **4.9 USB Redirection** for more information.

## 5.8 Smart BIOS

The **Smart BIOS** function allows you to update the BIOS of a device by uploading a BIOS file manually or from the BIOS Cache.




---

The client device will restart after a BIOS flash is finished for the changes to take effect.

---

### 5.8.1 BIOS Flash Management

You can flash the BIOS by manually uploading a BIOS file or by selecting a previously flashed BIOS file from the BIOS cache. You may also remove BIOS files from the BIOS cache if needed.

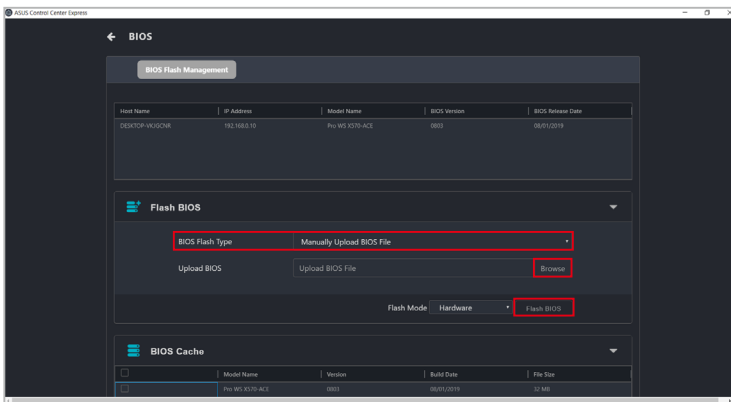
## Flashing BIOS by manually uploading BIOS file

Manually upload a BIOS file to flash the BIOS of the client device. The BIOS file uploaded and flashed with will be added to the BIOS Cache.

1. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.
2. Click on **Browse** to select a BIOS file, then click **OK** to confirm the BIOS file was uploaded successfully. The uploaded BIOS file will also be added to the **BIOS Cache**
3. Click on **Flash BIOS**.



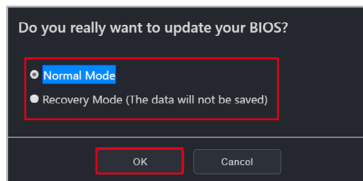
**Flash Mode** will be defaulted to **Hardware Mode**.



4. Select if you wish to perform a **Normal Mode** BIOS flash or if you wish to do a **Recovery Mode** BIOS flash, then click **OK**.



Performing a **Recovery Mode** BIOS Flash will reset all BIOS configurations, and remove all previous configurations.





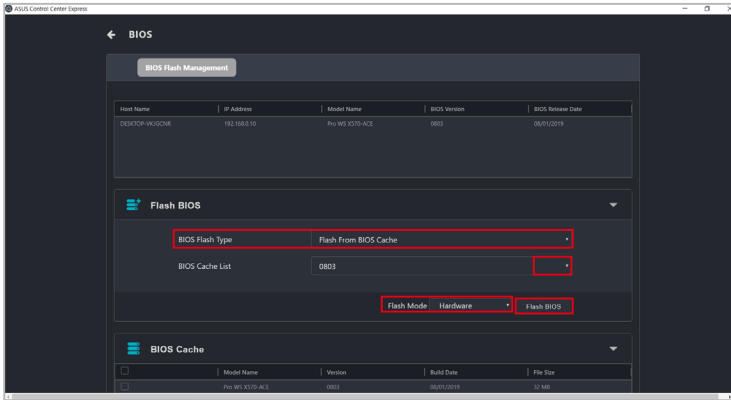
## Flashing BIOS from the BIOS cache

You can select a BIOS file from the BIOS cache.

1. Select **Flash from BIOS Cache** in the **BIOS Flash Type** field.
2. Select a BIOS file from the **BIOS Cache List** drop down menu.
3. Click on **Flash BIOS**.



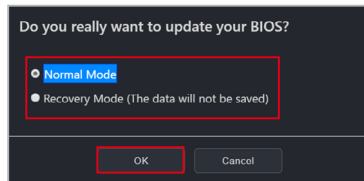
**Flash Mode** will be defaulted to **Hardware Mode**.



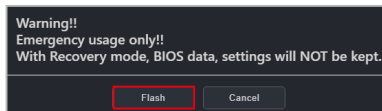
4. Select if you wish to perform a **Normal Mode** BIOS flash or if you wish to do a **Recovery Mode** BIOS flash, then click **OK**.



Performing a **Recovery Mode** BIOS Flash will reset all BIOS configurations, and remove all previous configurations.

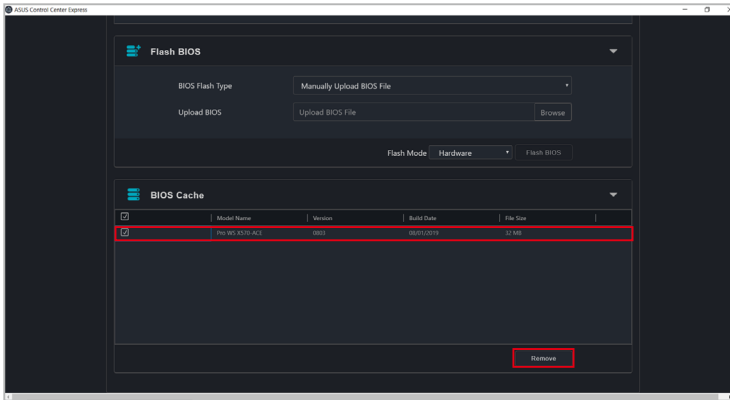


5. (Optional) If you selected **Recovery Mode**, you will be prompted with a warning message, as **Recovery Mode** will remove all previous BIOS data and configurations. Click **Flash** to continue with using **Recovery Mode**.



## Removing a BIOS file from the BIOS cache

You can view the BIOS files available for the client device in the BIOS Cache block. To remove a BIOS file from the BIOS Cache, check the BIOS file you wish to remove, then click on **Remove**.



## 5.9 Firmware Update

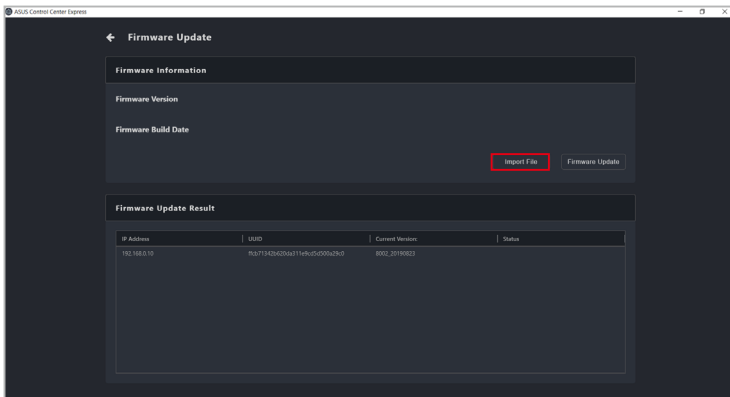
The **Firmware Update** function allows you to update the firmware of the RTL 8117 LAN IC, and also displays the results of the firmware update.



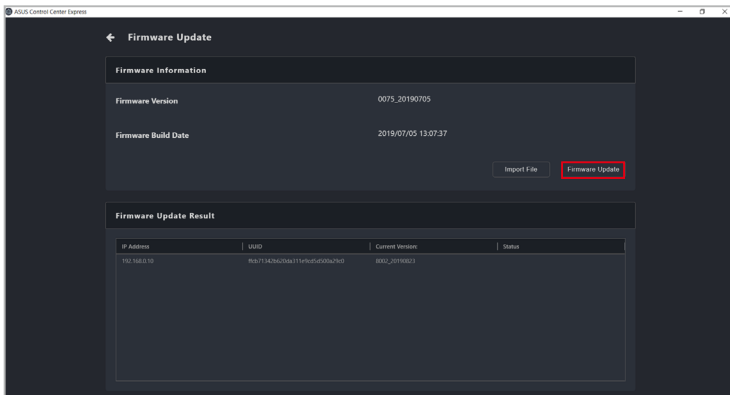
**Firmware Update** will be disabled when KVM is set to enabled. To update firmware please set KVM to disabled.

### 5.9.1 Uploading and updating firmware

1. Click on **Import File**, then select your firmware file (.img) and click **Open**.



2. Click on **Firmware Update**, then wait for the update to be completed.



3. You can check the results of the firmware update in the **Firmware Update Result** block.
4. (optional) If the client device's firmware was updated while it was powered on, please reboot the client device after the firmware has been successfully updated.

## 5.10 Software Management

This item provides centralized software management, such as dispatching software setup and script files to selected devices, adding software packages to the Software Pool, view software information, or blacklisting software on selected client devices.

### 5.10.1 Software Dispatch

This item allows you to dispatch software setup and script files.

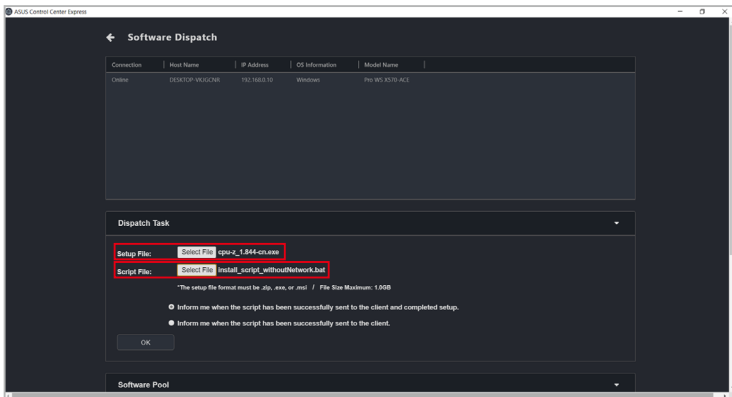
To access **Software Dispatch**, select the client device(s) then click on **Select Function > Software Management > Software Dispatch**.

#### Dispatching software to client device

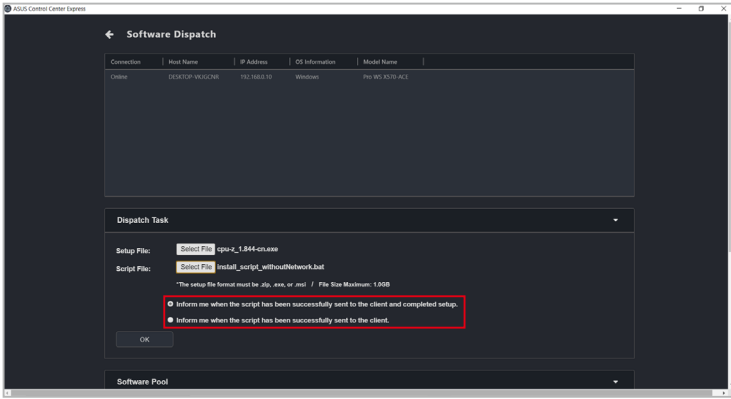
1. Select the **Setup File** and **Script File** you would like to upload and dispatch to the client device.



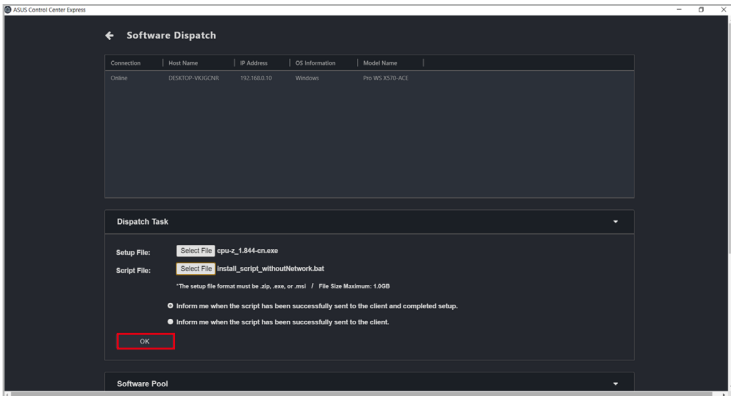
- The following setup file formats are supported: .zip, .exe, or .msi.
- The file size of the setup file should not exceed 1.0 GB.



- (optional) Select the notification scenario for when the script has been successfully sent to the client and completed setup, or if the script has been successfully sent to the client.



- Click on **OK**, then wait for the software dispatch process to finish. Once it is completed you should receive a notification based on the notification scenario selected.



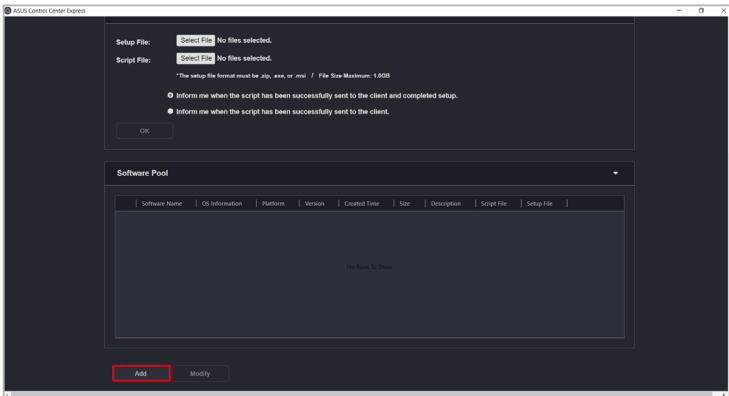
## 5.10.2 Software Pool

You can dispatch, remove or modify software packages uploaded to your software pool.

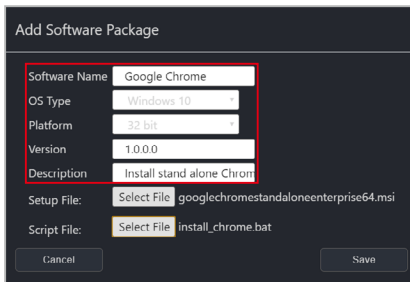
To access the software pool, select the client device(s) and click on **Select Function > Software Management > Software Dispatch**, then scroll to the bottom of the **Software Dispatch** screen.

### Adding software packages to the Software Pool

1. Click on **Add**.



2. Enter the required information into the **Software Name**, **OS Type**, **Platform**, and **Version** fields. You may also type in a brief description of the software package into the **Description** field.



3. Select the **Setup File** and **Script File** you would like to upload. Click on **Save** once you have finished.



- The following setup file formats are supported: .zip, .exe, or .msi.
- The file size of the setup file should not exceed 1.0 GB.

Add Software Package

Software Name: Google Chrome

OS Type: Windows 10

Platform: 32 bit

Version: 1.0.0.0

Description: Install stand alone Chrom

Setup File:

Script File:

Cancel Save

4. The added software package should appear in the Software Pool list.

Dispatch Task

Setup File:  No files selected.

Script File:  No files selected.

\*The setup file format must be .zip, .exe, or .msi / File Size Maximum: 1.0GB

Inform me when the script has been successfully sent to the client and completed setup.

Inform me when the script has been successfully sent to the client.

OK

Software Pool

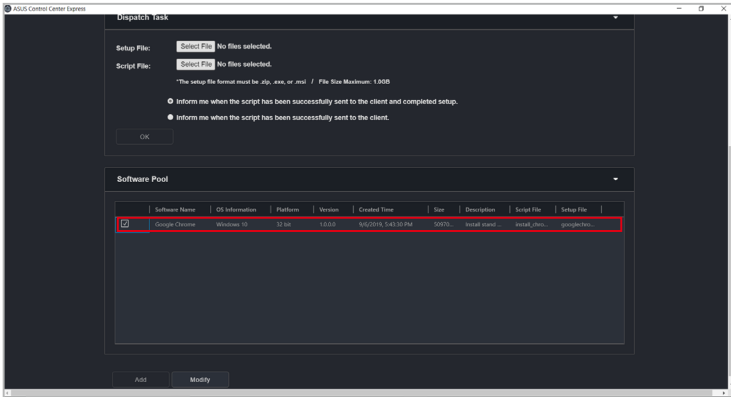
Software Name	OS Information	Platform	Version	Created Time	Size	Description	Script File	Setup File
Google Chrome	Windows 10	32 bit	1.0.0.0	5/5/2018, 5:43:10 PM	500KB	Install stand	install_chrome	googlechrom

Add Modify

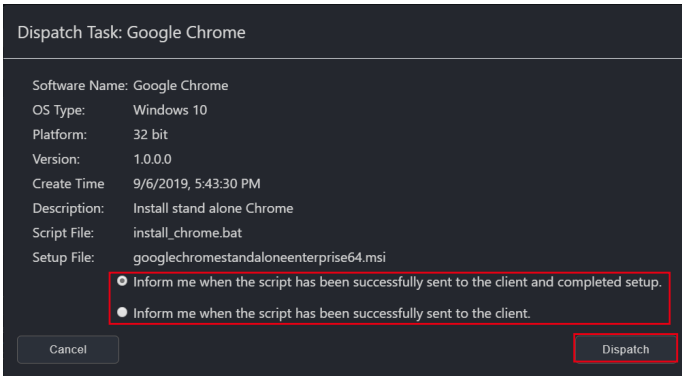


## Dispatching software using the Software Pool

1. Click on the software package you would like to dispatch from the **Software Pool**.

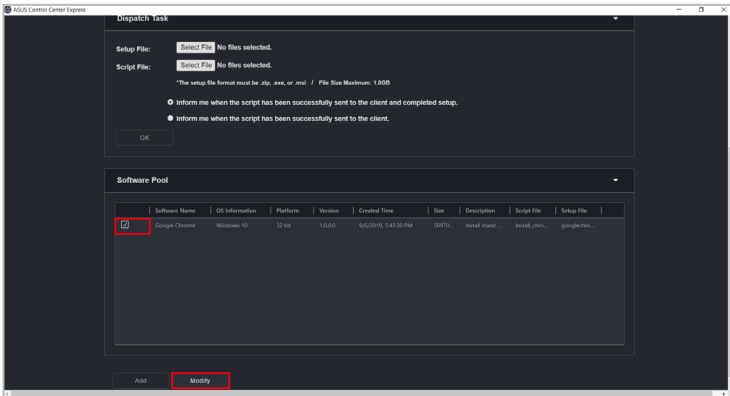


2. Select the notification scenario, then click on **Dispatch**. Once the software dispatch process is completed you should receive a notification based on the notification scenario selected.

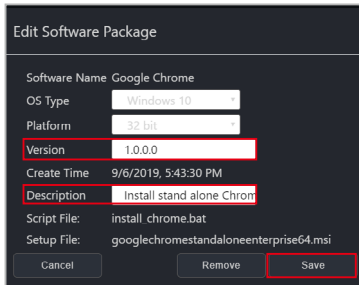


## Modifying a software package

1. Check the software package you would like to modify from the **Software Pool**, then click on **Modify**.

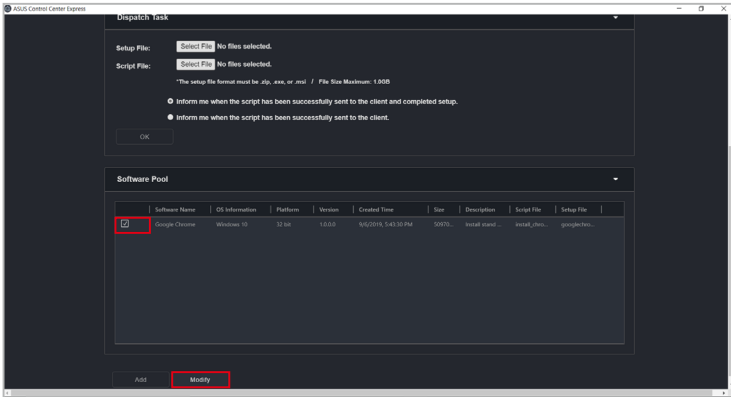


2. You can edit the **Version** and **Description**, once you have finished, click on **Save** to save the changes made.

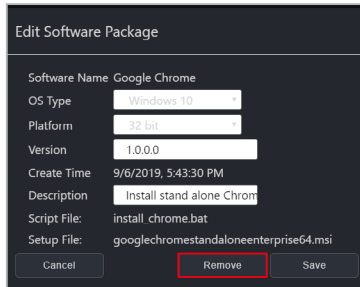


## Deleting a software package

1. Check the software package you would like to delete from the **Software Pool**, then click on **Modify**.



2. Click on **Remove** to remove the software package from the Software Pool.



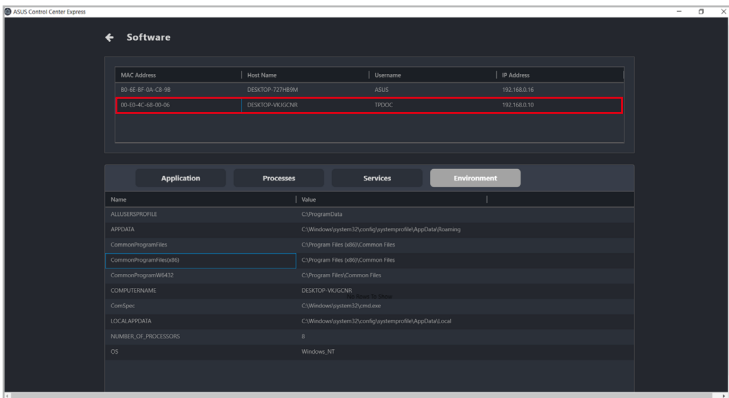
### 5.10.3 Software Information

You can view the information on Application, Processes, Services and Environment variables of multiple devices, by selecting the client device(s) you wish to view software information on and clicking on **Select Function > Software Management > Software Information**.

Click on a device in the top block of the Software Information screen and the Application, Processes, Services, and Environment variables of the selected device should be displayed in the different tabs below.



Some operating system applications, processes, and services cannot be removed, terminated, or stopped.



#### Application tab

The **Application** tab allows you to view information on applications installed on the selected client device. You may also click on an application then select **Uninstall** to uninstall the application on all selected devices.



The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.

#### Processes tab

The **Processes** tab allows you to view information on active processes. You may also click on a process then select **End Task** to end the process.

## Services tab

The **Services** tab allows you to view information on the services available on the selected device. You may click on a service then choose to start the service by clicking on **Start**, or stop a running process by clicking on **Stop**.

## Environment tab

The **Environment** tab allows you to view information on the common environment variables.

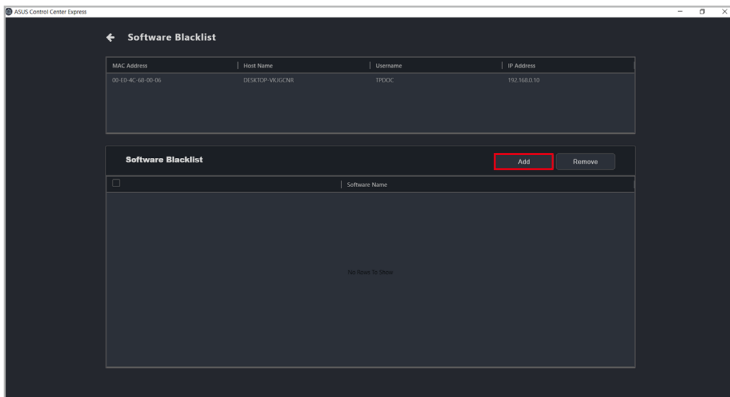
### 5.10.4 Software Blacklist

You can add software to the software blacklist of all selected devices.

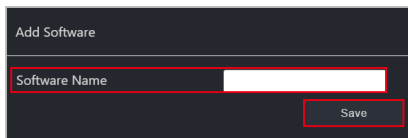
To access the **Software Blacklist**, select the client device(s) and click on **Select Function > Software Management > Software Blacklist**.

#### Adding a software to the Software Blacklist

1. Click on **Add**.

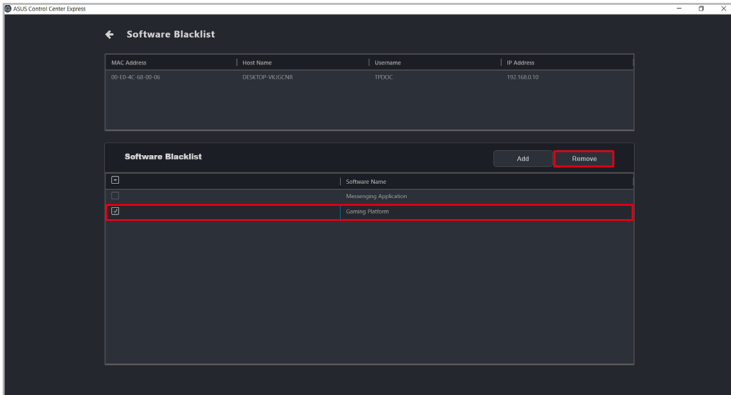


2. Enter the name of the software you wish to blacklist, then click on **Save**.




## Removing a software from the Software Blacklist

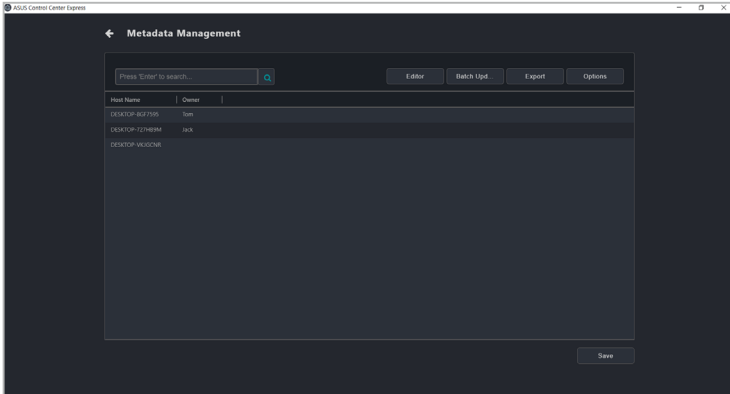
Select the software from the Software Blacklist and click on **Remove**, then click on **OK**.



## 5.11 Metadata Management

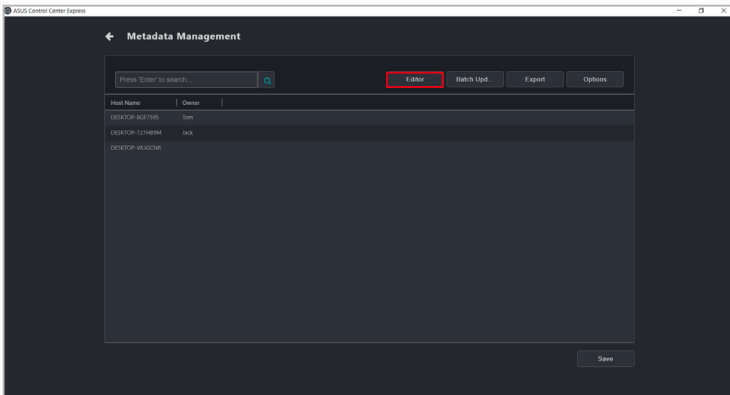
This item allows you to add or edit metadata fields and information which is displayed when viewing device information.

To access **Metadata Management**, click on  located at the top right menu bar.

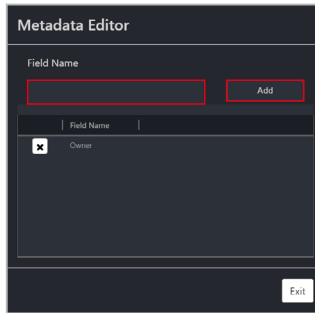


### 5.11.1 Adding metadata fields

1. Click on **Editor**.



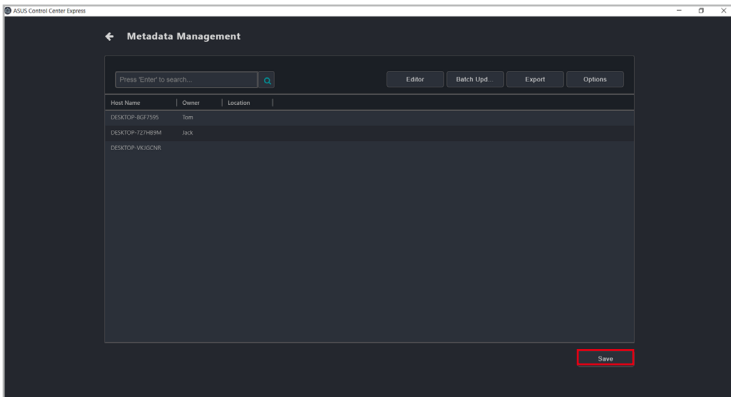
2. Enter the name of the metadata field you would like to add, then click on **Add**.



3. Your new metadata field should appear in the metadata management list, click on **Save** to save the changes done.



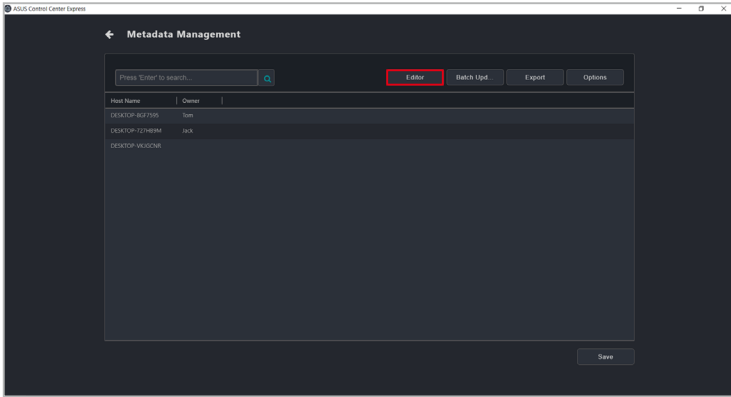
For this example we have added the "Location" metadata field.



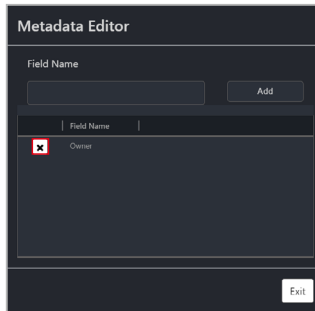


## 5.11.2 Removing metadata fields

1. Click on **Editor**.



2. Click on the **X** next to the metadata field you would like to remove, then click **Yes**

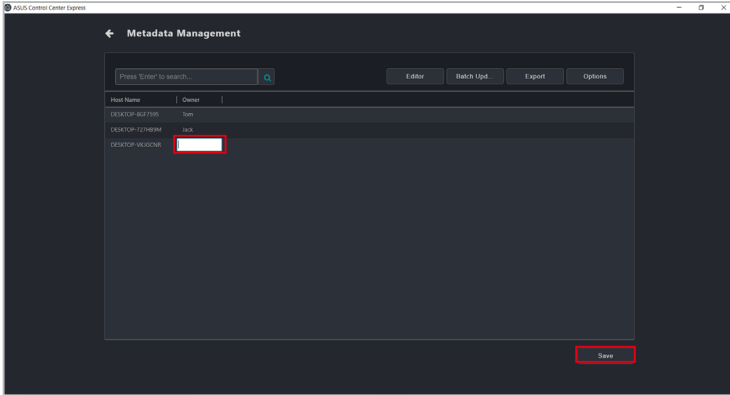


### 5.11.3 Updating the metadata manually

You can edit the metadata of each device by double clicking on the cell of the field you would like to update, then clicking on **Save** once you are finished to save the changes made.



The **Host Name** field displays a list of the client devices, and cannot be edited.

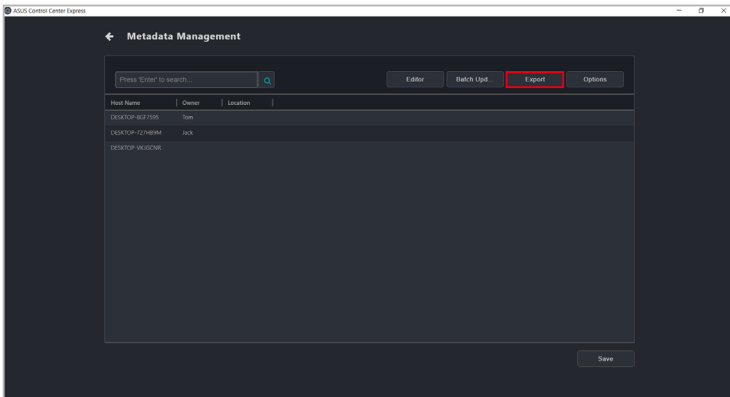


## 5.11.4 Updating the metadata using a batch update

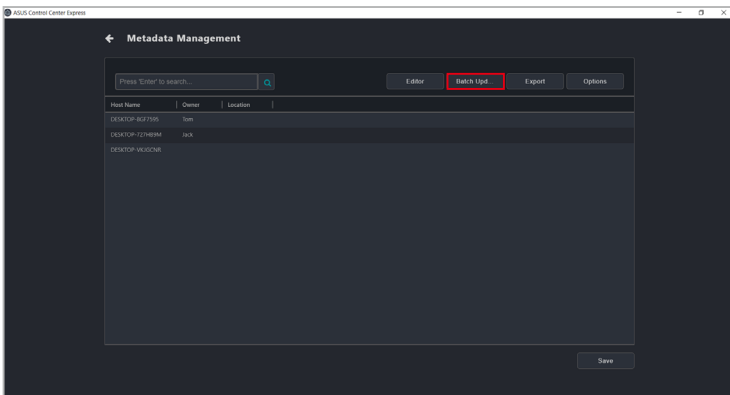
1. First export a .csv file of the metadata fields you wish to populate by clicking on **Export**.



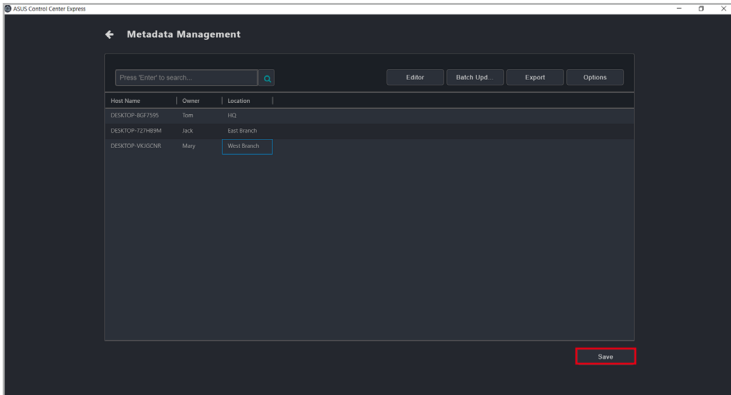
To customize which metadata fields to export, click on **Options**, then select the metadata fields you wish to export. Deselecting a metadata field will hide the metadata field and will not add that field to the exported .csv file.



2. Update the exported .csv file with the data you wish to populate the metadata fields on ASUS Control Center Express with.
3. Click on **Batch Update**, then select the .csv file you updated and click **Open**. Your metadata fields should be populated with the information on the .csv file.



4. Click on **Save** to save the changes made.



# Chapter 6

This chapter describes how to import configurations of your ACC CSM to ASUS Control Center Express, and also allow you to deploy ASUS Control Center Express agents to devices managed by ACC CSM.

# Settings Migrator

## 6.1 Settings Migrator

If you are already using ACC CSM and wish to import all your ACC CSM configurations to ASUS Control Center Express, you can use the Settings Migrator function. This will also allow you to deploy ASUS Control Center Express agents to existing devices managed by your ACC CSM.

To access **Settings Migrator**, click on  located at the top right menu bar, then select **Settings Migrator**.



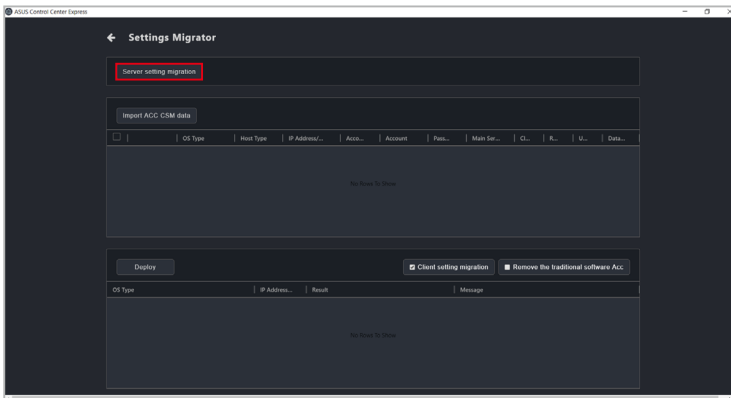
---

The screenshots in this section are for reference only.

---

### 6.1.1 Importing configurations of ACC CSM server

1. Click on **Server setting migrator** located at the top of the screen,



- Enter the required information into the fields, then click on **Save**.

Enter server information

ACC CSM server IP

ACC CSM account

ACC CSM password

Sync metadata

Sync general setting

Sync SMTP setting

Sync rule management

Sync account setting

<b>ACC CSM server IP</b>	IP address of the ACC CSM server you wish to import		
<b>ACC CSM account</b>	The administrator account of the ACC CSM server you wish to import		
<b>ACC CSM password</b>	The password for the administrator account of the ACC CSM server you wish to import		
<b>Sync metadata</b>	Check to import metadata fields of ACC CSM		
<b>Sync general setting</b>	<p>Check to import specific general settings of ACC CSM. These settings include:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; vertical-align: top;"> <u>MainServer Settings</u> <ul style="list-style-type: none"> <li>- Web page refresh timer</li> <li>- Check for updates timer</li> </ul> </td> <td style="width: 50%; vertical-align: top;"> <u>Agent Configuration</u> <ul style="list-style-type: none"> <li>- Hardware sensor interval</li> <li>- Utilization time interval</li> <li>- Agent response timer</li> </ul> </td> </tr> </table>	<u>MainServer Settings</u> <ul style="list-style-type: none"> <li>- Web page refresh timer</li> <li>- Check for updates timer</li> </ul>	<u>Agent Configuration</u> <ul style="list-style-type: none"> <li>- Hardware sensor interval</li> <li>- Utilization time interval</li> <li>- Agent response timer</li> </ul>
<u>MainServer Settings</u> <ul style="list-style-type: none"> <li>- Web page refresh timer</li> <li>- Check for updates timer</li> </ul>	<u>Agent Configuration</u> <ul style="list-style-type: none"> <li>- Hardware sensor interval</li> <li>- Utilization time interval</li> <li>- Agent response timer</li> </ul>		
<b>Sync SMTP setting</b>	Check to import the SMTP settings of ACC CSM		
<b>Sync rule management</b>	<p>Check to import notification rules of ACC CSM</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Imported notification rules will only be applied to ACC CSM client devices managed by ASUS Control Center Express.</p> </div>		
<b>Sync account setting</b>	<p>Check to import the accounts and roles of ACC CSM</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>The default account for ACC CSM cannot be imported.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Due to security reasons, the passwords for imported ACC CSM accounts will not be imported to ASUS Control Center Express. The password for these accounts will be defaulted to “admin”, ensure to edit and change these passwords to the correct administrator passwords of the imported client devices.</p> </div>		

## 6.1.2 Deploying ACCE agents to ACC CSM devices

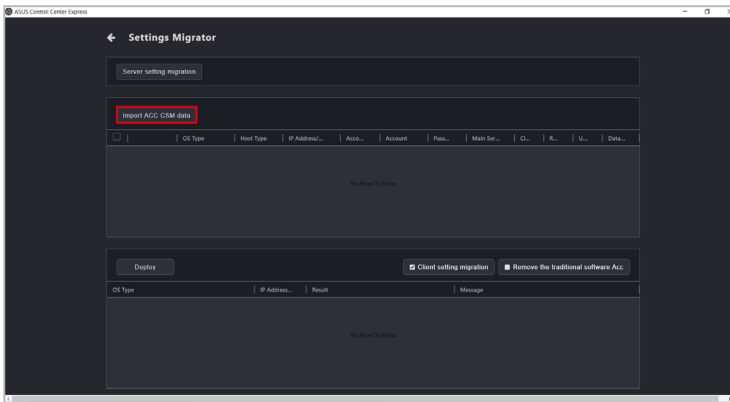
You can import the client device information of ACC CSM which will allow you to deploy ASUS Control Center Express agents to their ACC CSM client devices.

1. Before deploying ASUS Control Center Express agents to ACC CSM devices, please ensure you have registered CSM license keys for ACC CSM product devices.



For more information on registering CSM license keys, please refer to **7.1.4 License Key**.

2. Click on **Import ACC CSM data**.

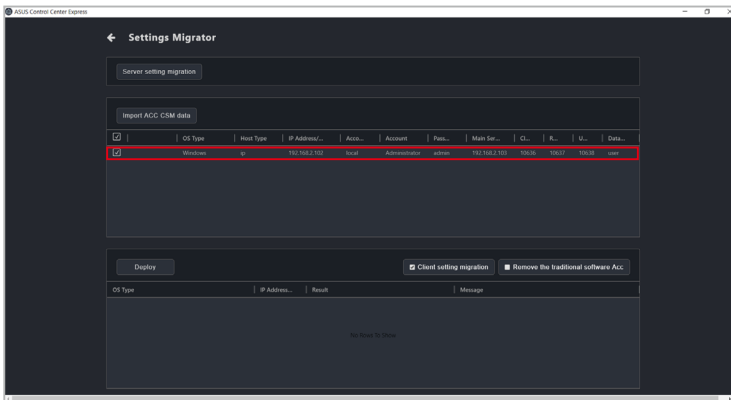




2. Enter the required information into the fields, then click on **Save**.

<b>ACC Express server IP</b>	IP address of ASUS Control Center Express server
<b>ACC CSM server IP</b>	IP address of the ACC CSM server you wish to import
<b>ACC CSM account</b>	The administrator account of the ACC CSM server you wish to import
<b>ACC CSM password</b>	The password for the administrator account of the ACC CSM server you wish to import

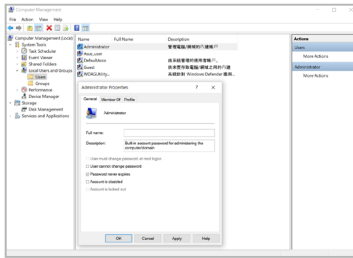
3. The data of client devices managed by ACC CSM should be imported and appear in the devices block.



4. Due to security reasons, the administrator passwords for imported ACC CSM client devices will be defaulted to “admin”. Double click on the imported client devices and change the password to the administrator password of the client device, then click on **Save**.



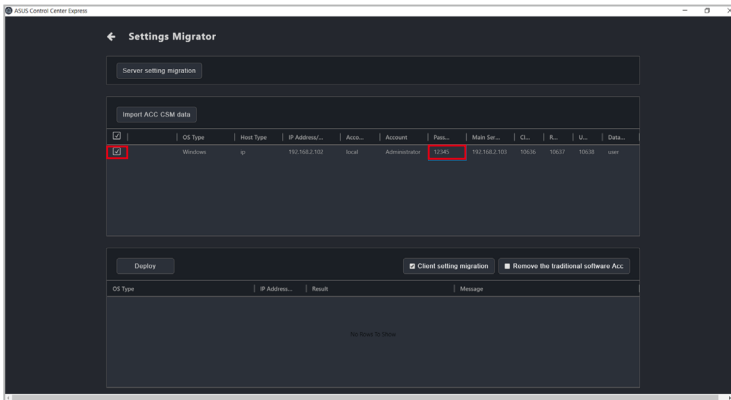
Ensure the Administrator account of the client is enabled and has a password set. (Windows disables the Administrator account by default, to enable the account click on the Windows button from the Desktop > **Windows Administrative Tools > Computer Management > System Tools > Local Users and Groups > User > Administrator**, then uncheck the **Account is disabled** field)



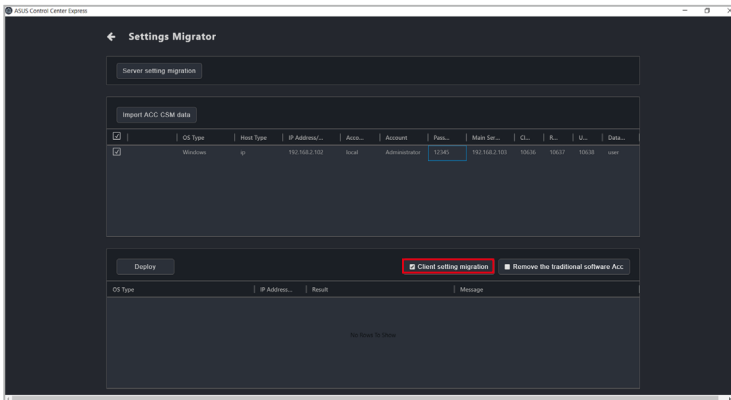
Dialog box titled "Edit Target Host" with the following fields and options:

- Main Server: 192.168.2.103
- OS Type:  Windows
- Host Type:  IP Address  Host Name
- Host Port: 10636
- Account Type:  Local  Domain
- Account: Administrator
- Password: admin (highlighted with a red box)
- Remote: 10637
- Undeploy: 10638
- Buttons: Cancel, Save (highlighted with a red box)

5. Ensure you have changed the administrator password of the client devices you wish to deploy ASUS Control Center Express agents to, then select those devices.



6. (optional) Check **Client setting migration** to import the ACC CSM client settings and data for the selected devices when you deploy. Please refer to the table below for more information on the client settings and data **Client setting migration** will import.

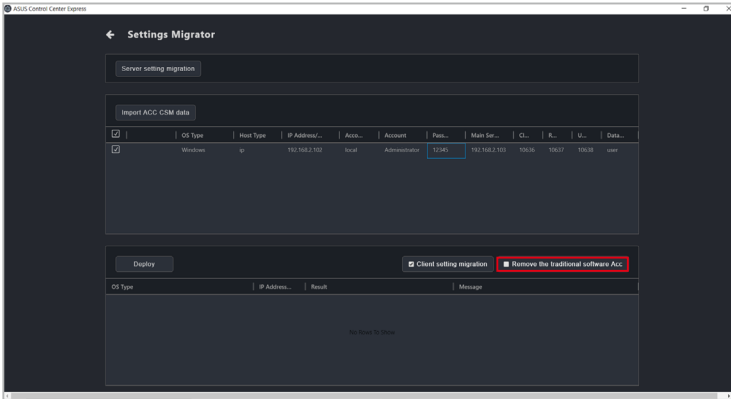


<b>Utilization</b>	CPU threshold values
	DIMM threshold values
	Partition threshold values
	Network threshold values
<b>Control</b>	<b>Enable/Disable Regedit</b> setting
	<b>USB Storage Device</b> setting
<b>Event log</b>	Event log information on the device
<b>Scheduled tasks</b>	<b>Power Control</b> related scheduled tasks
	<b>Service Control</b> related scheduled tasks
	<b>Software Dispatch</b> related scheduled tasks
	<b>Security Control</b> related scheduled tasks
	<b>BIOS Cache</b> related scheduled tasks

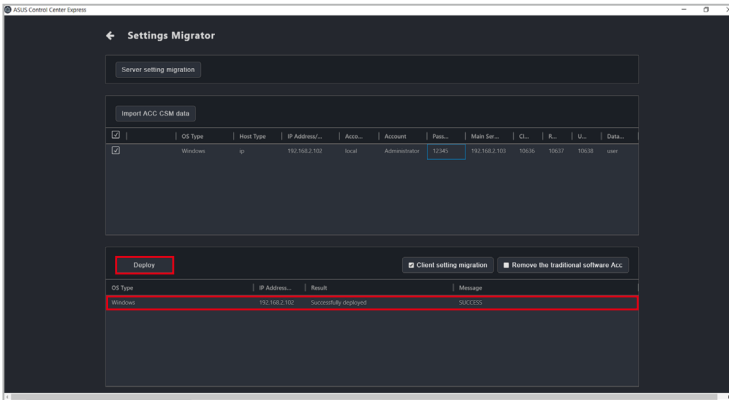


If there are imported Scheduled tasks on devices which do not have ASUS Control Center Express agents deployed yet, tasks relating to these devices will be added to the Task Scheduler once ASUS Control Center Express agents have been deployed to these devices.

- (optional) Check the **Remove the traditional software Acc** box to remove any previous versions of ASUS Control Center agents installed on the selected client devices when deploying new agents.



- Click on **Deploy** and wait for the agent deployment to be completed. Once the process is completed, you may view the deploy status below.





# Chapter 7

This chapter describes the User and ASUS Control Center Express settings.

# Account & General Settings

## 7.1 Settings menu

You can set the general settings such as configuring **SMTP Settings**, **Rule Management**, **General Configurations**, or add more **License** keys.

To access **Settings**, click on  located at the top right menu bar.



The information entered in this section is for reference only.

### 7.1.1 SMTP Settings

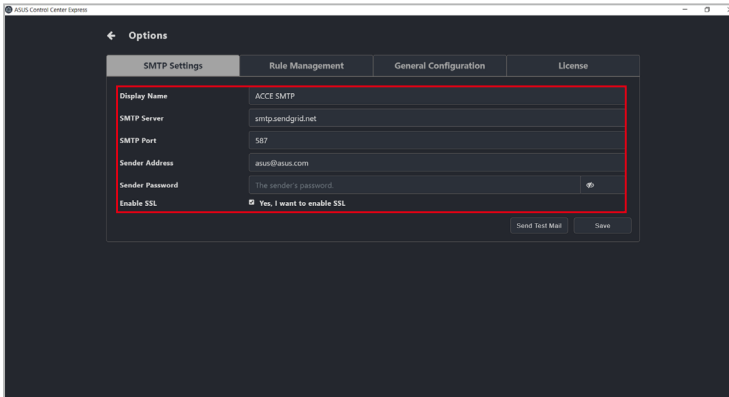
Set up the SMTP (Simple Mail Transfer Protocol) for ASUS Control Center Express to allow feedback on system failures and alerts to be sent via email to the system administrator.

#### To set up the SMTP Server



The settings entered may vary depending on the service provider, please refer to the information provided by your service provider.

1. Fill in and check the required fields.



<b>Display Name</b>	The name of this SMTP setting. The display name will not appear on sent emails
<b>SMTP Server</b>	The SMTP server responsible for collecting and sending emails
<b>SMTP Port</b>	Service port for SMTP. Common ports used are 25 (SMTP former default port), 465 (encrypted SMTP), and 587 (new SMTP default)
<b>Sender Address</b>	The email of the ACCE notification sender. This email address must exist within the SMTP Server service
<b>Sender Password</b>	The password for the ACCE notification email sender
<b>Enable SSL</b>	Enables mail sent or forwarded through this SMTP server to be SSL encrypted



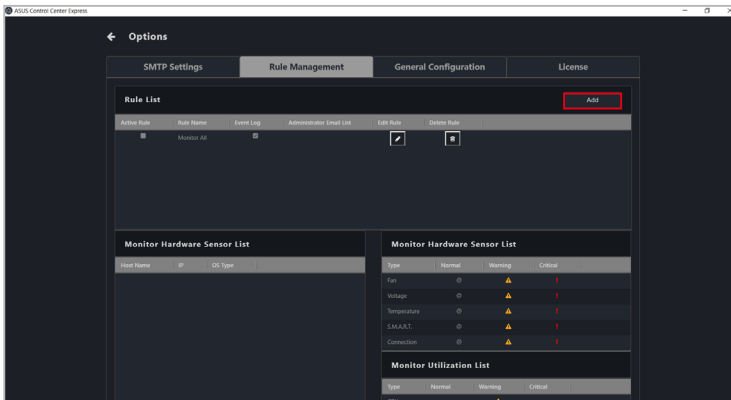
- (optional) Click on **Send Test Mail**, then enter an email and click **Send** to receive the test mail allowing you to check the status of the SMTP. If the SMTP is functioning properly, you should receive an email.
- Click **Save** to save the changes made.

## 7.1.2 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.

### Adding a new rule

- Click on **Add**.



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



- You may use the Search box to search and filter devices according to the keywords you enter. Click **Clear** to clear any search filters applied.
- To view more column items in the **Host List**, click on **Options**, then check the metadata item you wish to display and click on **Save**.
- Click **Select All** to select all devices in the **Host List**.

**Edit Rule**

Step 1: Assign the rule name and select the hosts.

**Rule Name**  
Monitor Pro WS X57-ACE

**Host List**

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

Select All

	Host Name	OS Information	IP Address
<input type="checkbox"/>	DESKTOP-8GF7595	Windows	192.168.0.15
<input type="checkbox"/>	DESKTOP-7Z7HB9M	Windows	192.168.0.16
<input checked="" type="checkbox"/>	DESKTOP-VKJGCR	Windows	192.168.0.10

**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**.

**Add Rule** ✕

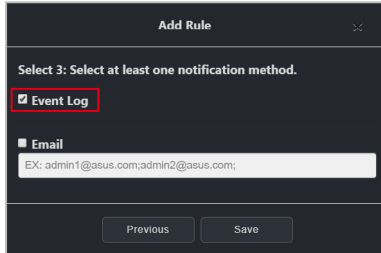
Step 2: Select the hardware sensor or utilization type and status.

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

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

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 dark-themed 'Add Rule' dialog box. At the top, it says 'Add Rule' with a close button. Below that, it says 'Select 3: Select at least one notification method.' There are two options: 'Event Log' with a checked checkbox and a red border around it, and 'Email' with an unchecked checkbox. Below the 'Email' option is a text input field containing 'EX: admin1@asus.com;admin2@asus.com;'. At the bottom are 'Previous' and 'Save' buttons.

- Email  
The notification is sent to the entered email addresses.



---

Ensure to set up the SMTP server settings before using the email function. For more information please refer to **7.1.1 SMTP Settings**.

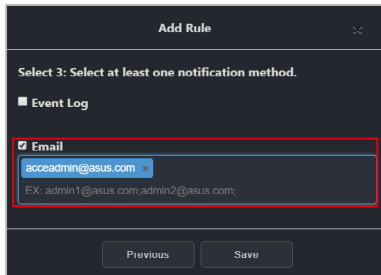
---



---

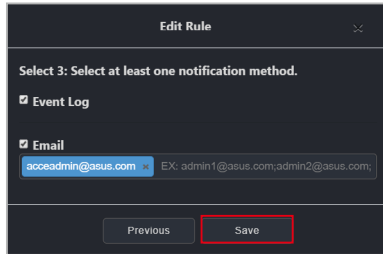
When entering multiple emails, press <Enter> after each email to separate the emails.

---

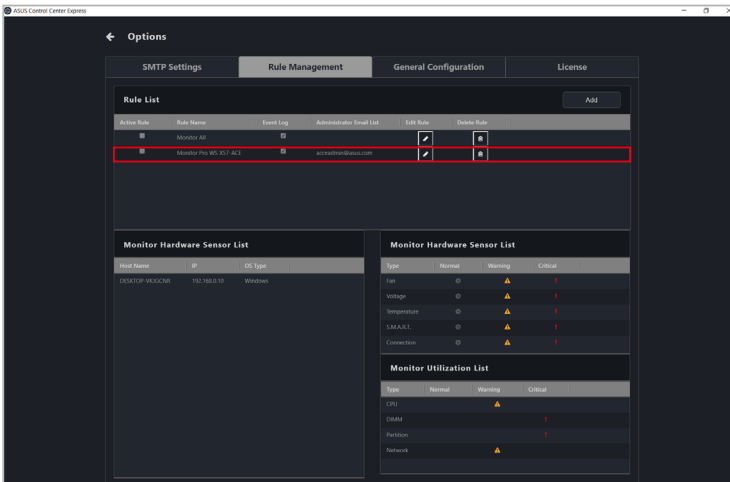


The screenshot shows the same 'Add Rule' dialog box. The 'Event Log' option is now unchecked, and the 'Email' option is checked. A dropdown menu is open for the 'Email' option, showing 'aaceadmin@asus.com' with a red border around the entire 'Email' section. Below the dropdown is the same text input field with the example email addresses. 'Previous' and 'Save' buttons are at the bottom.

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




Your newly added rule should appear 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 **Monitor Hardware Sensor List**, and the list of hardware and utilizations being monitored in the **Monitor Hardware Sensor List** and **Monitor Utilization List**.

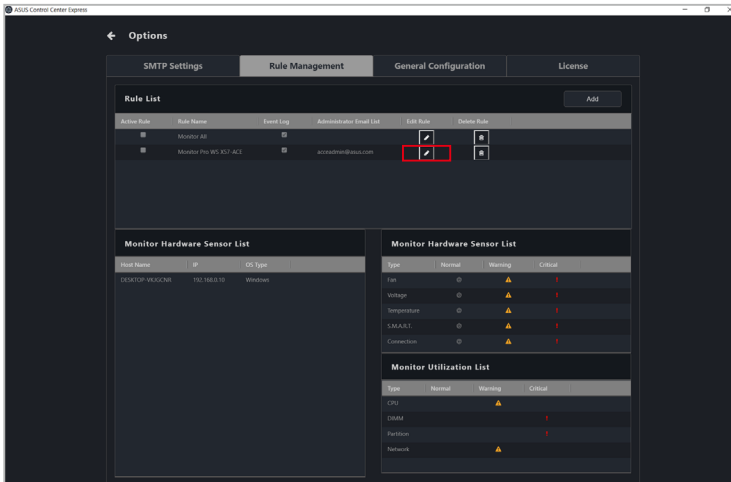


## To edit a notification rule:




Use the edit function to add new devices or devices which have been re-deployed to the notification rule.

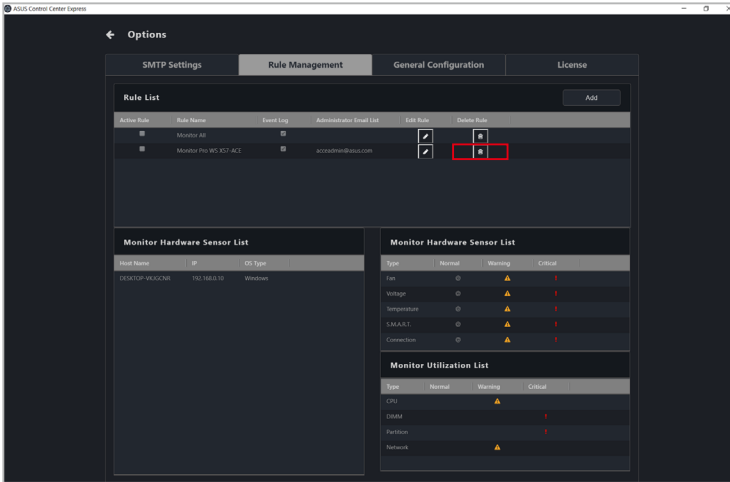
1. Select a rule in the **Rule List** you wish to edit, then click on  in the **Edit Rule** column.



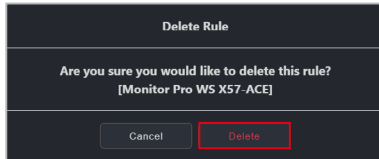
2. Follow steps 2 to 4 edit your Rule, then click **Save** to save the changes made.

## To delete a notification rule:

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

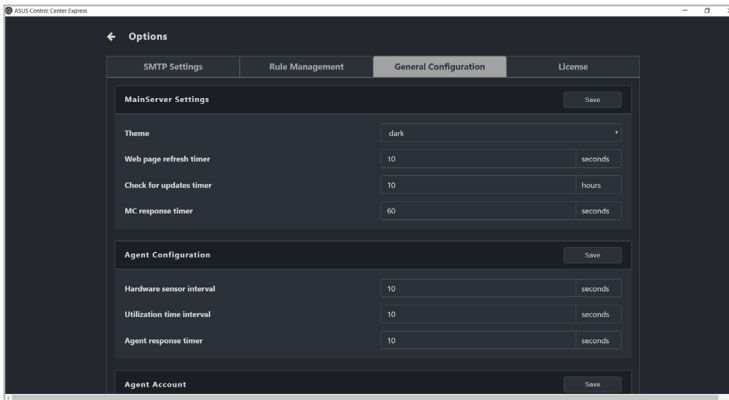


2. Click **Delete** to delete the rule.



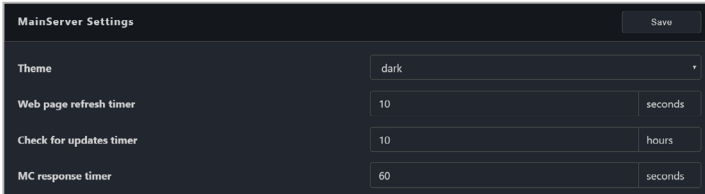
## 7.1.3 General Configuration

The General configurations allows you to configure different settings for the Main Server and agents. Scroll down to view more options.



### MainServer Settings:

Configure items for the main ASUS Control Center Express server. Click on **Save** to save the changes made.

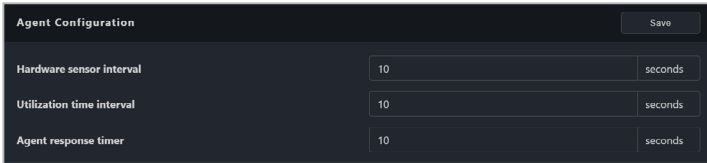


<b>Theme</b>	Select a color theme ( <b>dark</b> , <b>acc_csm</b> , <b>acc</b> ) for your main server
<b>Web page refresh timer</b>	Set the time interval in seconds between each refresh of all webpages of the main server
<b>Check for updates timer</b>	Set the time interval in hours between each main server update check
<b>MC response timer</b>	Set the time interval for management controller (RTL8117) to return status updates to the main server



## Agent Configuration:

Configure the agent sensor intervals and response times. Click on **Save** to save the changes made.

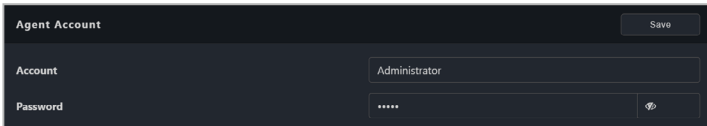


The image shows a dark-themed configuration window titled "Agent Configuration". It contains three rows of settings, each with a label, a text input field, and a unit dropdown menu. The "Hardware sensor interval" is set to "10" with "seconds" selected. The "Utilization time interval" is also set to "10" with "seconds" selected. The "Agent response timer" is set to "10" with "seconds" selected. A "Save" button is located in the top right corner.

<b>Hardware sensor interval</b>	Set the time interval in seconds for the hardware sensor to return sensor vaules
<b>Utilization time interval</b>	Set the time interval in seconds for the utilization sensor to return sensor vaules
<b>Agent response timer</b>	Set the time interval in seconds for the agent to query tasks from the main server

## Agent Account:

Set the default administrator account and password for client devices if no administrator account and password were entered when deploying agents. Click on **Save** to save the changes made.



The image shows a dark-themed configuration window titled "Agent Account". It contains two rows of settings. The "Account" field has the text "Administrator" entered. The "Password" field has "\*\*\*\*\*" entered and a toggle icon to its right. A "Save" button is located in the top right corner.

<b>Account</b>	Set the default administrator account
<b>Password</b>	Set the default administrator password

## Agent Port:

Configure the ports for the agent and main server to use when connecting to the client device. Click on **Save** to save the changes made.



We recommend using the default values as this will require no further adjustments to the client device's firewall settings.

Agent Port		Save
HTTPS	10636	
Remote	10637	
Undeploy	10638	

<b>HTTPS</b>	Set the port for webpage access
<b>Remote</b>	Set the port for remote desktop
<b>Undeploy</b>	Set the port for removing the agent from clients

## Appearance Configuration:

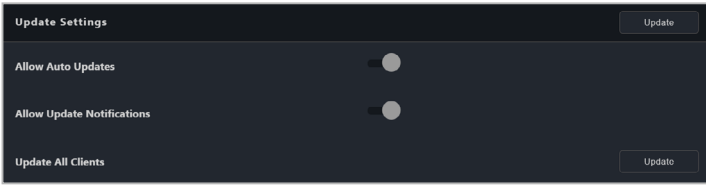
View the version of the main server, as well as customize the banner logo. Click on **Save** to save the changes made, or click on **Reset** to return to the default banner logo.

Appearance Configuration		Save	Reset
Version	1.2.1		
Banner Logo	Choose file <input type="button" value="Browse"/>		
Ignore MC Descriptor	<input type="checkbox"/>		

<b>Version</b>	Displays the version of the main ASUS Control Center Express server
<b>Banner Logo</b>	Click <b>Browse</b> to select and upload a new banner logo. The banner logo can be viewed in the top left corner of the main dashboard overview
<b>Ignore MC Descriptor</b>	Enable or disable debug mode

## Update Settings:

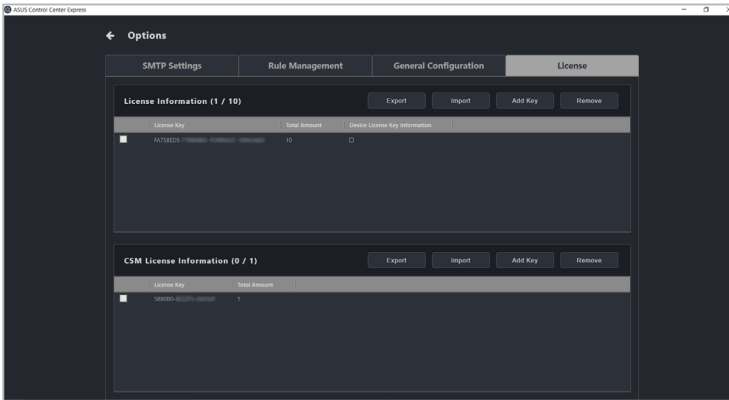
Configure the update settings for the main server and clients. Click on **Update** to save the changes made.



<b>Allow Auto Updates</b>	Enable / Disable auto updates for the main server
<b>Allow Update Notifications</b>	Enable / Disable notifications for new updates and update statuses.
<b>Update All Clients</b>	Click <b>Update</b> to begin updating all client agents

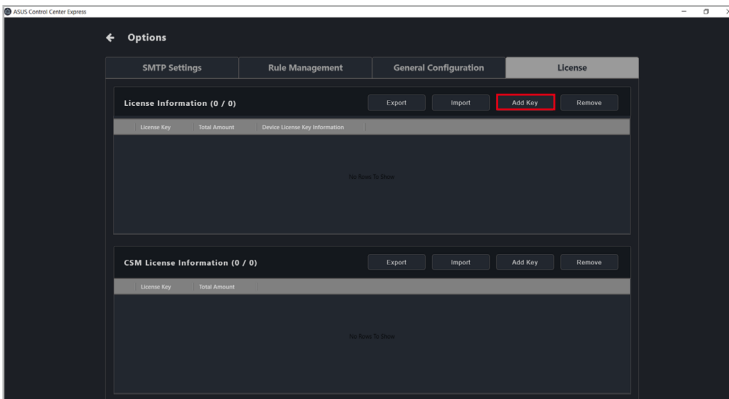
## 7.1.4 License

You may add or remove license keys in this menu. You may also import license information from previous versions of ACC.

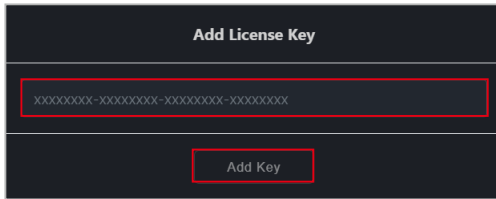


### To add a license key

1. Locate the License Key on the ASUS Control Center Express card bundled in your motherboard's giftbox.
2. Click on **Add Key**.

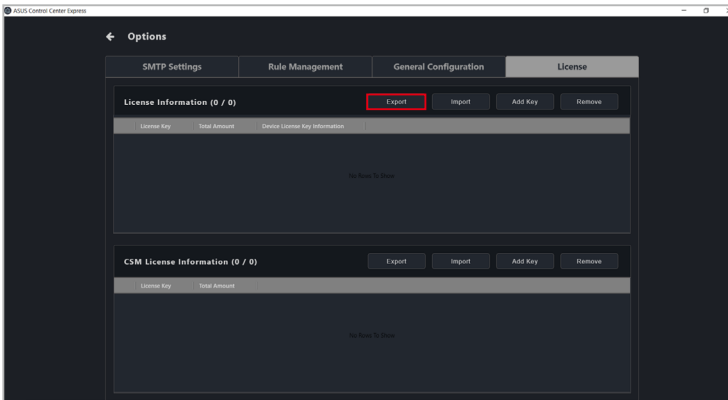


3. Key in the license key and then click on **Add Key** to register a license for a single device on ASUS Control Center Express.

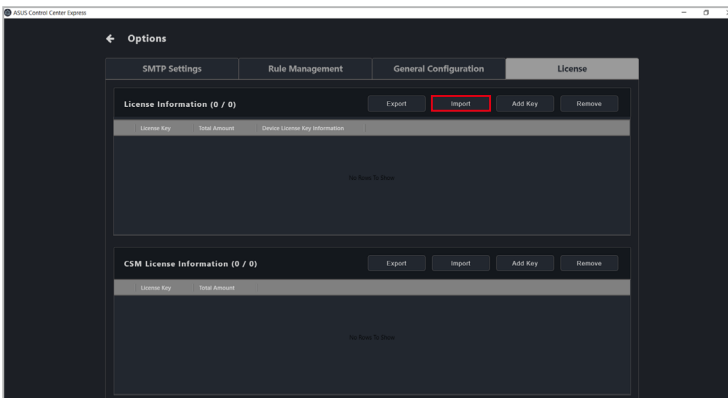


## To import multiple license keys

1. Click on **Export** to export a template .csv file, then enter the required information in the .csv file.

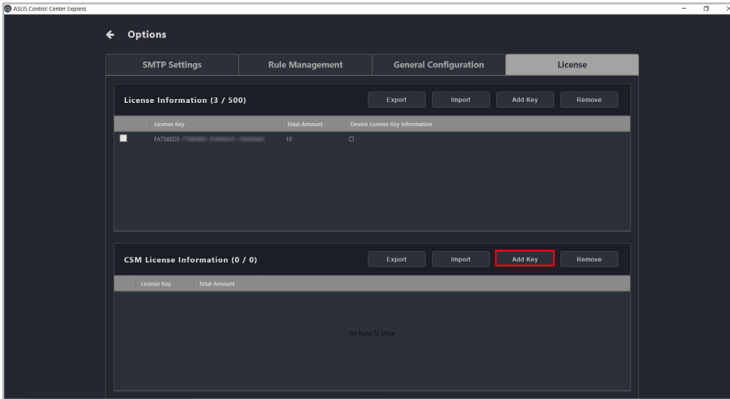


2. Click on **Import** to import your edited .csv file.

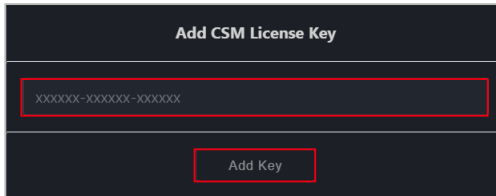


## To add an ACC CSM license key

1. Prepare your ACC CSM license key(s).
2. Click on **Add Key**.

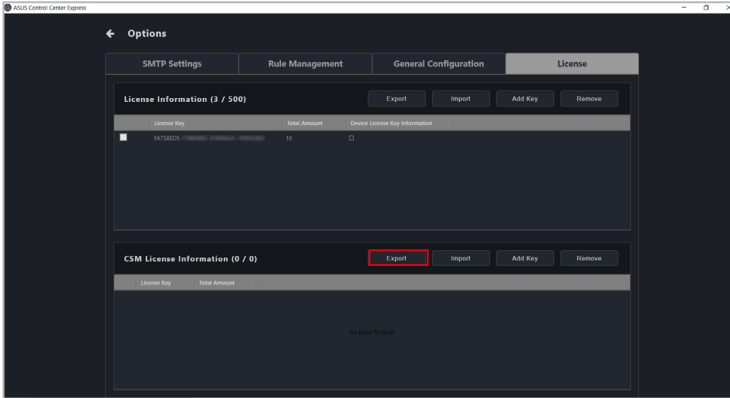


3. Key in the license key and then click on **Add Key** to register a license for a single device on ASUS Control Center Express.

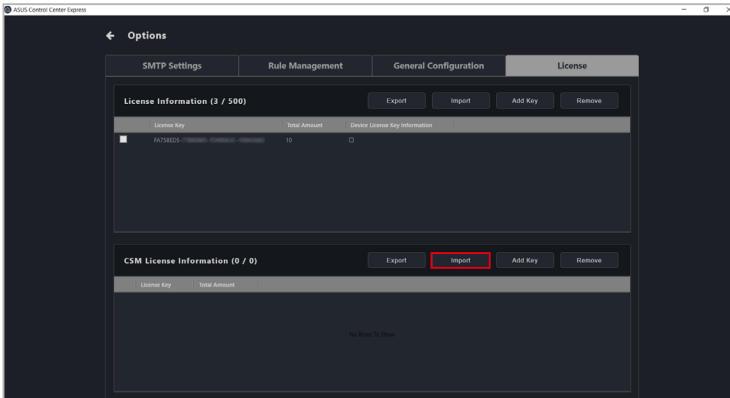


## To import multiple ACC CSM license keys

1. Click on **Export** to export a template .csv file, then enter the required information in the .csv file.

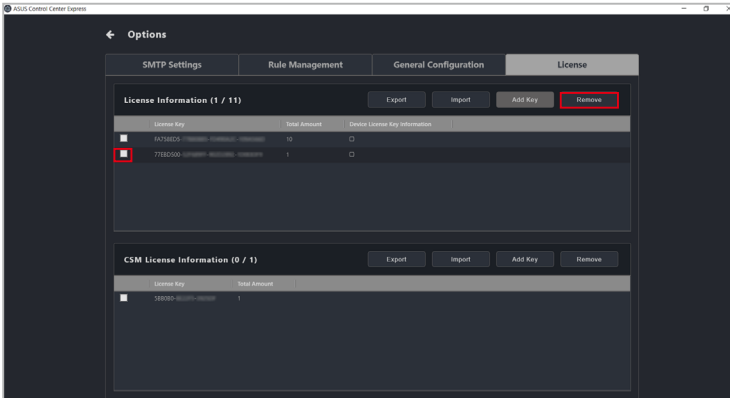


2. Click on **Import** to import your edited .csv file.



## To remove a license key

1. Select the license key(s) or ACC CSM license key(s) you would like to remove, then click **Remove**.





## 7.2 Account menu

The Account menu allows you to manage accounts for ASUS Control Center Express, or migrate ACC CSM settings to ASUS Control Center Express. You can also scan a QR code for easy access to the web version of ASUS Control Center Express or provide feedback to the developers.

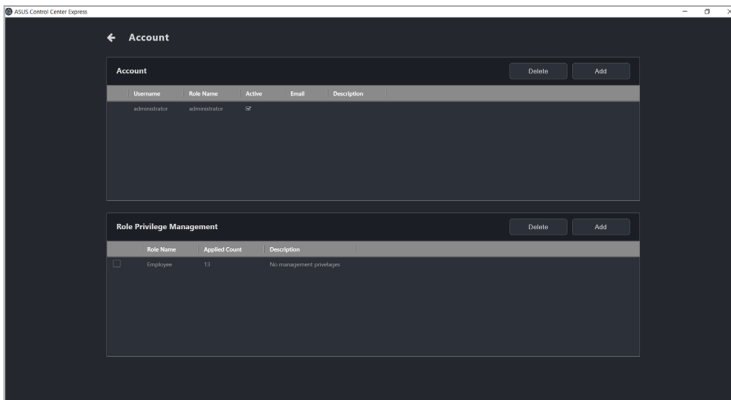


- The information entered in this section is for reference only.
- For more information on migrating ACC CSM settings, please refer to **Chapter 6 Settings Migrator**.

### 7.2.1 Account Settings

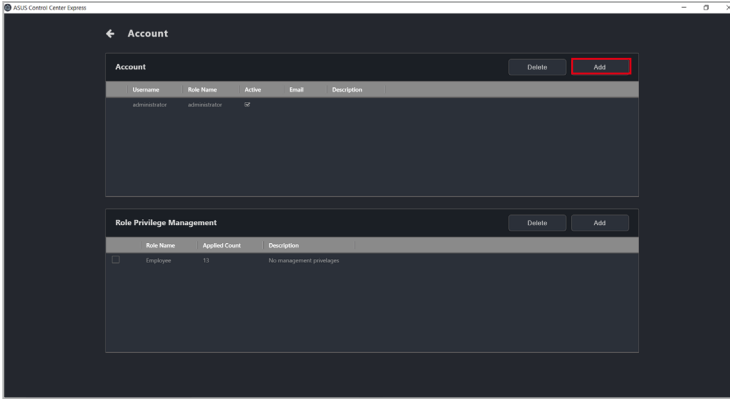
Account settings displays all user accounts on ASUS Control Center Express, and allows you to add, edit, or delete user accounts.

To access **Account Settings**, click on  located at the top right menu bar, then select **Settings**.




## To add an account

1. Click on **Add**.

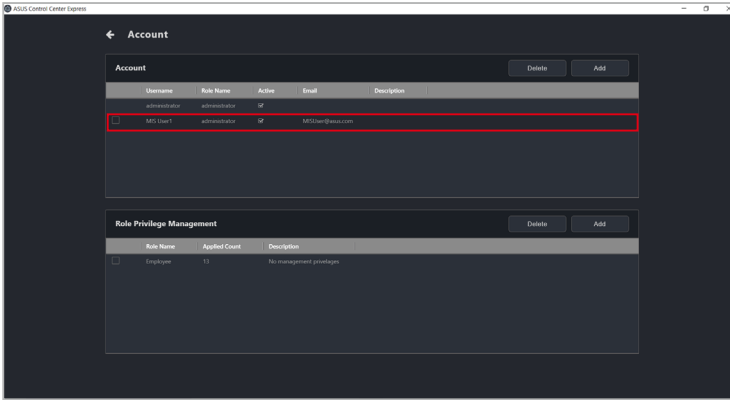


2. Enter the required information into the fields, and check **Enable the account** in the **Active** field to enable this account, then click on **Save** to add this new account.

<b>Username</b>	Username of the account
<b>Password</b>	Password for the account
<b>Confirm Password</b>	Confirm the password for the account
<b>Email</b>	Email associated with the account
<b>Role Name</b>	The role assigned to the account will determine what privileges it has   To add or modify roles, please refer to the <b>Role Privilege Management</b> .
<b>Description</b>	Enter a brief description on the account
<b>Active</b>	Check to enable the account

## To edit an account

1. Click on the account you wish to modify.



2. You may edit the account details, click on **Update** once you are finished.

The 'Edit Account' dialog box is shown with the following fields and options:

- Username: MIS User 1
- New password: e.g. \*\*\*\*\*
- Confirm Password: e.g. \*\*\*\*\*
- Email: MISUser@asus.com
- Role Name: administrator (dropdown menu)
- Description: About this account...
- Active:  Enable the account

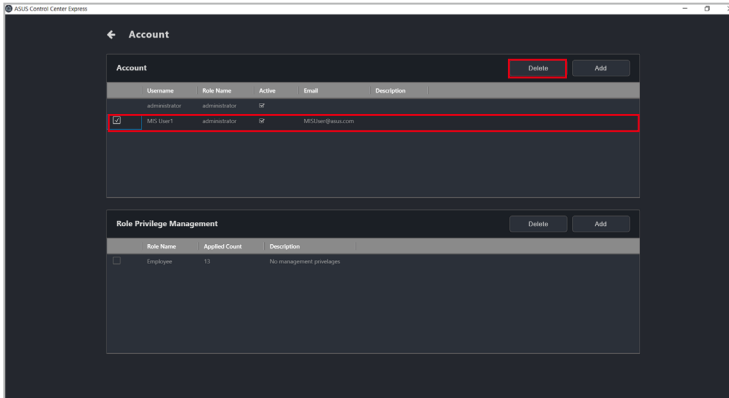
Buttons: Cancel, Update (highlighted with a red border)

## To delete an account

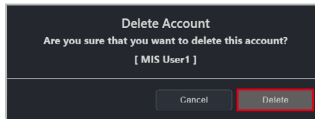
1. Check the account(s) you wish to delete, then click **Delete**.



The administrator account for ASUS Control Center Express cannot be deleted.




2. Confirm that you wish to delete the account(s), then click **Delete**.



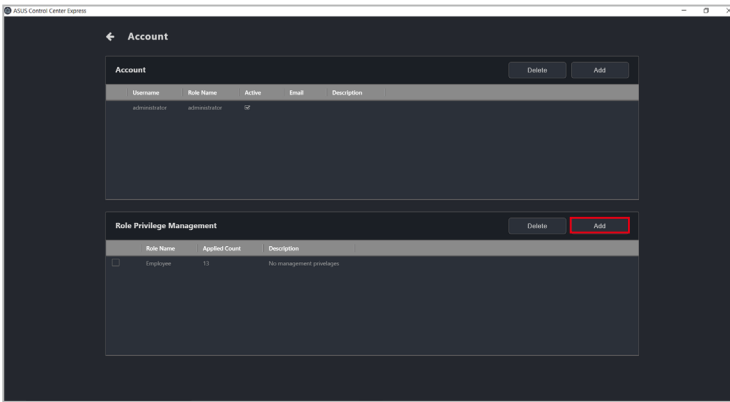
## 7.2.1 Role Privilege Management

The Role Privilege Management displays all roles on ASUS Control Center Express, and allows you to add, edit, or modify permissions of different roles that you may assign to users.

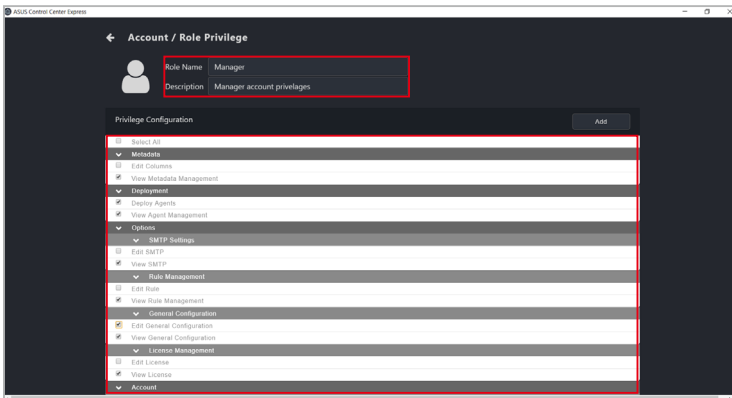
To access **Role Privilege Management**, click on  located at the top right menu bar, then select **Settings**.

### To add a new role

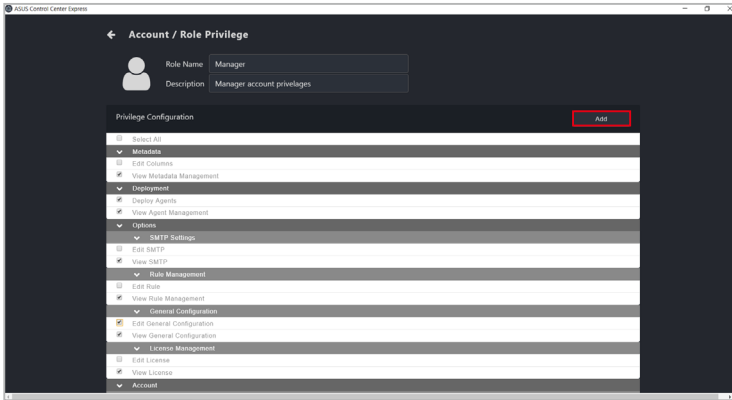
1. Click on **Add**.



2. Enter the **Role Name** and **Description** for the role, then check the privileges you want to assign to this role in the Privilege Configuration block.

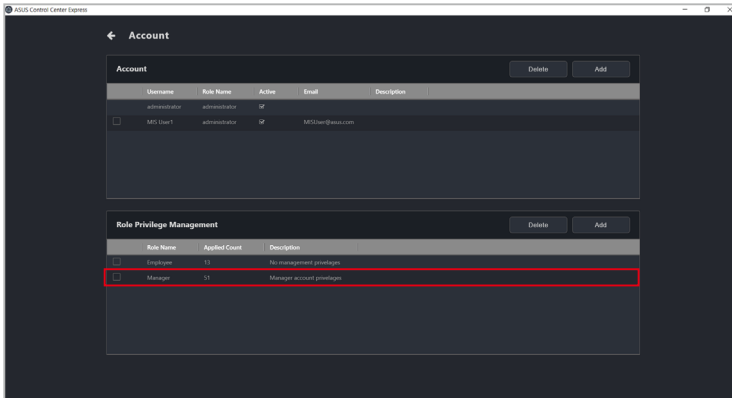


3. Click **Add** to add the new role.

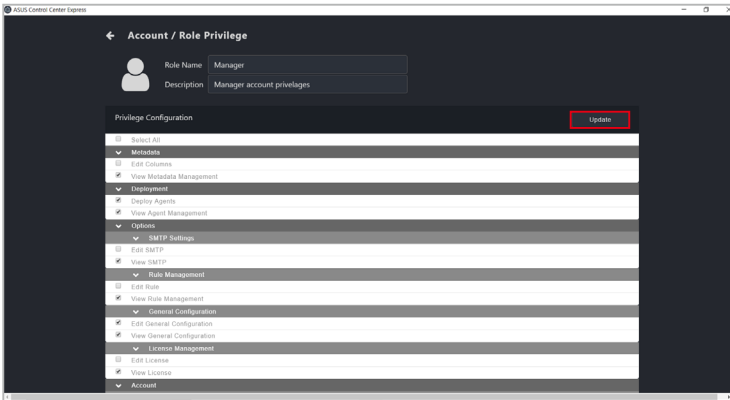


**To edit a role**

1. Click on the role you wish to edit.

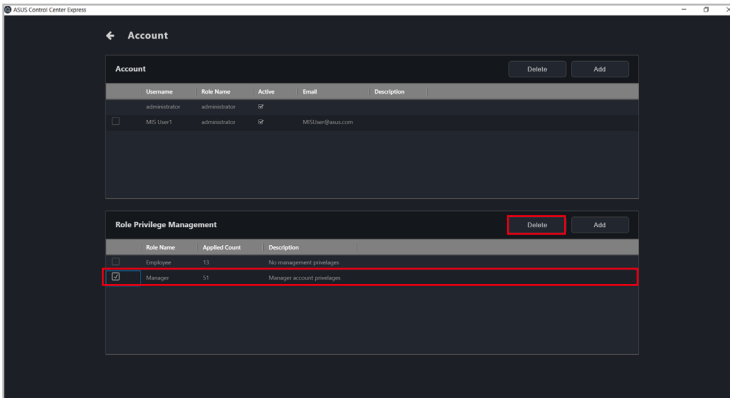


- You may edit the **Role Name** and **Description**, or modify the **Privilege Configuration**. Click on **Update** once you are finished.



## To delete a role

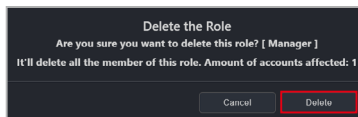
- Check the role(s) you wish to delete, then click **Delete**.



- Confirm that you wish to delete the account(s), then click **Delete**.




If there are accounts associated with the role(s) you wish to delete, the accounts will also be deleted when you delete the role(s). The pop up message will notify you of the amount of accounts affected by this action.



## 7.3 QR Code

You can scan the QR code to quickly access the web version of ASUS Control Center Express on your mobile device.

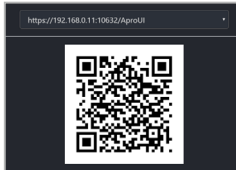
To access **QR Code**, click on  located at the top right menu bar, then select **QR Code**.



---


The illustration in this section is for reference only.

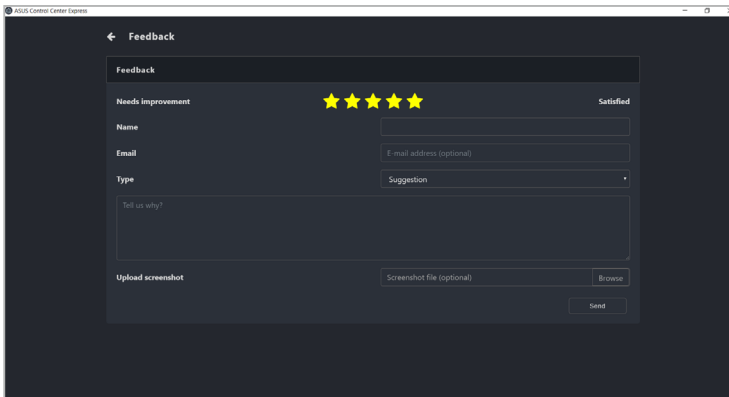
---



## 7.4 Submit Feedback

You can provide feedback to the developers using the Feedback function. You may also upload screenshots if required.

To submit feedback, click on  located at the top right menu bar, then select **Feedback**.

A screenshot of the "Feedback" form in the ASUS Control Center Express. The form is titled "Feedback" and includes a "Needs Improvement" section with a five-star rating system (all five stars are yellow). Below the rating is a "Satisfied" checkbox. The form contains several input fields: "Name", "Email", "E-mail address (optional)", "Type", and "Suggestion". There is also a text area labeled "Tell us why?". At the bottom, there is an "Upload screenshot" section with a "Screenshot file (optional)" input field and a "Browse" button. A "Send" button is located at the bottom right of the form.