ASUS Control Center Express

User Manual

Version: 01.05

E22036
Revised Edition V5
September 2023

Copyright © 2023 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 of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

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

Contents

About this guide x

Chapter 1: Getting Started

1.1 Setting up 1-2

1.1.1 Installing ASUS Control Center Express (ACCE) 1-2

1.1.2 Logging in to ASUS Control Center Express 1-8

1.1.3 Changing the account password 1-9

1.1.4 Activating your license key 1-10

1.1.5 Changing languages 1-10

1.1.6 Updating ASUS Control Center Express 1-11

1.2 Main menu overview 1-15

Chapter 2: Main Menu Overview

2.1 Dashboard overview 2-2

2.1.1 Switching sensor views 2-3

2.1.2 Event Log 2-4

2.2 Device overview 2-5

2.2.1 Filtering client devices 2-6

2.2.2 Redirecting to device information 2-8

2.2.3 Customizing device list metadata 2-8

2.2.4 Export device list 2-9

2.2.5 Creating client device groups 2-9

2.2.6 Using shortcut functions 2-11

2.3 Customizing the graphic view 2-18

2.3.1 Customizing the Graphic view for the first time 2-18

2.3.2 Using the Graphic view menu items 2-20

2.3.3 Using the client device icons 2-21

2.4 Mission Center 2-22

2.4.1 Using the Mission Center 2-22

2.4.2 Mission Center tasks 2-24

Contents

Chapter 3: Deploy Management

3.1 Agent Management overview 3-2

3.2 Deploying agents 3-5

3.2.1 Automatically scanning and deploying to devices 3-5

3.2.2 Scanning an IP range 3-7

3.2.3 Adding and deploying to devices 3-9

3.2.4 Editing device information 3-11

3.2.5 Installing agents manually 3-12

3.2.6 Installing Agents in silent mode 3-15

3.2.7 Upgrading or repairing agents 3-17

3.2.8 Setting up a Windows 7 deployment environment 3-22

3.3 Removing agents 3-24

3.3.1 Removing agents through main server 3-24

3.3.2 Removing manually installed agents 3-25

3.4 Client Agent Updater 3-26

3.4.1 Updating agents 3-27

Contents

Chapter 4: Device Information

4.1 Device Information Overview 4-2
4.2 Operating Status 4-4
4.3 Hardware Sensor (software) 4-5
4.4 Utilization 4-8
4.5 Inventory (Software) 4-9
4.5.1 Disk Information 4-9
4.5.2 Asset Information 4-10
4.6 Software 4-11
4.6.1 Application tab 4-11
4.6.2 Processes tab 4-12
4.6.3 Services tab 4-12
4.6.4 Environment tab 4-13
4.7 Control (software) 4-14
4.8 Event Log 4-15
4.8.1 Monitor tab 4-15
4.8.2 Application tab 4-16
4.8.3 System tab 4-17
4.8.4 Security tab 4-18
4.9 Remote Desktop (General) 4-19
4.10 BIOS 4-21
4.10.1 BIOS Flash Management 4-21
4.10.2 BIOS Setting 4-28
4.11 Installer 4-30
4.12 Device Manager 4-33
4.13 System Restore 4-35
4.14 BitLocker 4-37

Contents

Chapter 5: Management Functions

5.1 Metadata Management 5-2

5.1.1 Adding metadata fields 5-2

5.1.2 Removing metadata fields 5-4

5.1.3 Updating the metadata manually 5-5

5.1.4 Updating the metadata using a batch update 5-6

5.2 Software Management 5-8

5.2.1 Software Dispatch 5-8

5.2.2 Software Pool 5-11

5.2.3 Software Information 5-17

5.2.4 Software Blacklist 5-18

5.2.5 Installer 5-19

5.2.6 Software Rule Management 5-20

5.3 Task Scheduler 5-30

5.3.1 Task scheduler calendar overview 5-30

5.3.2 Setting a new task 5-31

5.3.3 Editing a task 5-41

5.3.4 Deleting a task 5-42

5.4 OOB Control 5-43

5.4.1 Setting remote management controller credentials 5-43

5.4.2 Using OOB - Control functions 5-52

5.5 Management Control Overview 5-56

5.5.1 Scanning for devices 5-56

5.5.2 Managing devices with multiple remote management controllers 5-57

Contents

5.6 Management Control Information Overview 5-59

5.7 DASH Management Control Information 5-60

5.7.1 Hardware Sensor 5-61

5.7.2 Inventory 5-62

5.7.3 Control 5-62

5.7.4 USB Redirection 5-66

5.7.5 Network 5-67

5.7.6 Text Redirection 5-69

5.7.7 Account Management 5-70

5.7.8 Role privileges 5-71

5.7.9 Event Log 5-74

5.8 RTL8117 Management Control Information 5-75

5.8.1 Hardware Sensor 5-76

5.8.2 Inventory 5-77

5.8.3 Control 5-78

5.8.4 Remote Desktop 5-81

5.8.5 USB Redirection 5-84

5.8.6 Smart BIOS 5-85

5.8.7 Firmware Update 5-89

5.8.8 Trust Zone 5-90

5.8.9 Event Log 5-95

5.9 vPro Management Control Information 5-96

5.9.1 Inventory 5-97

5.9.2 Control 5-100

5.9.3 Remote Desktop 5-101

5.9.4 Storage Redirection 5-103

5.9.5 Power 5-106

5.9.6 Network 5-109

5.9.7 Wake-up Alarm 5-119

5.9.8 System Record 5-122

5.9.9 Certificate 5-124

5.10 BMC Management Control Information 5-129
5.10.1 Hardware Sensor 5-131
5.10.2 Inventory 5-131
5.10.3 Control 5-132
5.10.4 Remote Desktop 5-134
5.10.5 Smart BIOS 5-135
5.10.6 Firmware Update 5-140
5.10.7 Event Log 5-141
5.10.8 IPMI 5-141
5.10.9 IPMI Serial-over-LAN (SOL) 5-142
5.10.10 Settings 5-143
5.10.11 Configuration 5-159
5.10.12 FRU Information 5-160
5.10.13 Image Redirection 5-161
5.10.14 Platform Event Filters 5-162
5.10.15 BSOD Capture 5-162
5.10.16 Error Codes 5-163
5.11 Screen Broadcast 5-164
5.11.1 Setting up the broadcast environment 5-166
5.11.2 Adding a new Broadcast Room 5-169
5.11.3 Managing video playlists 5-173
5.11.4 Starting or stopping a broadcast 5-174
5.11.5 Editing an existing Broadcast Room 5-175

Chapter 6: Settings Migrator

6.1 Settings Migrator 6-2
6.1.1 Migrating configurations of ACC CSM server 6-2
6.1.2 Importing ACC CSM data 6-5
6.1.3 Deploying ACCE agents to ACC CSM devices 6-6

Chapter 7: Report Generator

7.1 Report Generator 7-2
7.1.1 Connection Report 7-2
7.1.2 Software Report 7-4
7.1.3 Hardware Report 7-6

Chapter 8: Account & General Settings

8.1 Options menu 8-2
8.1.1 SMTP Settings 8-2
8.1.2 Rule Management 8-3
8.1.3 General Configuration 8-10
8.1.4 License 8-16
8.2 Account menu 8-21
8.2.1 Account Settings 8-21
8.2.2 Role Privilege Management 8-24
8.3 QR Code 8-27
8.4 Submit Feedback 8-28
8.5 Mailbox 8-29
8.5.1 Setting the Mailbox notification 8-30
8.6 Backup and Restore 8-30
8.6.1 Managing data and settings in MySQL databases 8-31
8.6.2 Backing up data and settings in SQLite databases 8-35
8.6.3 Restoring data and settings in SQLite databases 8-36

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: Main Menu Overview**

   This chapter describes the functions available on the main control panel.

3. **Chapter 3: Deploy Management**

   This chapter describes how to automatically or manually deploy ASUS Control Center Express agents and remove agents, and updating agents.

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, task scheduler, 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: Report Generator**

   This chapter describes how to generate various reports on client devices.

8. **Chapter 8: 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

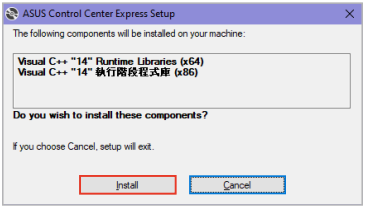
1.1 Setting up

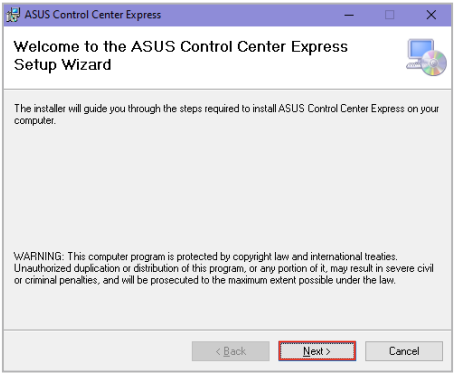
1.1.1 Installing ASUS Control Center Express (ACCE)

It is strongly recommended to backup your data and settings before updating ASUS Control Center Express. Refer to the **Backup and Restore** section of the **Account and General Settings** chapter for more information.

1. Please visit the product website of your ASUS product to download the ASUS Control Center Express installer.
2. Unzip the installation file, then execute Setup.exe. You should be guided to install vcredist_x64, vcredist_x86, database, and ASUS Control Center Express respectively.

- Ensure that Microsoft .NET Framework V4.6.1 or higher is installed before installing ASUS Control Center Express.
- 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.

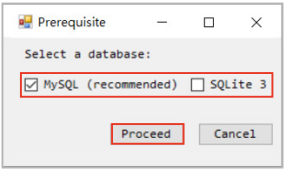




The illustrations in this section are for reference only and may differ between options selected. The steps in this section use MySQL as an example, if you wish to use another database, please follow the installation instructions for the database selected.

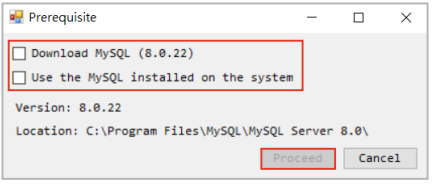
3. Select the database (**MySQL, SQLite 3**) you would like to install for ASUS Control Center Express, then click **Proceed**. For this example, we will select **MySQL**.

- We recommend selecting **MySQL** as the database for ASUS Control Center Express.
- Before installing the database, ensure the main server is connected to a public WAN with a stable connection.



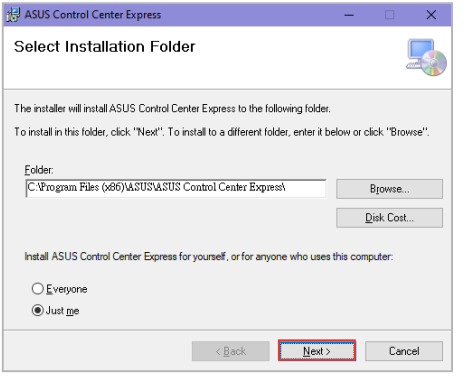
4. Read through the prerequisites then check **I Agree**, and click **Proceed**.

5. Select whether to download the MySQL installation files from the internet, or if you wish to use a preexisting MySQL installed on the system, then click **Proceed**.



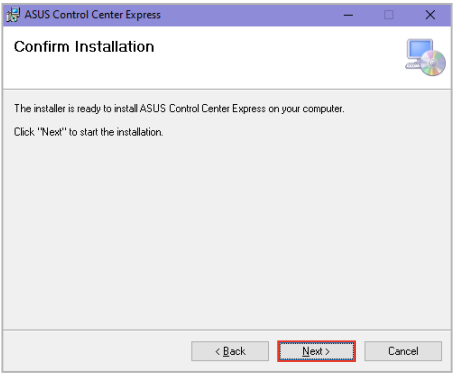
- Click on **Download MySQL** to download the MySQL installation files. After the download is completed, a manual installation will be required.
- Click on **Use the MySQL installed on the system** to automatically detect a preexisting MySQL already installed.

6. Once the database has been setup, the ASUS Control Center Express installation will begin.
7. Select the folder you would like to install ASUS Control Center Express to; we recommend using the default folder, then click **Next** once you have finished.



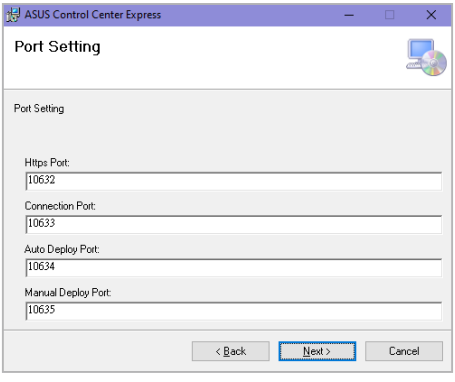
- Click on **Browse...** to select a new path to install ASUS Control Center Express.
- Click on **Disc Cost...** to view the server disk space and disk space required to install ASUS Control Center Express.

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



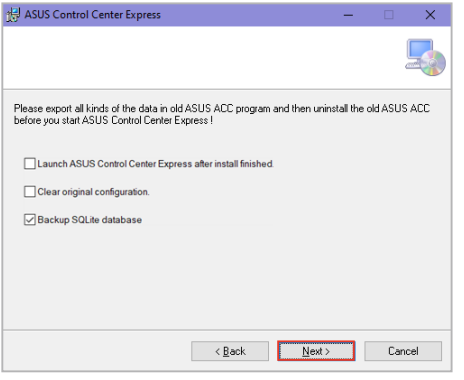
9. Once in the Port Setting page, you may adjust the default set ports if your working environment is already using a port that is displayed. Once you have finished adjusting the ports or if you wish to use the default ports, click on **Next**.

Https Port	Main ACCE server log in port.
Connection Port	Main ACCE server and client device connection port.
Auto Deploy Port	Main ACCE server auto deploy port.
Manual Deploy Port	Main ACCE server manual deploy port.
KVM Port	Main ACCE server OOB KVM port
Broadcast Port	Main ACCE server broadcasting port.
MySQL Port	Main ACCE server database port.
Indication	Main ACCE server alert notification function port.

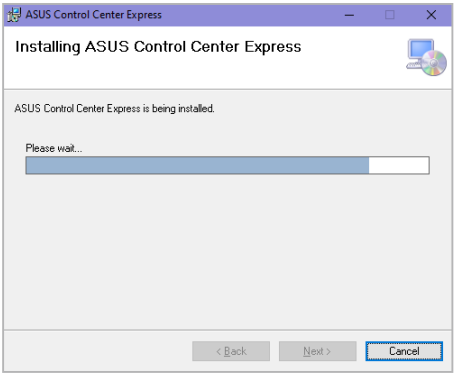


10. Select and check the options you wish to execute during the installation, then click **Next**.

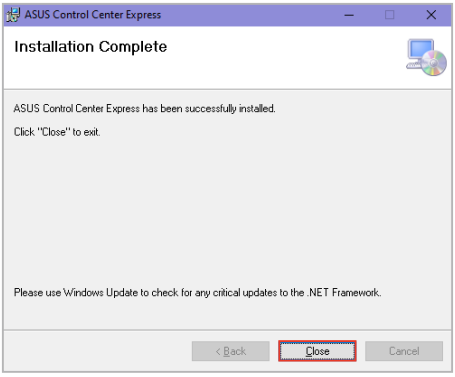
- **Launch ASUS Control Center Express after install finished:** Launches ASUS Control Center Express after the installation has finished.
- **Clear original configuration:** (not recommended) Remove previously set data of ASUS Control Center Express. If you wish to use this option, we recommend you backup the data of your ASUS Control Center Express.
- **Backup SQLite database:** (recommended) Backs up any existing SQLite database during installation. The default backup location is set to *C:\Program Files (x86)\ASUS\ASUS Control Center Express\apro_console\backup*.



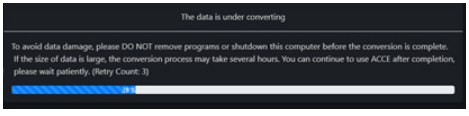
11. Please wait while ASUS Control Center Express is installing.



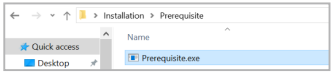
12. Once the installation is completed, click on **Close** to finish the installation.



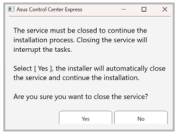
- If you are upgrading from a previous version of ASUS Control Center Express (v1.4.x or earlier) or if you are upgrading from SQLite to MySQL, some time may be needed to convert the database. To prevent loss of data, please do not uninstall any applications or turn off the main server until the database conversion is completed. If for any reason the database conversion fails to complete, you can still continue to use ASUS Control Center Express using the existing database.



- Before installing the database, ensure the main server is connected to a public WAN with a stable connection.
- If you need to perform a manual installation of MySQL database, please launch **Prerequisite.exe**, located under the **Installation** > **Prerequisite** folder.



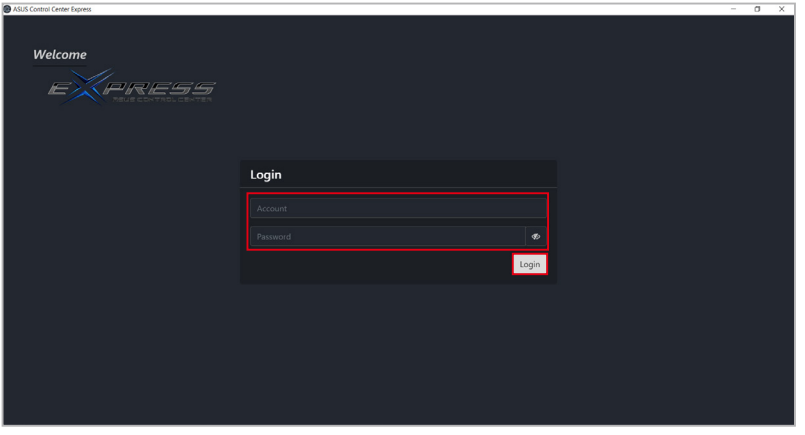
- If prompted to close ASUS Control Center Express services during an upgrade, click yes to automatically close background services and continue installation.



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.
- ASUS Control Center Express supports nine languages (English, Traditional Chinese, Simplified Chinese, Japanese, German, French, Russian, Korean, and Spanish). The display language will be set on first launch according to the operating system language. If the operating system language is not supported, the display language will default to English.
- It is strongly recommended to install a database to backup your data and settings. For more information, refer to the **Backup and Restore** section in the **Account & General Settings** chapter.

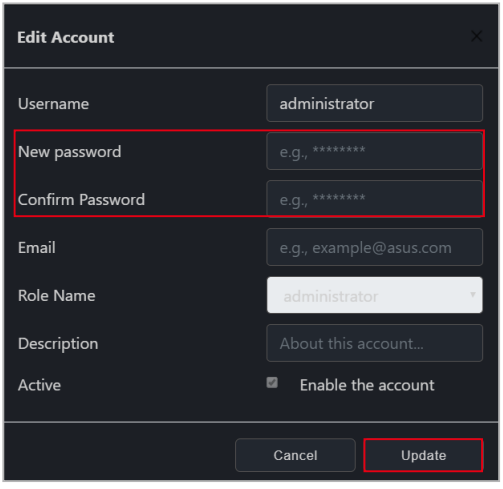


1.1.3 Changing the account password

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.

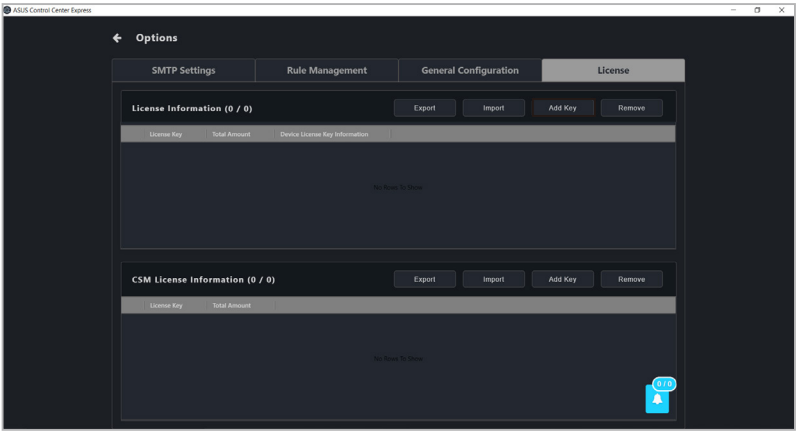
2. Click on the icon located at the top right menu bar, then click on **Settings**.
3. Click on the account to enter a new password, then click on **Update** to save the changes made.



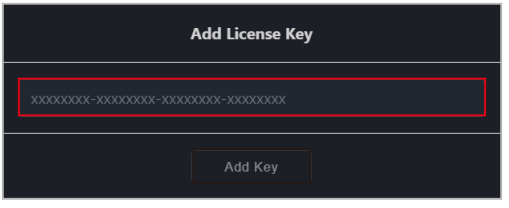
1.1.4 Activating your license key

- You must activate a license key before deploying an agent. Each client device you wish to deploy an agent to requires a corresponding license key.
- Please use the **Import** function if you already have a list of license keys to import or a previously exported list of license keys available. For more details on License Keys please refer to **8.1.4 License**.

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 **Options** > **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.

1.1.6 Updating ASUS Control Center Express

If you have already installed and are already using ASUS Control Center Express, you can follow the methods below to update the ASUS Control Center Express version:

Downloading the installation files and manually updating

1. Download the latest version of the ASUS Control Center Express installation file from the product website of your ASUS product.
2. Unzip the installation file, then refer to the **Installing ASUS Control Center Express (ACCE)** section to update the ASUS Control Center Express main software on the main server.
3. Once the ASUS Control Center Express main software update on the main server is completed, please refer to **Client Agent Updater** or **Upgrading or repairing agents** in the **Deploy Management** chapter to update the agents on the client device(s).

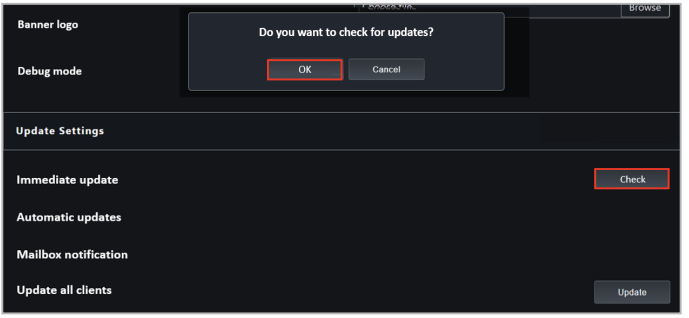
- It is strongly recommended to backup your data and settings before updating ASUS Control Center Express. Refer to **8.6.1 Managing data and settings in MySQL databases** or **8.6.2 Backing up data and settings in SQLite databases** for more information depending on the type of database installed.
- Monitoring and management functions may be affected or unavailable if you only updated the ASUS Control Center Express main software, but did not update the client device agents to v1.6.3 or above. Please refer to **Upgrading or repairing agents** in the **Deploy Management** chapter to update the client agent versions.
- If you have already installed and are using ASUS Control Center Express v1.4.x, and are upgrading to ASUS Control Center Express v1.5.x or above, please note that due to the database update and data conversion, the first time loading the updated version may take some time. Once the data conversion is completed you can continue using ASUS Control Center Express.
- If prompted to close ASUS Control Center Express services during an upgrade, click yes to automatically close background services and continue installation.

Updating by using Immediate update

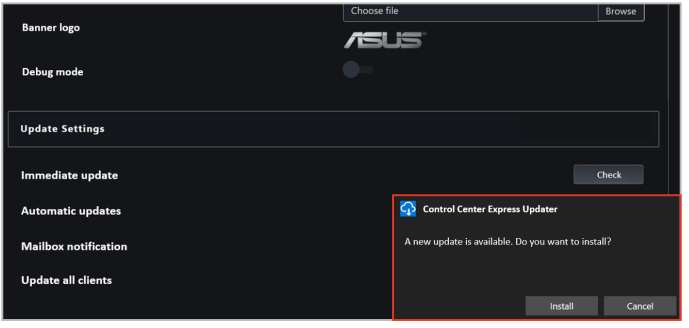
You can immediately update your ASUS Control Center Express from the **Update Settings** tab under **Options**.

1. Click on located at the top right menu bar, then select **Options** > **General Configuration**, then scroll to **Update Settings**.

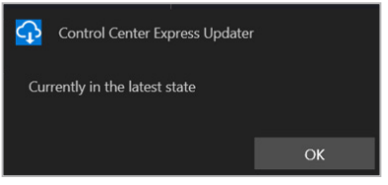
2. Click on **Check** next to the **Immediate update** field, then click **OK**.



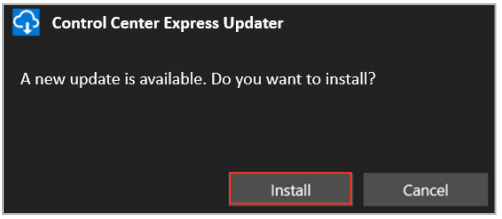
3. If a new update is available, a pop up notification will appear notifying you of a new update available for ASUS Control Center Express. Click **Install** on the pop up notification to install the new update, or click **Cancel** to cancel the update.



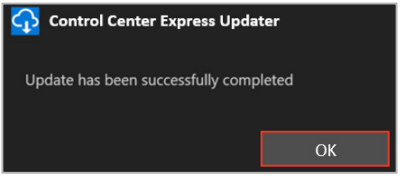
If your ASUS Control Center Express is already the latest version, the pop up notification will display a **Currently in the latest state** message.



4. Click on **Install** to begin the update. ASUS Control Center Express will automatically close when the update is ongoing, ensure to launch ASUS Control Center Express again after the update is completed.



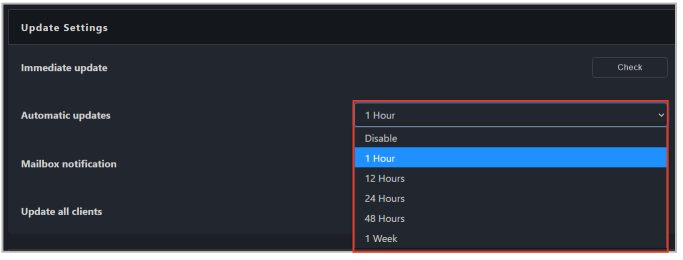
5. Click on **OK** once the update has been successfully completed.



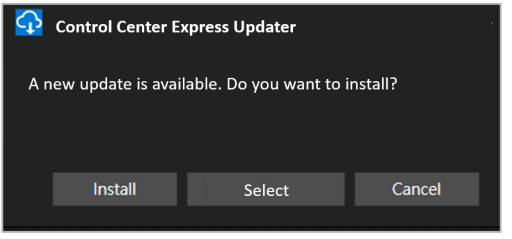
Updating by setting Automatic updates

Enable the **Automatic updates** function to receive a new update pop up notification on the bottom right of your ASUS Control Center Express window. You can choose whether to install or cancel the update from this pop up window.

1. Click on located at the top right menu bar, then select **Options** > **General Configuration**, then scroll to **Update Settings**.
2. Select how often to check for updates and prompt update notifications from the **Automatic updates** drop down menu.



3. When a new update is available, the pop up notification will appear in the bottom right corner of the ASUS Control Center Express window. You can do one of the following actions when the notification appears:
   - Click on **Install** to immediately download and begin updating.
   - Click on **Select** to select a different time to prompt you with the update notification.
   - (not recommended) Click on **Cancel** if you do not wish to update ASUS Control Center Express. If you select this option, the update notification will appear again the next time the selected notification time for **Automatic updates** is reached.



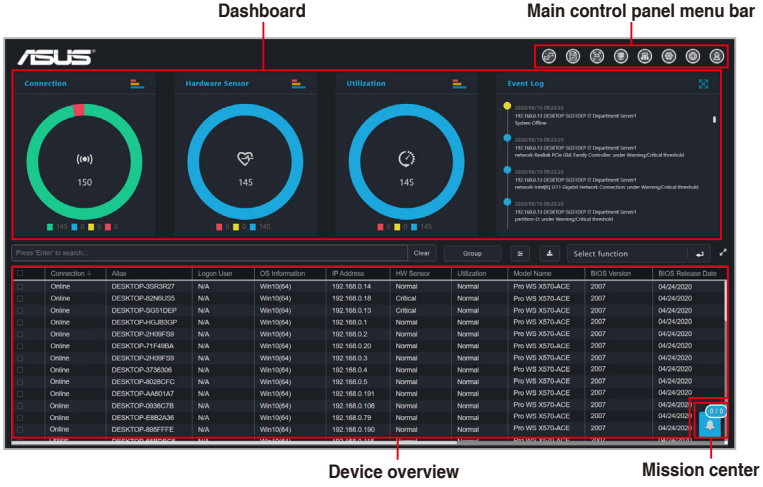
1.2 Main menu overview

You can toggle between Classic and Graphic views by clicking on .

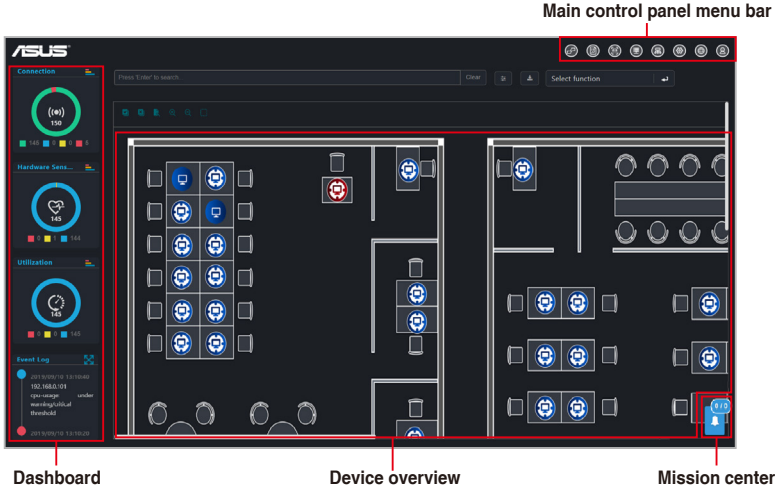
A brief overview of both views of ASUS Control Center Express is displayed as below:

The screenshots in this section are for reference only.

Classic view



Graphic view



Menu bar items:

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

Top menu bar items		Description
	Switch view	Switches user interface.
	Report generator	Generates graphs and reports of the online/offline status of client devices, and also generates lists and reports of software installation and hardware.
	Management control*	Check device hardware and execute functions using the remote management controller, for devices that are powered off, devices that have no OS installed, or devices where you cannot enter the OS.
	Metadata	Customize device metadata on a single or multiple devices.
	Deploy	Automatically or manually deploy or remove ASUS Control Center Express agents
	Settings	Configure SMTP Server setting, notification rules, ASUS Control Center Express main server settings, License key management, and data transfer.
	Language	Select the language for ASUS Control Center Express
	Account	• Add and edit accounts, and permission settings. • Scan QR code. • Logout.
	Mailbox	Read notifications related to ASUS Control Center Express

* To use the Management control function, ensure that the motherboard you wish to control supports remote management controller.

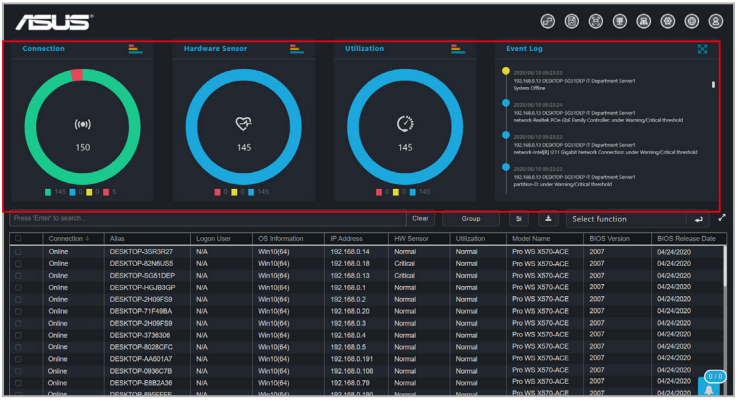
Chapter 2

This chapter describes the functions available on the main control panel.

Main Menu Overview

2.1 Dashboard overview

The Dashboard 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	Maintenance
Yellow	Standby
Red	Offline

Hardware Sensor

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

Color	Status
Red	Critical
Yellow	Warning
Blue	Normal

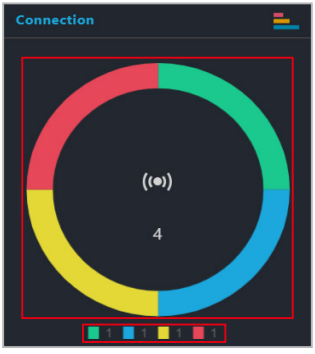
Utilization

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

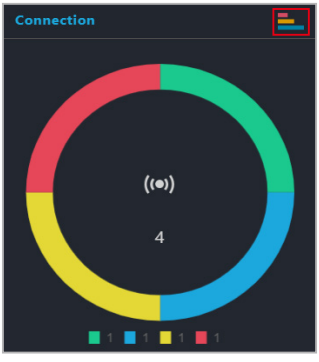
Color	Status
Red	Critical
Yellow	Warning
Blue	Normal

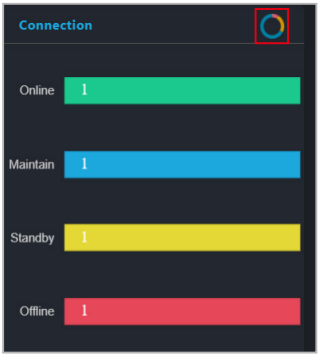
2.1.1 Switching sensor views

You can customize the information shown on the **Connection**, **Hardware Sensor**, and **Utilization** graphs by clicking on a color block on the graph or using the graph keys to filter devices which match the selected status. For example, on the **Connection** graph, you can choose to show or hide devices that are Online, under Maintenance, in Standby, or Offline.



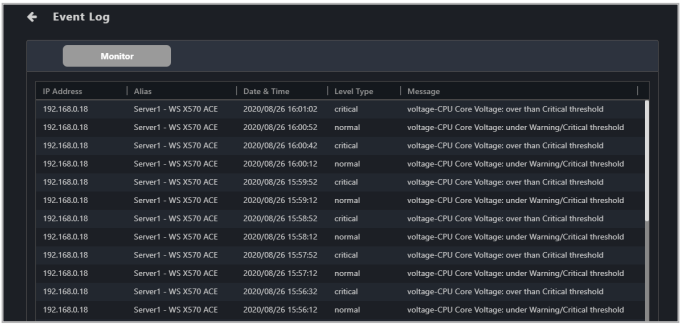
You can also click on the top right corner of each graph to switch between pie graph and bar graph views.





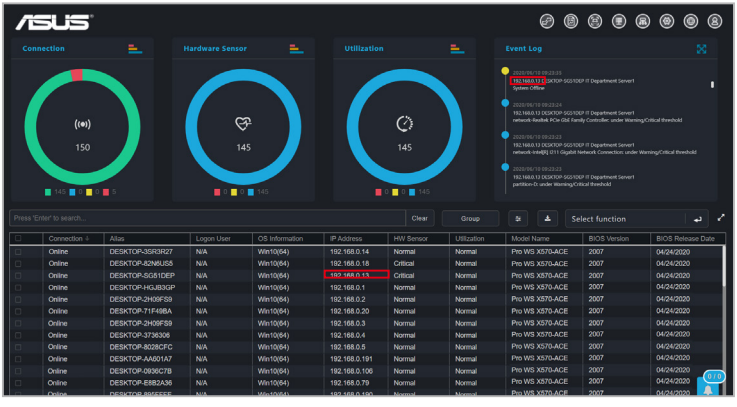
2.1.2 Event Log

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.



Please use the Notification Rule Management menu to manage which client devices, utilization status messages, hardware sensor events, or management controller alarms are shown in the Event Log. To set up notification rules, please click on located at the top right menu bar of the Dashboard, then select **Options** > **Rule Management**. For more information, please refer to **8.1.2 Rule Management**.

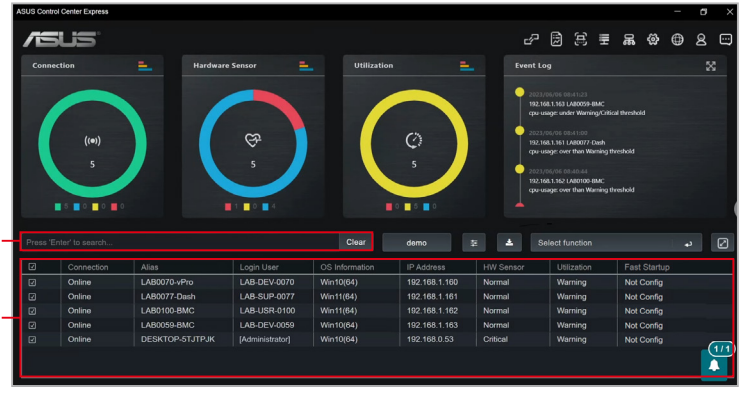
Clicking on a client device IP address on the Event Log will highlight the selected device in the Devices list, helping you quickly locate devices which require immediate attention.



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.

- Certain fields may show a value of “Not Config” if they have not yet been configured using ASUS Control Center Express.
- If the client device is powered off, offline, or logged out, the **Logon User** field will show the last logged in user enclosed in brackets (“[ ]”).



2.2.1 Filtering client devices

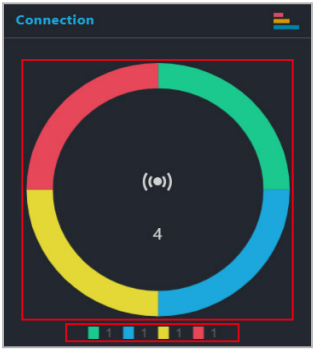
To clear the filter and view all devices, click on **Clear** in the Search bar.

- To filter 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. If you wish to remove a keyword, click on the **X**.

- To filter devices using the Dashboard:

  On the **Connection**, **Hardware Sensor**, or **Utilization** overview, click on a color block on the graph or use the graph keys to filter devices which match the selected status.



- To filter the devices using Devices list:

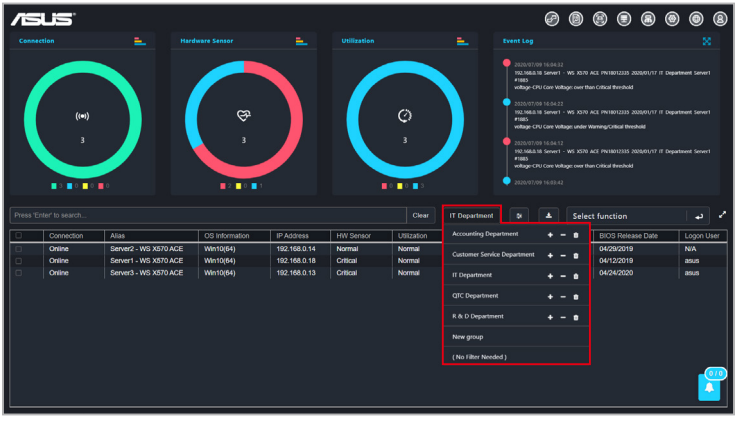
  1. Hover over the column you wish to use as your filter criteria in the Devices list.
  2. Click on ☰, then select the filter rule (**Equals**, **Not equal**, **Starts with**, **Ends with**, **Contains**, **Not contains**) and enter the keyword to search.

- Click on the name of a column header to sort the filter results alphabetically, in ascending or descending order.
- Click on the expand icon in the top right corner of the Devices overview block to expand the client device list; clicking on the expand icon again will revert the list back to its original size.
- Click and drag on a column title rearrange the columns of the Devices list.

- To filter the devices using Group:

To clear the filter and view all devices, click on **(No Filter Needed)** in the **Group** drop down menu.

Click **Group**, then select a group from the drop down menu to only display the devices in that group.



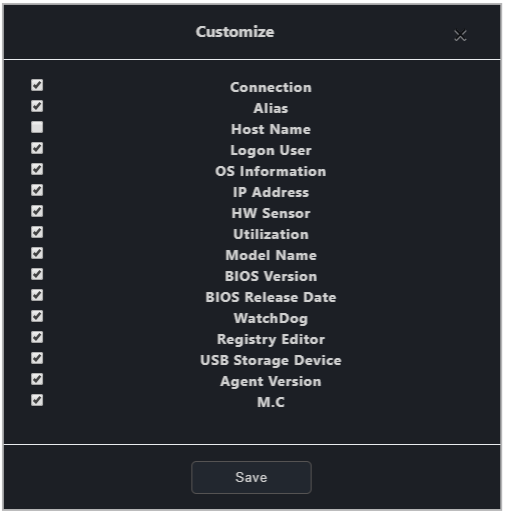
2.2.2 Redirecting to device information

You can view the device information of a device by clicking on a cell for a client device in the device overview list. You can view more detailed information on the client device, or operate different functions available for the client device on the device information page.

For more information on the device information page, please refer to the **Device Information** chapter.

2.2.3 Customizing device list metadata

Click on the **Customize** icon to select which items to display in the client device list, you can also display newly added metadata columns to the device overview list by checking the new metadata item.



2.2.4 Export device list

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

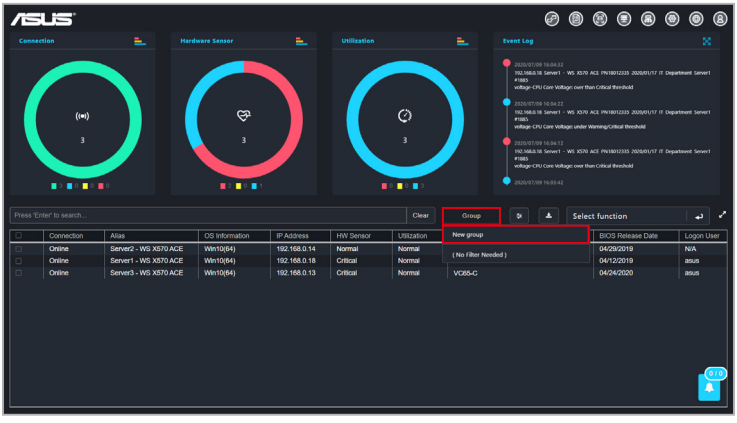
To Export the device list, click on **(Export)**, then enter your file name and click **Save** to save the device list as a .csv file.

2.2.5 Creating client device groups

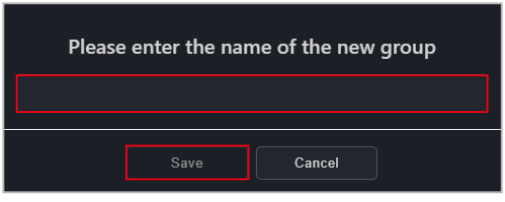
Group client devices on the client device list into groups according to your needs. Using the group function and filter function, you can quickly locate, view, and manage client devices. You can also apply notification rule settings to these groups, or easily add devices which appear on reports from the **Report generator** to existing groups.

To create a new device group:

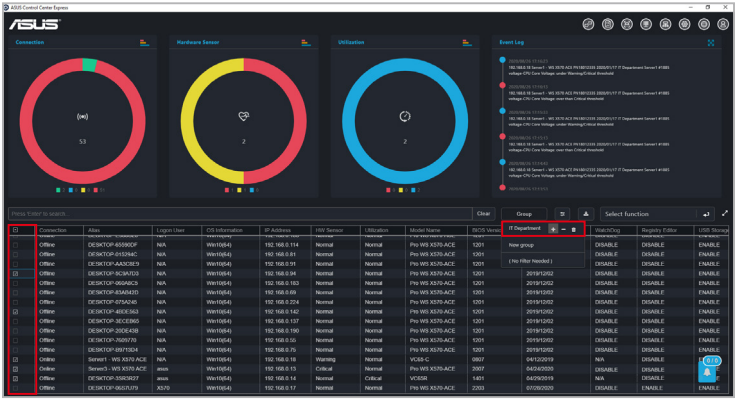
1. Click on **Group**.
2. Select **New group** from the drop down menu.



3. Enter a name for the group, then click **Save**.



4. Select the devices you wish to add to the group, then click **Group** and click .



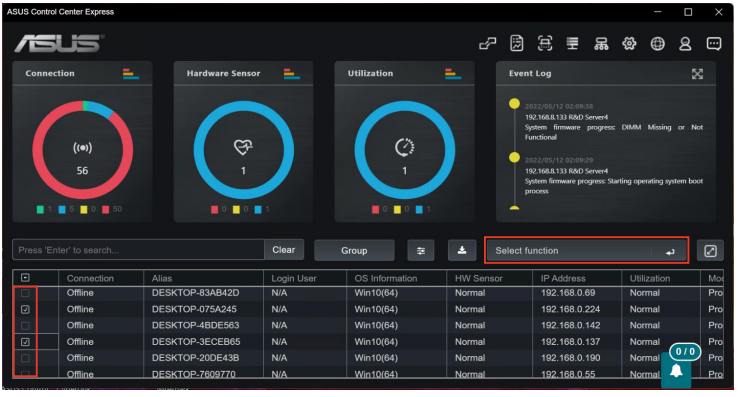
- Click on to remove the selected devices from the group.
- Click on to delete the group.

5. Click **Yes** on the confirmation window, then click **OK** to finish adding devices to a group.

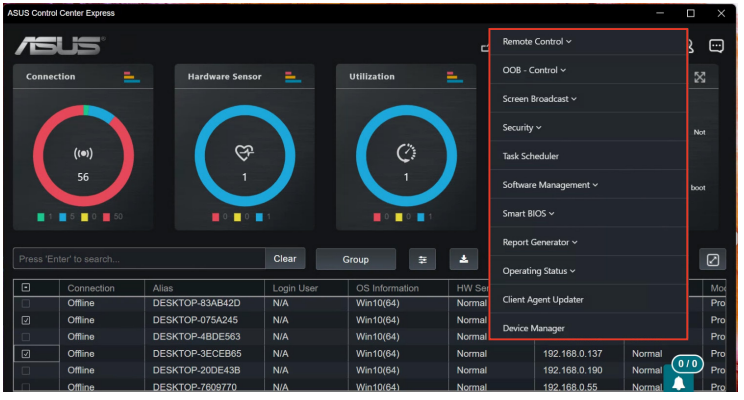
2.2.6 Using shortcut functions

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

1. Tick the checkbox for 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.



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

3. Use the Mission Center to check if the task was completed successfully. Refer to the **Mission Center** section for more information.

Remote Control

Restart computer	Restart the selected device(s).
Power off	Power off the selected device(s).
Power on	Power on the selected device(s). A powered off client device can only be powered on if it supports Wake on LAN.

OOB-Control

- Only available on client devices connected using a management LAN port with motherboards which support remote management controllers.
- The **OOB-Control** menu includes functions from the 4 remote management controllers: BMC, DASH, RTL8117, and vPro. If a selected device does not support a selected function, you can view related information in the mission center after executing the function.

- **Power control**

Power On (G0/S0)	Power on the selected device(s) through the remote management controller.
Power Off - Soft (G2/S5)	Power off the selected device(s) through the remote management controller.
Power Off - Hard (G3)	Force a power off of the selected device(s) through the remote management controller.
Power Cycle - Soft off (G2/S5)	Set the selected device(s) to restart after shutting down the OS through the remote management controller.
Sleep - Deep (G1/S3)	Set the selected device(s) to enter sleep mode (G1/S3) through the remote management controller.
Master Bus Reset	Reset the hardware of the selected device(s) through the remote management controller.
Hibernate (G1/S4)	Set the selected device(s) to enter hibernate mode (G1/S4) through the remote management controller.
Restart Computer to BIOS	Set the selected device(s) to enter BIOS after a restart through the remote management controller.
Power On to BIOS	Set the selected device(s) to enter BIOS after powering on through the remote management controller.
Restart Computer to IDE-R Floppy	Set the selected device(s) to enter IDE-R floppy drive after a restart through the remote management controller.
Power On to IDE-R Floppy	Set the selected device(s) to enter IDE-R floppy drive after powering on through the remote management controller.

- **Power control (continued)**

Restart Computer to IDE-R CDROM	Set the selected device(s) to enter IDE-R ODD after a restart through the remote management controller.
Power On to IDE-R CDROM	Set the selected device(s) to enter IDE-R ODD after powering on through the remote management controller.
Sleep - Light (G1/S2)	Set the selected device(s) to enter sleep mode (G1/S2) through the remote management controller.
Power Cycle - Hard Off (G3)	Power off and restart the selected device(s) through the remote management controller.
Diagnostic Interrupt (NMI)	Set the selected device(s) to print error report and restarting through the remote management controller.
Power Off - Soft Graceful (G2/S5)	Normal shut down via the OS of the selected device(s) through the remote management controller.
Power Off - Hard Graceful (G3)	Normal shut down via the hardware of the selected device(s) through the remote management controller.
Master Bus Reset Graceful	Normal shut down and resetting the hardware of the selected device(s) through the remote management controller.
Power Cycle (Graceful Soft Off) (G2/S5)	Normal shut down via the OS then restarting the selected device(s) through the remote management controller.
Power Cycle (Graceful Hard Off) (G3)	Normal shut down via the hardware then restarting the selected device(s) through the remote management controller.

- **Watchdog**

Watchdog Enable	Enable RTL8117 Watchdog monitoring for selected device(s).
Watchdog Disable	Disable RTL8117 Watchdog monitoring for selected device(s).

- **BIOS**

Clear CMOS	Clear CMOS for selected device(s) through RTL8117 or BMC to reset them to factory settings.

- **Account management**

Set password	Setting the remote management controller account password for selected RTL8117 or vPro device(s).
Login	Log into the remote management controller account of selected BMC or DASH device(s).

- **System**

Restart service	Restart the RTL8117 service on selected device(s).
Port	Set the BMC port for selected device(s).
Sync OEM port	Synchronize the BMC port for selected device(s).

- **KVM**

KVM Remote Multi-display	Set RTL8117 KVM of selected device(s) as remote Multi-display.
KVM Local Multi-display	Set RTL8117 KVM of selected device(s) as local Multi-display.
KVM Remote Single-display	Set RTL8117 KVM of selected device(s) as remote single-display.
KVM Enable	Enable KVM for selected RTL8117 and vPro machine(s).
KVM Disable	Disable KVM for selected vPro machine(s).
KVM Password	Set the vPro KVM password for selected device(s).

- **USB redirection**

USB Redirection	Configure USB redirection of selected device(s) through the client device's remote management controller.
Enable USB Redirection	Enable USB redirection for selected device(s).
Disable USB Redirection	Disable USB redirection for selected device(s).

- **Firmware update**

Firmware Update	Update the RTL8117 or BMC firmware of selected device(s). Firmware Update will be disabled if KVM is Enabled.

- **Trust zone**

Trust Zone	Set the main server IP addresses which are allowed to perform RTL8117 function operations on client devices.

- **Certificate management**

Certificate Management	Manage the vPro certificates for selected device(s).

- **System trap alert**

Enable Trap Alert	Enable the DASH and vPro system trap alert on selected device(s).
Enable Trap Alert - Info	Set the DASH and vPro system trap alert as information level on selected device(s).
Enable Trap Alert - Warning	Set the DASH and vPro system trap alert as warning level on selected device(s).
Enable Trap Alert - Error	Set the DASH and vPro system trap alert as error level on selected device(s).
Disable Trap Alert	Disable the DASH and vPro system trap alert on selected device(s).

- **IPMI**

IPMI Tool Lanplus Command Redirect	Configure command redirection on selected BMC device(s).
FRU Info. Write	Write information from the FRU to the BMC device(s).

- **Settings**

Settings	Configure settings for selected BMC device(s).

- **OOB - Control Help**

OOB - Control Help	View descriptions of supported OOB control functions.

Screen broadcast

Create a broadcast room	Create a broadcast room and broadcast to selected device(s).

Security and boot settings

If the below settings have not previously been configured using ASUS Control Center Express, the default value of “Not config” will be displayed.

Enable Regedit	Enable Windows Registry Editor on device(s).
Disable Regedit	Disable Windows Registry Editor on device(s).
Enable USB	Enable the USB ports on device(s).
Disable USB	Disable the USB ports on device(s).
USB Read Only	Set the USB ports to Read Only privileges on device(s).
Fast Startup Enable	Enable fast startup on device(s).
Fast Startup Disable	Disable fast startup on device(s).
Enable Windows Update	Enable Windows Update on device(s).
Disable Windows Update	Disable Windows Update on device(s).

Task scheduler

Task Scheduler	Schedule tasks for selected device(s).

Software management

Software Dispatch	Dispatch software and scripts to device(s).
Software Information	View or configure applications, processes or services on device(s).
Software Blacklist	View or add blacklisted software for device(s).
Installer	Download or update the driver, utility applications, and BIOS for device(s).
Software Rule Management	Set rules for software blacklist and whitelist, as well as the email receiver for the notifications.

Smart BIOS

BIOS	Upload, update or flash the BIOS of the selected device(s)
Enable BIOS settings	Enable the BIOS settings of client devices.

Report generator

Connection	Generate a report and analysis on connection status (online / offline) of client devices.
Software	Generate a report and list of software installations and permissions.
Hardware	Generate a report and list of client device’s hardware.

Operating status

Maintenance	Set the operating status of device(s) to maintenance.
Standby	Set the operating status of device(s) to standby.
Normal	Set the operating status of device(s) to normal.

Client agent updater

Client Agent Updater	Update client device's agent.

Device manager

Device Manager	View device manager information for device(s).

System restore

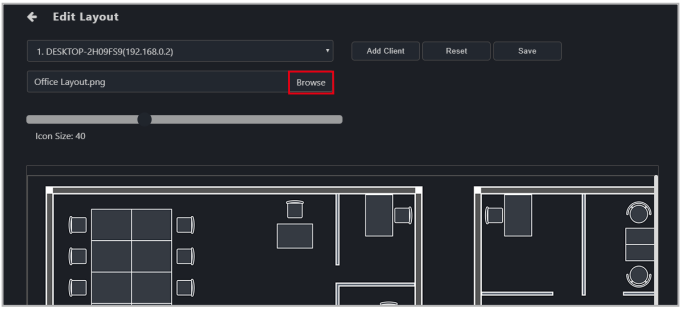
Quick Create	Create a system restore point for the selected device(s).
System Restore Point	Restore the selected device(s) from a system restore point.

2.3 Customizing the graphic view

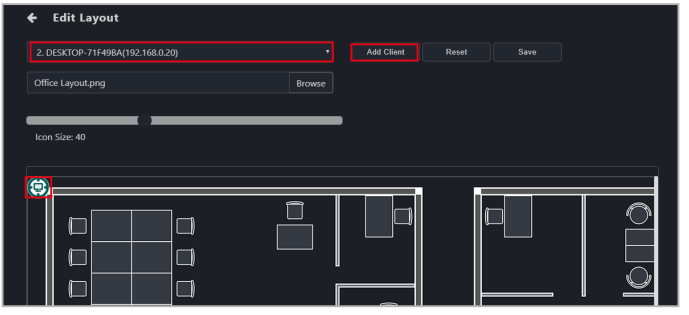
You can toggle between the Classic view or Graphic view. The Graphic view allows you to upload a layout image (such as the office floor) and place shortcut icons of client devices onto their respective places on the layout.

2.3.1 Customizing the Graphic view for the first time

1. Click on to toggle to the Graphic 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 an client device icon by selecting the device from the drop down list, then clicking on **Add Client**. The client device icon should appear in the background area.

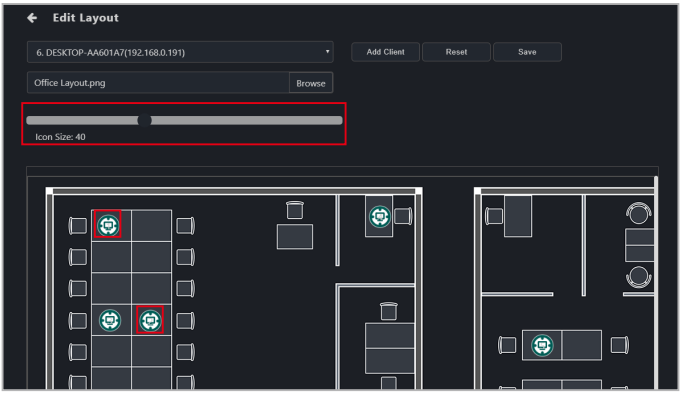


The client devices are assigned numbers in the order in which they are added. If a client device is redeployed, it will be assigned a new sequential number instead of its original number.

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

To remove all client device icons click on **Reset**.

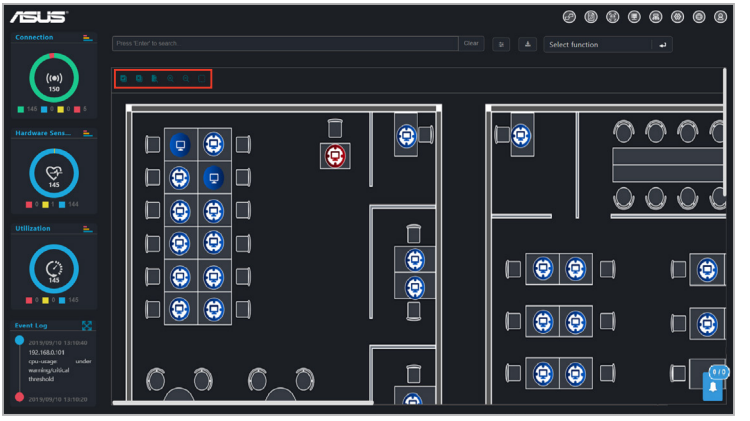
6. You may adjust the positions of the client device icons by clicking and dragging the client device icon to your preferred location, or adjust the size of the client device icons using the **Icon Size** scroll bar.



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

2.3.2 Using the Graphic view menu items

Please refer to the table below for the different functions available on the Graphic view.



	Check all machines	Select all client devices on the layout
	Uncheck all machines	Deselect all client devices on the layout
	Edit	Edit the shortcut icons and background, please refer to steps 3 to 7 of the **Customizing the Graphic view for the first time** section to edit the background and shortcut icons.
	Zoom In	Zoom in on the layout area
	Zoom Out	Zoom out on the layout area

2.3.3 Using the client device icons

- Hover over client device icon:
  Hover over a client device 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 client device icon:
  A single click on the client device icon will select the icon, for when you wish to use a function on a client device or multiple devices. To deselect the icon, click on the client device icon again.

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

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

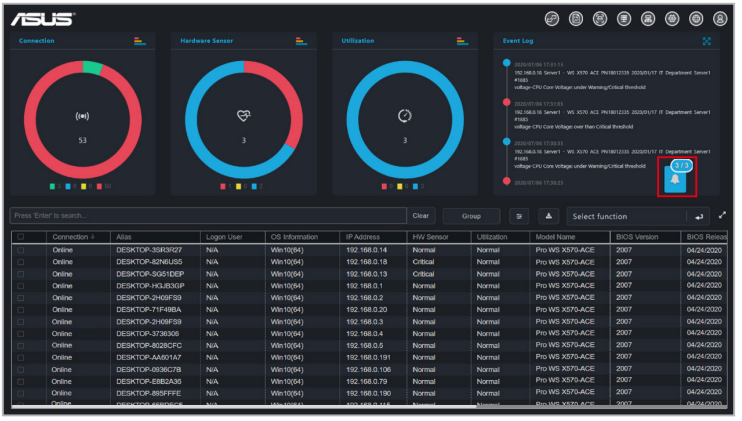
For more information on the Device Information screen please refer to **Chapter 4 Device Information**.

- Client device icon status:
  The client device icon will change or change colors depending on the status.

Unchecked	Checked	Status
		Offline
		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 Mission Center

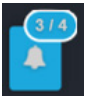
The Mission Center allows you to view the progress and status of tasks. Tasks that are still pending, finished tasks, and ongoing tasks can all be viewed in the Mission Center as well as the progress and execution results of the tasks.



2.4.1 Using the Mission Center

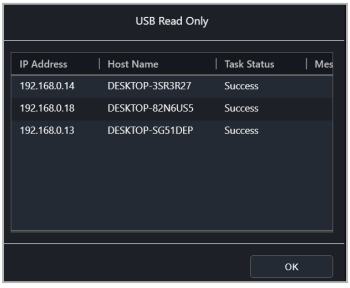
There are a number things you can do with the Mission center, please see the list below for more information.

- Reposition the Mission Center:
  Click and drag the Mission Center icon to move it to another location.
- Viewing finished/total amount of tasks:
  View the number finished tasks (left number) and the total number of tasks (right number) from a quick glance on the Mission Center icon.

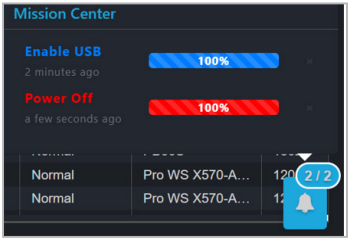


- Expanding / minimizing the Mission Center:
  You can click the Mission Center icon to expand the Mission Center and view the progress and starting time of the tasks; clicking on the Mission Center icon again will minimize the expanded window.

- Viewing task information:
  Clicking on a task name in the expanded view of the Mission Center will allow you to view the client devices the task is being performed on as well as the status or results for each client device.



- Failed tasks:
  A failed task will be marked in red in the Mission Center. You can click on the task name to view more details on the failed task.



2.4.2 Mission Center tasks

The table below lists the tasks you can view on the Mission Center.

- Click on the **X** next to the task progress bar to delete a completed task. Only completed tasks can be deleted, tasks that are still pending and ongoing tasks cannot be deleted until they are completed.
- Tasks that are split up into steps can also be completed through the Mission Center. For example a task that restarts the client device after BIOS update; you can restart the client device through the Mission Center once the BIOS update step has been completed.
- The Mission Center will record current ongoing tasks on the ASUS Control Center Express main server, if the ASUS Control Center Express main server is closed and restarted, the mission center's tasks will be reset and only record the ongoing tasks once the ASUS Control Center Express main server has restarted.

Power Control		Power off/power on/restart computer
Security and Boot	**Registry Tool**	Enable/disable regedit
	USB Control	Enable/disable USB control
		Set USB to read only
	Fast Startup	Enable/disable fast startup
Software Management		Software Dispatch
		Software Blacklist
		Installer
Smart BIOS		BIOS update
Client Agent Updater		Update client device's agent
Settings Migrator		Migrate server settings
Main Server Settings		Agent deployment
OOB Control*		Power Control
		Watchdog
		BIOS
		Account Management
		System
		KVM
		USB Redirection
		Firmware Update
		Trust Zone
		Certificate
		System Trap Alert
		IPMI
		Settings
		Configuration

* **These functions are only available on motherboards that support remote management controllers.**

Chapter 3

This chapter describes how to automatically or manually deploy ASUS Control Center Express agents and remove agents, and updating agents.

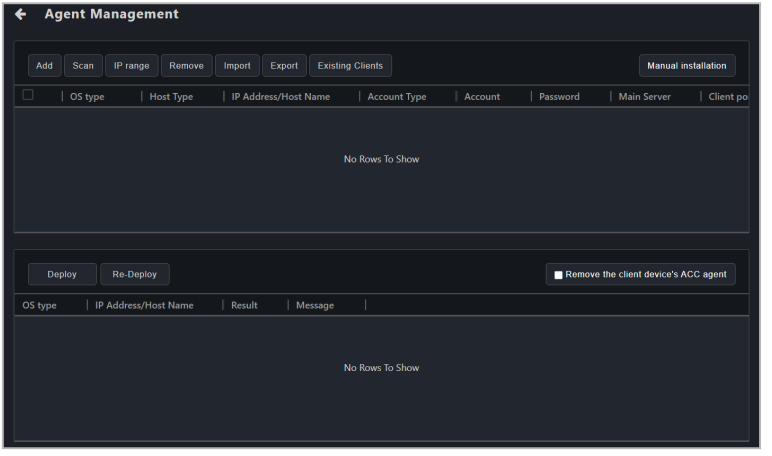
Deploy Management

3.1 Agent Management overview

The Agent Management menu allows you to manage ASUS Control Center Express agents, such as automatic or manual agent installation or removal.

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

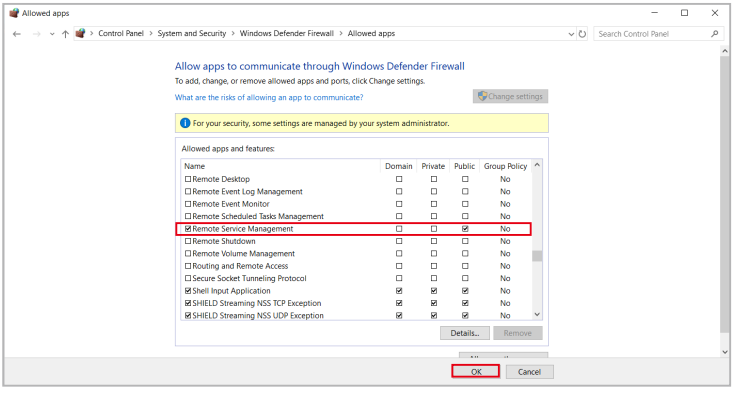
The screenshots in this section are for reference only.



Add	Add a single device to deploy an agent to.
Scan	Automatically scan all client devices in the same subnet as the Main server available for agent deployment
IP Range	Scan an IP Range entered that you wish to scan.
Remove	Remove client device(s) that you do not wish to deploy agent(s) to.
Import	Import an already exported device list (.csv file).
Export	Export the current device list of devices added or scanned to a .csv file.
Existing Clients	Display all client device(s) that already have agents deployed.
Manual Installation	Download the agent installation file, then manually install the agent on the client device, or install the agent in silent mode.
Deploy	Automatically deploys the agent to the selected client device(s) .
Re-Deploy	Repairs the agent on client device(s) which already have agents installed.
Remove the client device's ACC agent	If an ACC CSM agent is already installed on a client device, checking this option will automatically remove the ACC CSM agent when deploying an ASUS Control Center Express agent.

Before you begin deploying, please ensure the following:

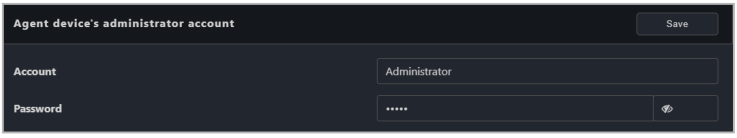
- Activate the license keys before deploying agents to client devices. Each client device you wish to deploy an agent to requires a corresponding license key. For more information on activating license keys, please refer to **8.1.4 License.**
- The client and ACCE server are in the same network domain.
- The Remote Service Management option is checked under the client device's firewall settings. (Right click on the Windows **Start** icon > **Settings** > **Update & Security** > **Windows Security** > **Firewall & network protection** > **Allow an app through firewall**)



- Temporarily disable the client device's anti-virus firewall; you may re-enable the anti-virus firewall once the agent deployment process is successfully completed. For more information on disabling the anti-virus firewall please refer to the user manual or product website for your anti-virus.
- The default Agent device's administrator account and password may differ according to your system language, ensure the Agent device's administrator account and password matches the client device's actual administrator account and password before deploying.
- The client device's system time and date should not be changed unless necessary.

- The Administrator account of the client should be enabled with a password set, ensure to enter this account and password when you deploy to that client device. If no account and password has been entered, a default account and password will be used and can be viewed or edited in **Settings** > **Options** > **General Configurations** > **Agent device's administrator account**, please refer to **8.1.3 General Configurations** for more information.

  Administrator account settings may differ between different versions of Windows, please refer to the Microsoft website for more information on Windows account settings.



- If an agent has already been deployed to the client device but requires a redeployment, please remove the agent from the client device then redeploy the agent. For more information, please refer to **3.3 Removing agents**.
- **Re-Deploy** function is only used for upgrading versions before ASUS Control Express v1.5, and for repairing agent.
- If the main server or client device is running Windows 7, please install the following: .Net Framework 4.6.1 or above, SHA-2, and TLS 1.2 on the main server before deploying agents. For more information please refer to **3.2.8 Setting up Windows 7 deployment environment**.
- If a client device with Windows 7 OS does not support SHA-2 and TLS 1.2, the necessary installations will still be carried out when deploying an agent to the client device. When the agent deployment is finished, please follow the instructions and reset the client device, then redo the agent deployment process on the client device.
- If the main server or client device is running Windows 11, connect to the internet, then run Windows Update and confirm that Windows Defender is updated to the latest version before attempting agent deployment.

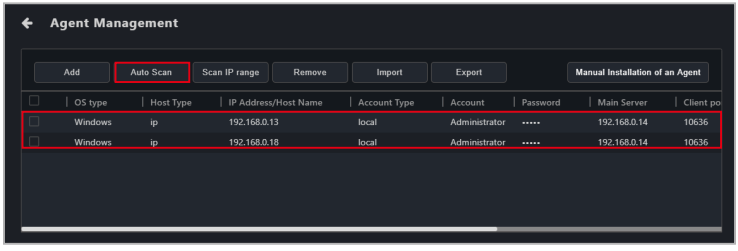
3.2 Deploying agents

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

You must activate a license key before deploying an agent. Each client device you wish to deploy an agent to requires a corresponding license key. For more information on activating license keys, please refer to **8.1.4 License**.

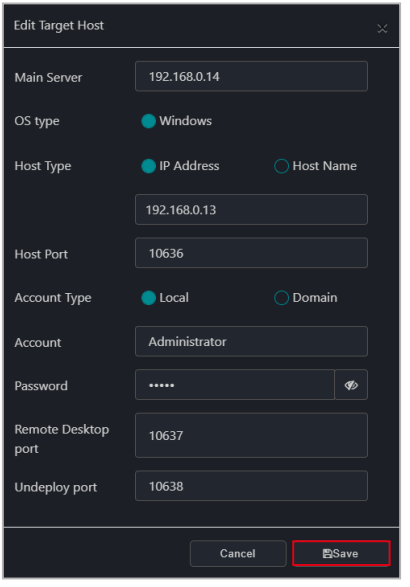
3.2.1 Automatically scanning and deploying to devices

1. Click on **Auto Scan**.
2. After the scan is completed, the devices should appear in the scan results block shown below..



3. Double click on a device in the scan results to edit the device information, then click **Save** once you are finished.

- Ensure that the account entered in the **Account** field has administrator privileges.
- The default account and password displayed is the Agent device's administrator account and password, this can be edited under **Settings** > **Options** > **General Configurations** > **Agent device's administrator account**. Please refer to **8.1.3 General Configuration** for more information.



4. Once you have finished editing the scanned device information, select the devices you wish to deploy agents to, then click **Deploy**.

If ACC CSM is already installed on the client device, please export and backup the data first, then check the **Remove the client device's ACC agent** option before deploying.

5. After the deployment is completed, you may view the deploy status in the deploy list.

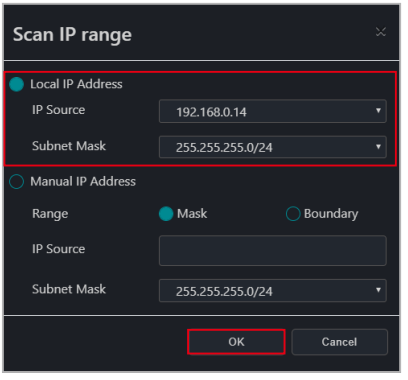
3.2.2 Scanning an IP range

Depending on your network environment, you may set an IP range to scan for devices, helping you deploy agents quickly and efficiently.

Main Server IP address

This will allow you to set the main server's IP as the scan range.

1. Click on **Scan IP range** and select **Local IP Address**.
2. Select the main server's IP address in the **IP Source** field and the subnet mask range to scan in the **Subnet Mask** field.
3. Click **OK** to begin scanning.



4. Double click on a device in the scan results to edit the device information, then click **Save** once you are finished.
5. Once you have finished editing the scanned device information, select the devices you wish to deploy agents to, then click **Deploy**.

If ACC CSM is already installed on the client device, please export and backup the data first, then check the **Remove the client device's ACC agent** option before deploying.

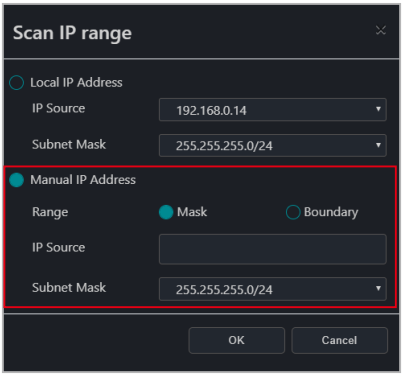
6. After the deployment is completed, you may view the deploy status in the deploy list.

Client device IP address

This will allow you to set the client device's IP as the scan range.

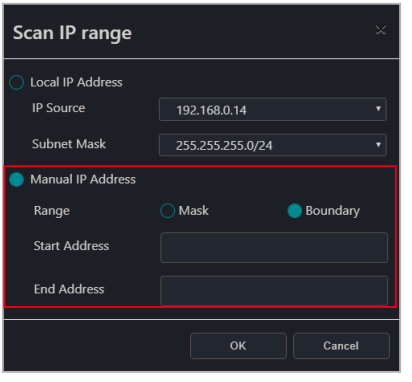
1. Click on **Scan IP range** and select **Manual IP Address**.
2. Select **Mask** to scan the subnet mask range of the client device, or select **Boundary** to set a starting IP and ending IP to scan in the **Range** field.

   Mask:



IP Source	Enter the client device's IP.
Subnet Mask	Select a subnet mask range to scan.
NIC	Select the IP of the main server network card to scan.

   Boundary:



Start Address	Enter the start IP address of the client device you wish to scan.
End Address	Enter the end IP address of the client device you wish to scan.
NIC	Select the IP of the main server network card to scan.

3. Click **OK** to begin scanning.
4. Double click on a device in the scan results to edit the device information, then click **Save** once you are finished.
5. Once you have finished editing the scanned device information, select the devices you wish to deploy agents to, then click **Deploy**.

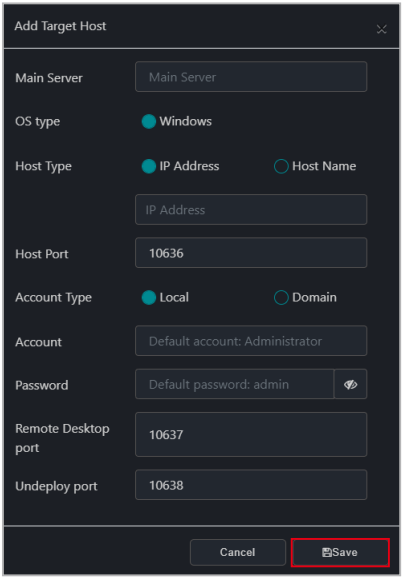
If ACC CSM is already installed on the client device, please export and backup the data first, then check the **Remove the client device's ACC agent** option before deploying.

6. After the deployment is completed, you may view the deploy status in the deploy list.

3.2.3 Adding and deploying to devices

Adding a single device

1. Click on **Add**.
2. Enter the information of the device you wish to add, then click on **Save**.



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

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

3. Click on **Save**, the device should appear in the device list.
4. Select the devices you wish to deploy agents to in the device list, then click **Deploy**.

If ACC CSM is already installed on the client device, please export and backup the data first, then select the Remove the client device's ACC agent option before deploying.

5. After the deployment is completed, you may view the deploy status in the deploy list.

Adding multiple devices

If you already have an existing exported device list CSV file for ASUS Control Center Express, you may use the **Import** function to import multiple devices for deployment.

1. Click on **Import**.
2. Browse for the CSV file you wish to import, then click **Open**.
3. The imported devices will appear in the device list, select the devices you wish to deploy agents to, then click **Deploy**.

If ACC CSM is already installed on the client device, please export and backup the data first, then check the Remove the client device's ACC agent option before deploying.

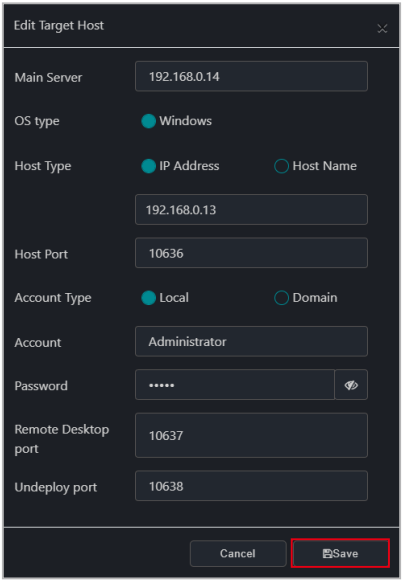
4. After the deployment is completed, you may view the deploy status in the deploy list.

Click on **Export** to export the current device list to a CSV file which you may edit using text editor.

3.2.4 Editing device information

You may edit the device information of scanned or added devices before deploying agents.

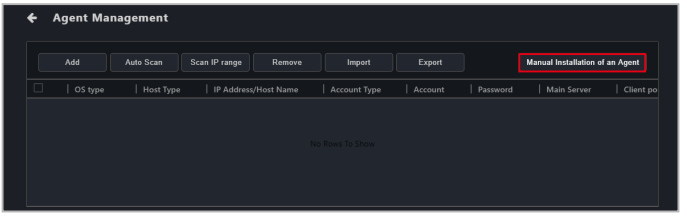
1. Double click on the device you wish to edit.
2. Click on **Save** once you have finished.



3.2.5 Installing agents manually

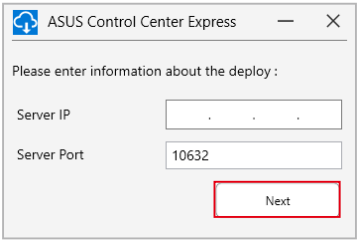
Installing an agent onto a client device

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

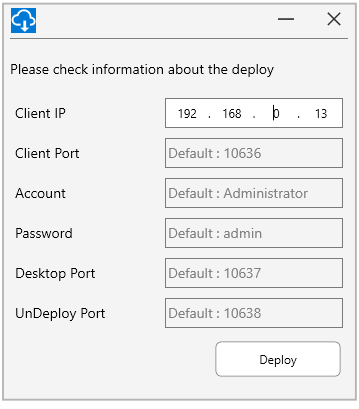


2. Copy and paste **Setup.msi** to the client you wish to install the agent on using an external storage device such as a USB flash drive.
3. On the client device, double click on the **Setup.msi** file to launch the installation.

4. Enter the main server's IP into the **Server IP** field, then click **Next**. The **Server Port** field's default port may be adjusted if necessary.



5. Please verify the client device information received by the main server. If any of the default ports are already in use, please make adjustments accordingly after the installation through the ASUS Control Center Express main server.



6. Click on **Deploy**, then wait for the deployment to be completed.

Installing an agent onto the main server

The agent can also be manually installed on the main server to perform management and maintenance tasks through ASUS Control Center Express.

- The main server can only be used as a broadcast source in the Screen Broadcast function in this configuration.
- A video feedback loop effect may occur if the Remote Desktop function is used to control the main server.

1. Click on **Manual Installation of an Agent** to start downloading the installation files (Setup.msi).
2. Double click on the **Setup.msi** file to launch the installation.
3. Enter the main server's IP or 127.0.0.1 into the **Server IP** field, then click **Next**. The **Server Port** field's default port may be adjusted if necessary.
4. Please verify the client device information received by the main server. If any of the default ports are already in use, please make adjustments accordingly after the installation through the ASUS Control Center Express main server.
5. Click on **Deploy**, then wait for the deployment to be completed.

3.2.6 Installing Agents in silent mode

Silent mode installation parameters

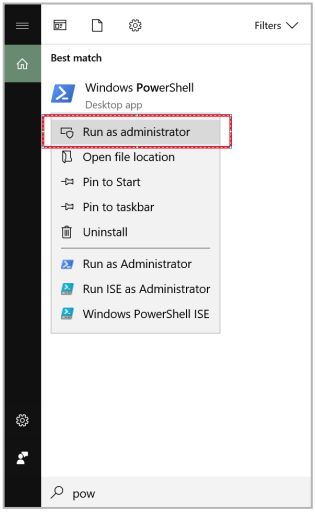
Server IP	ASUS Control Center Express server IP (mandatory)
Client IP	Local host IP (mandatory)
Client port	Local host port (optional)
Account	Local host user account (optional)
Password	Local host user password (optional)
Outfail	Dump deploy fail to file (optional)

Feedback results

0 ERROR_SUCCESS	Action completed successfully
1602 ERROR_INSTALL_USEREXIT	Installation canceled by user
1603 ERROR_INSTALL_FAILURE	Fatal error during installation
1639 ERROR_INVALID_COMMAND_LINE	Invalid command line argument

Please see an example below:

1. Run Windows PowerShell as Administrator.



2. Enter the command to run the agent installation. For example,
`(Start-Process msiexec '/i "C:\Setup.msi" serverip=192.168.1.2 /qb -Wait -Passthru).ExitCode`

Details during the deployment

1. Please add the outfail parameter in the command line. For example,
`(Start-Process msiexec '/i "F:\ Setup.msi" serverip=192.168.1.2 clientip=192.168.1.200` **`outfail`**`="D:\New folder\Fail.txt" /qb ' -Wait -Passthru).ExitCode`

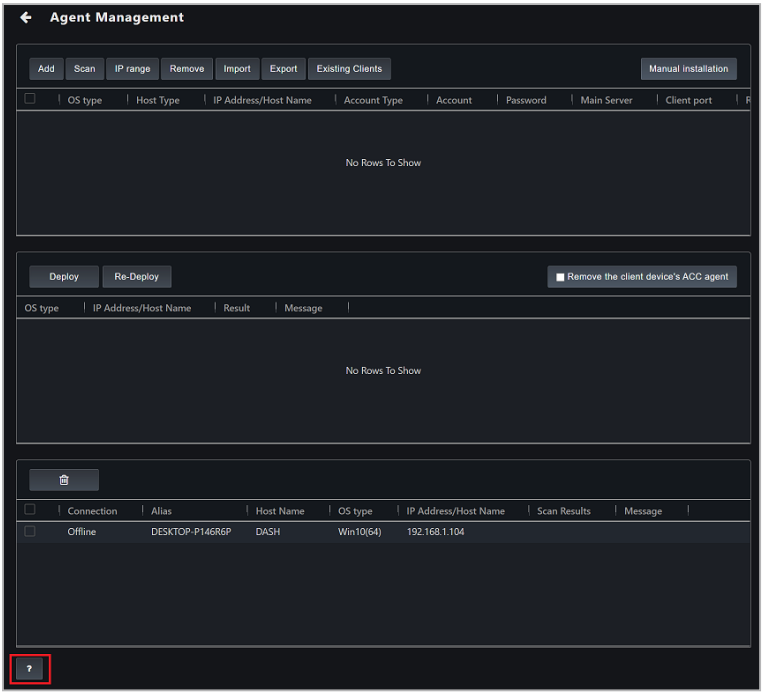
2. Once the installation is finished, the results will be saved to D:\New Folder\Fail.txt.

Client device has previously already installed the agent and needs to reinstall

1. Please remove the installed agent from the client device. For example,
`(Start-Process msiexec '/x "C:\ Setup.msi" /q ' -Wait -Passthru).ExitCode`
2. Run the agent installation command. For example,
`(Start-Process msiexec '/i "C:\Setup.msi" serverip=192.168.1.2 /qb -Wait -Passthru).ExitCode`

3.2.7 Upgrading or repairing agents

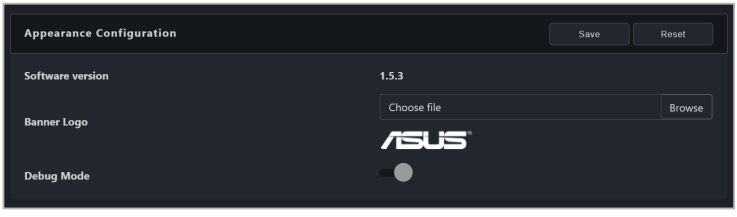
If the ASUS Control Center Express version is older than version 1.4.27, some functions may not work properly after restarting the client device. Please follow the steps below or click on the information icon on the bottom of the **Agent Management** page to upgrade the agent or repair the agent.



Before upgrading or repairing the agent, please check your ASUS Control Center Express version:

- ASUS Control Center Express main software version

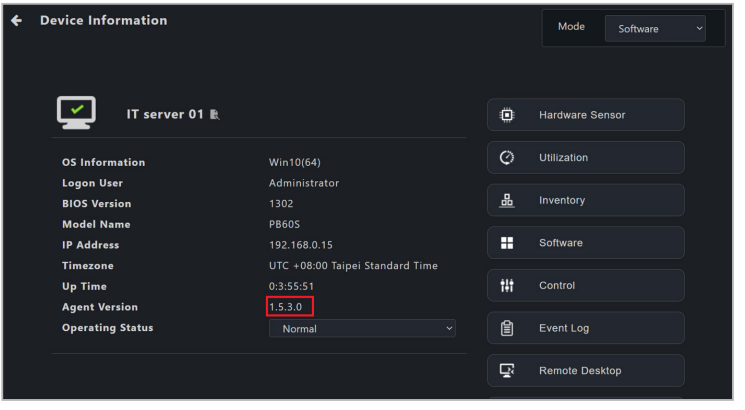
  Go to **Settings** > **Options** > **General Configuration**, then scroll down to the **Appearance Configuration** block, the Software version should be displayed there.



- Client device agent version

  The agent version of the client device will be displayed in the **Agent Version** column in the device list on the device overview.

You may also view the agent version of a single client device in the **Device Information** page by clicking on the client device.

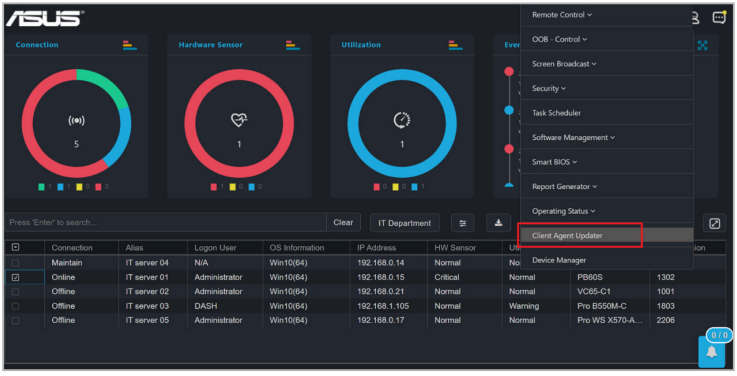


Updating from version 1.4.XX to version 1.5.X

1. Download the latest version of ASUS Control Center Express (1.5.X or later), then run the installation of the ASUS Control Center Express main software on the main server.

2. Once the installation is completed, check the device(s) you wish to update or repair from the device list, and select the **Client Agent Updater** from the shortcut function drop down menu.

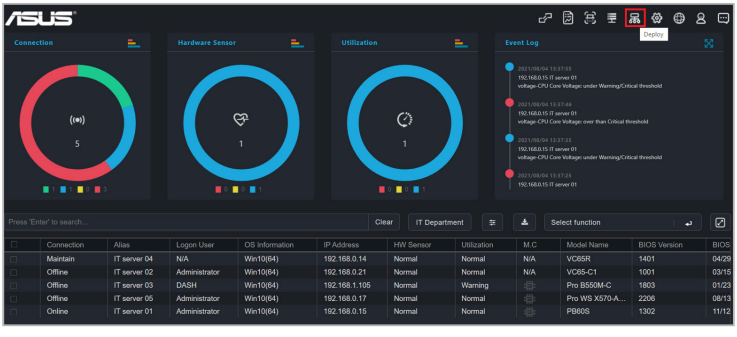
Please refer to section **2.2.6 Using shortcut functions** for more information on using the shortcut function.



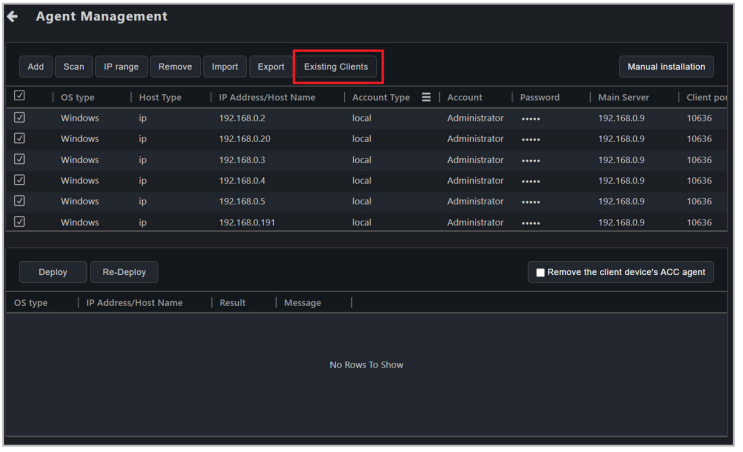
3. Click on **Yes** in the confirmation pop-up window to proceed with the update.
4. You can view the agent deployment and update results in the mission center.

Updating from version 1.3.X or earlier versions to version 1.5.X

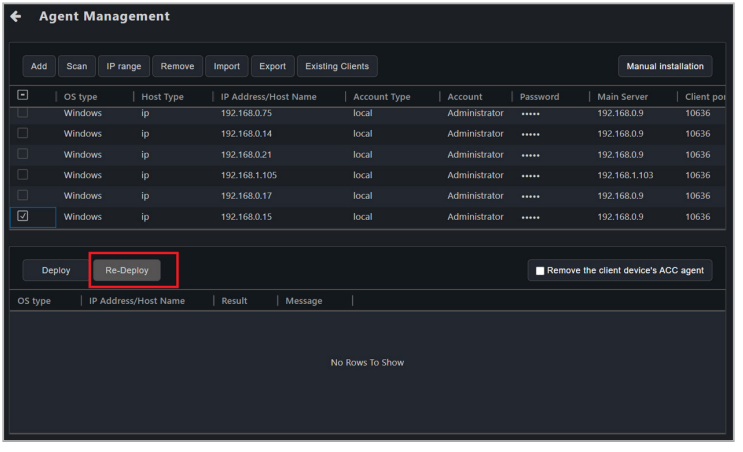
1. Download the latest version of ASUS Control Center Express (1.5.X or later), then run the installation of the ASUS Control Center Express main software on the main server.
2. Click on located at the top right menu bar of the main menu.



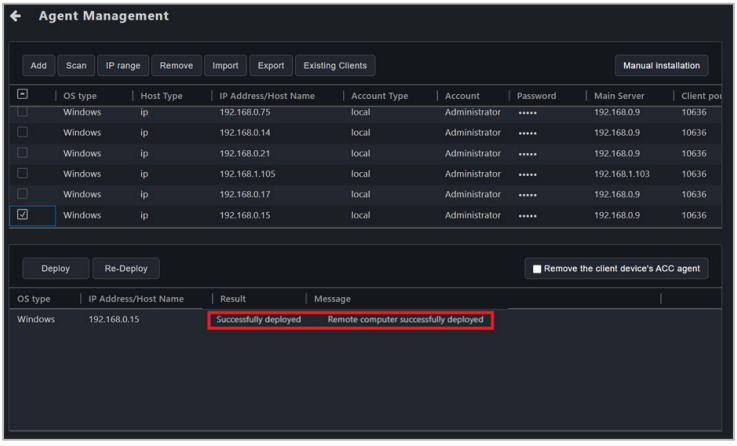
3. Click on **Existing Clients** to load and display all client devices with agents already deployed.



4. Once the list of client devices with agents already deployed has loaded, please check if the information for the client device(s) are correct, such as administrator account and password, for more information you can refer to **3.2.4 Editing device information**. Click **Re-Deploy** once you have confirmed the information of the client device(s) are correct.



5. After the re-deployment is completed, you may view the deploy status in the deploy list.



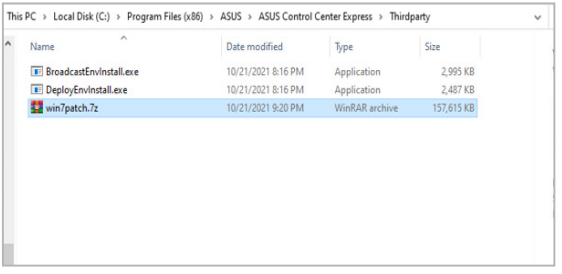
3.2.8 Setting up a Windows 7 deployment environment

You will need to set up the Windows 7 OS environment before deploying an agent if the main server or the client device is using Windows 7 OS.

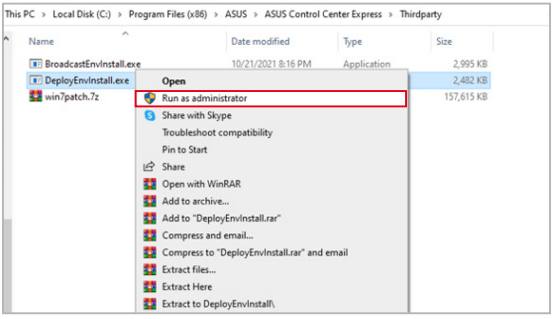
Certain features may not be available on client devices running Windows 7 due to antivirus software incompatibilities.

1. Download the **win7patch** installation file required for setting up the Windows 7 agent deployment environment from the ASUS website.
2. Move the **win7patch** zip file into the same folder as the deployment environment settings file (**DeployEnvInstall.exe**) located in the *ASUS Control Center Express\Thirdparty* installation folder.

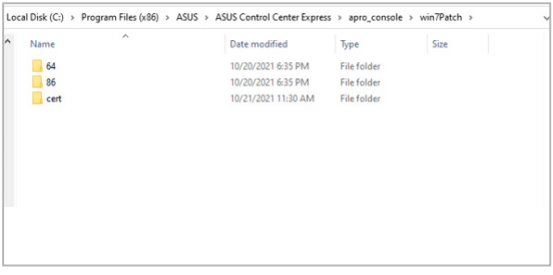
The default installation path for ASUS Control Center Express is *ASUS Control Center Express\Thirdparty*, if you selected a different path when installing ASUS Control Center Express, ensure to change the installation folder path accordingly.



3. Run **DeployEnvInstall.exe** as administrator to set the deployment environment settings.



4. Confirm that the required files for Windows 7 deployment are properly installed in the *ASUS Control Center Express\apro_console* folder.



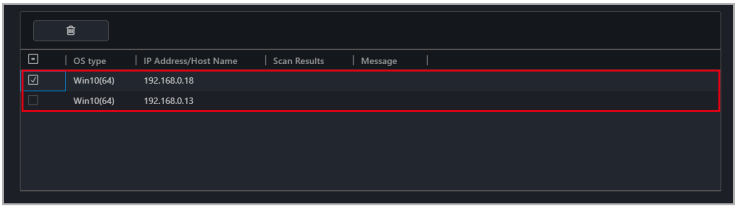
3.3 Removing agents

The screenshots in this section are for reference only.

This section will guide you through the agent removal process if you need to redeploy or remove agents.

3.3.1 Removing agents through main server

1. On the Agent Management page, double click on a single client device to remove the agent on that device, or check multiple devices you wish to remove agents from.



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

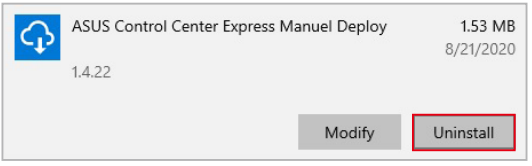
If the selected client device(s) are offline, the agents on these client device(s) will be removed once the client device(s) are online.

3.3.2 Removing manually installed agents

If you manually installed an agent on a client device, please follow the steps below to remove the agent from the client device.

- 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 **3.2 Deploying agents**.
- Ensure to remove the client device from the ASUS Control Center Express server as well as manually remove the agent from the client device.

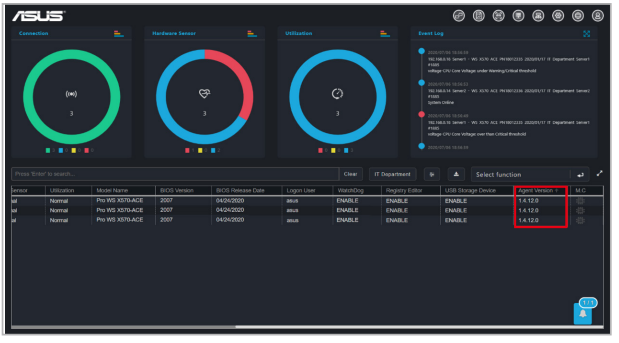
1. Remove the device from the ASUS Control Center Express server, for more details please refer to **3.3.1 Removing agents through main server**.
2. On the client device, navigate to the **Apps & features** menu.
3. Search for ASUS Control Center Express Manual Deploy, then click on it, and click **Uninstall**.

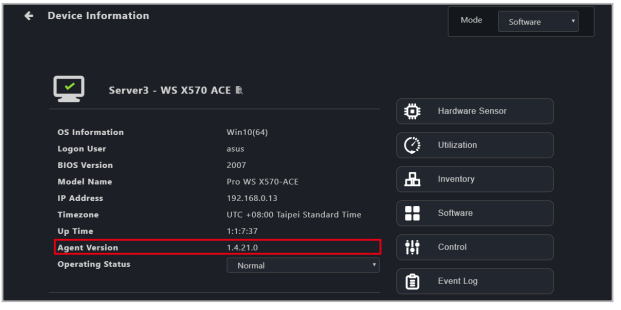


3.4 Client Agent Updater

When your main ASUS Control Center Express server has been updated, you can easily update the agents of all client devices, ensuring your main ASUS Control Center Express main server and client agents are all up to date with the latest updates using the **Client Agent Updater** function.

You can view the current agent version from the device overview on the main menu page or from the **Device Information** page.

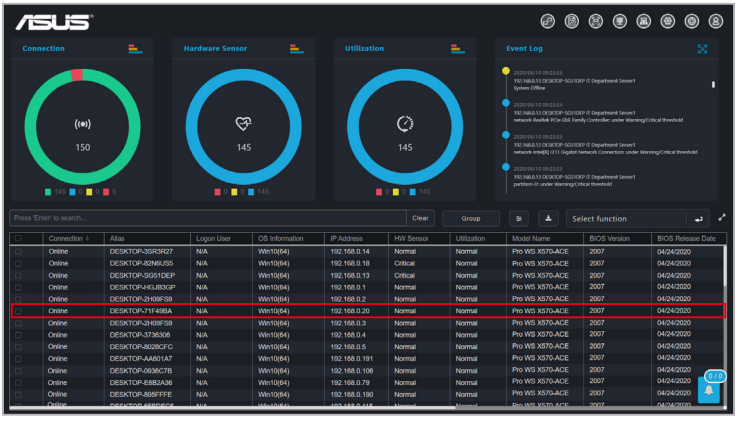




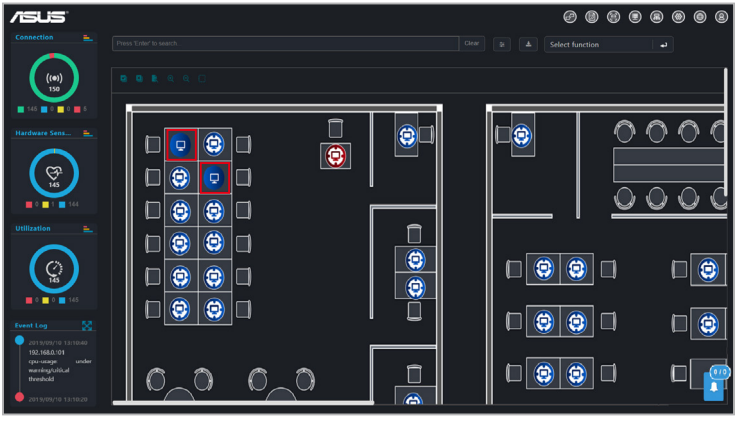
3.4.1 Updating agents

1. Select the devices you would like to perform an agent update on.

Classic dashboard

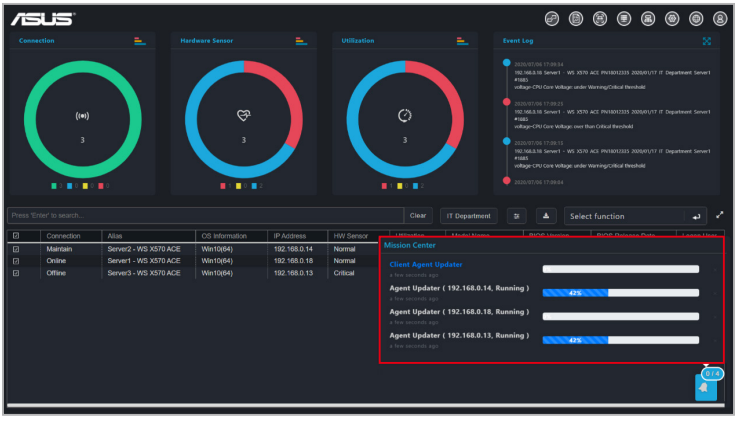


Graphic dashboard

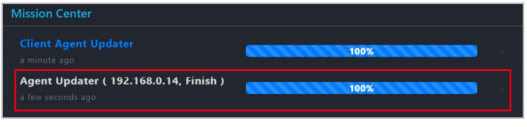


2. Click on **Select function**, then select **Client Agent Updater** from the drop down menu.
3. Click **Yes** on the confirmation pop up window.

4. You can view the agent deploy and update progress in the Mission Center.



- Agent updates can only be performed on client devices that are online. If you selected multiple devices and some of the devices selected are offline, you can view the failure to deploy and update message in the Mission Center, and update these devices when they are online.
- If the connection is unstable during the agent update process, the agent update status on the Mission Center will be displayed as **Finish**, and the task name will become grayed out and unclickable, the agent on the client device will be reverted to the version prior to the update. You can update the client device again when it is online.
- If the client device was powered off or restarted during the agent update process, the agent update status on the Mission Center will be displayed as **Finish**, and the task name will become grayed out and unclickable, and will resume the update process once the client device has restarted and is in OS.



- Certain functions may be affected if the main ASUS Control Center Express server version has already been updated to v1.4.x or above but the client device agent has not been updated (v1.3.x).

Chapter 4

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

Device Information

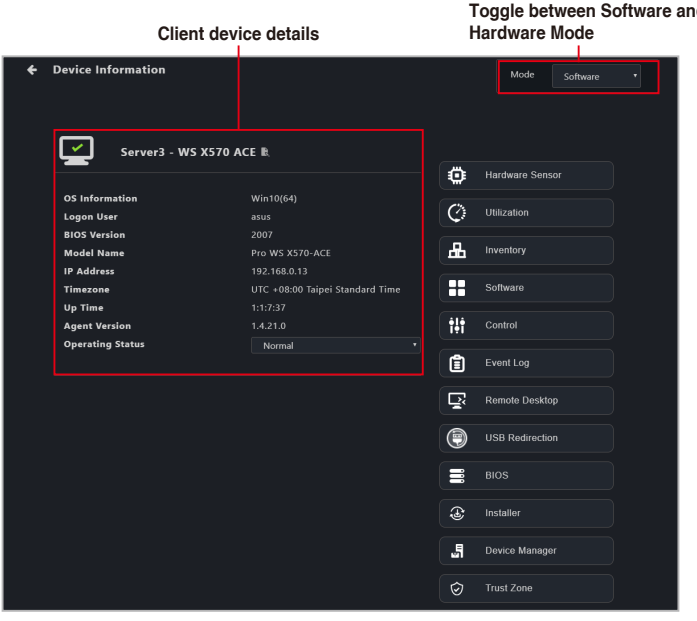
4.1 Device Information Overview

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 views, please refer to the following:

- Classic view: Click on a client device in the device list.
- Graphic 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.



Device Name	Displays the device name. Click on to edit the device name.
OS Information	Displays information on the Operating System.
Logon user	Displays the user logged into client device. If the client device is powered off, offline, or logged out, this field will show the last logged in user enclosed in brackets (“[ ]”).
BIOS Version	Displays information on the BIOS version.
Model Name	Displays the model name of client device.
IP Address	Displays the IP address of client device.
Time Zone	Displays the time zone client device is located in.
Up Time	Displays the up time of client device.
Agent Version	Displays information on the Agent version.
Operating Status	Allows you to set the operating status (**Maintenance**, **Standby**, **Normal**) of the device. For more information please refer to **4.2 Operating Status**.

The Device Information page also allows you to view information or utilize the different functions available to control and manage the device using the functions located to the right of the screen.

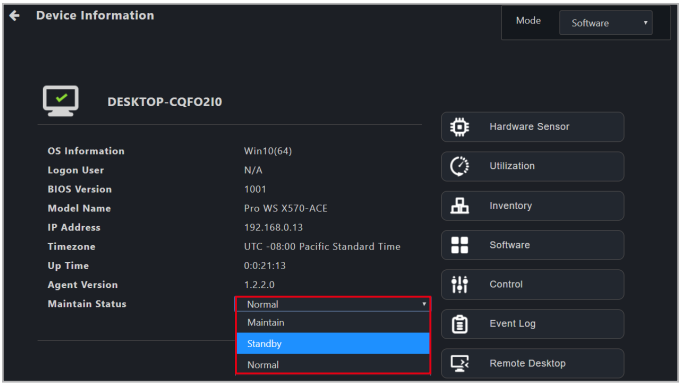
Hardware Sensor	Displays the device hardware sensor information.
Utilization	Displays the device utilization information
Inventory	Displays the device disk information and asset information.
Software	Allows you to view and manage software installed on the device.
Control	Allows you to view and adjust the Regedit, USB storage device, and remote power option settings.
Event Log	Allows you to view, import, or export the device event log.
Remote Desktop	Allows you to remotely control the device.
USB Redirection*	Allows you share a drive of single device.
BIOS	Allows you to manage the device BIOS.
Installer	Allows you to download and update drivers, applications, and BIOS of the device.
Device Manager	Allows you to browse through the Device Manager items of the device.
System Restore	Allows you to create, delete, or restore system restore points for the client device.

4.2 Operating Status

You can set the operating status of a single or multiple devices to **Maintenance**, **Standby**, or **Normal**. You can set the operating status either through the **Device Information** screen or by navigating back to the main menu page, then selecting multiple devices and selecting an operating status in the **Operating Status** field from the **Select Function** drop down menu.

The operating status changes can be viewed on the **Connection** overview. The **Maintenance** or **Standby** operating status will only be displayed when the client device is offline or powered off. If the device is not offline or powered off, it will display it's current connection status as the operating status.

- If a powered off or offline device set to **Maintenance** or **Standby** is powered on or connected to the network, the Connection overview status will display it as **Online**.
- The screenshot below shows the **Operating Status** drop down menu on the **Device Information** screen.



4.3 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 the following for information on **Hardware** mode:

- DASH devices: **5.7.1 Hardware Sensor**
- RTL8117 devices: **5.8.1 Hardware Sensor**
- BMC devices: **5.10.1 Hardware Sensor**

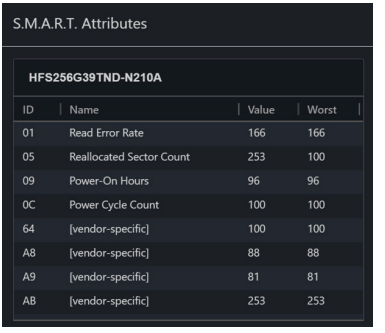
- Some options such as graphics card may only be available if you have the component installed on your client device.
- Click on ▼ to hide or show sub items.
- This item will not be available if your device is not logged into an OS environment, or is not connected using a management LAN port which supports DASH or RTL8117 remote management controller.
- If your motherboard supports a DASH or RTL8117 remote management controller, you may switch to **Hardware** mode, or you may view the hardware sensor information of the previous time the device was powered on if the device is currently powered off.

S.M.A.R.T.

Displays disk status, click on this item to show detailed S.M.A.R.T. attribute information.

The S.M.A.R.T. information will differ according to disk specifications and information provided by the brand.

SATA HDD:



NVMe SSD:

Voltage

Displays the CPU Core Voltage, and other voltage related items. You may edit the threshold for these items.

Temperature

Displays the CPU status and temperature. You may edit the threshold for these items.

Fans

Displays the status and fan speed of connected fans. You may edit the threshold for these items.

Graphics Card

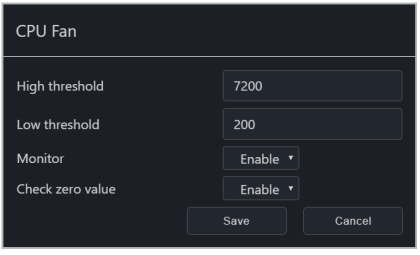
Displays the fan speed, voltage and temperature of NVIDIA or AMD graphics cards. You may edit the threshold for these items.

The information displayed may vary according to the support of the graphics card's driver. Items not supported will be displayed with a **Hardware sensor is not supported by the graphics driver** message.

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.

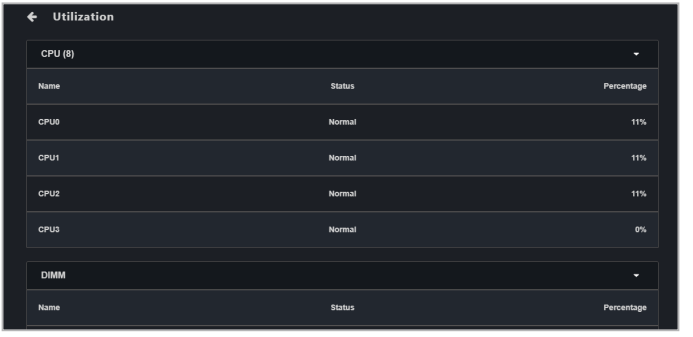


High threshold	When the value exceeds this threshold value, the sensor will display **Warning (Yellow)**. When the value exceeds this threshold value by 20%, the sensor will display **Critical (Red)**.
Low threshold	When the value is below this threshold value, the sensor will display **Warning (Yellow)**.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

4.4 Utilization

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

Click on ▾ to hide or show sub items.



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

Editing the threshold value

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

High Critical	When the value exceeds this threshold value, the sensor will display **Critical (Red)**.
High Warning	When the value exceeds this threshold value, the sensor will display **Warning (Yellow)**.

4.5 Inventory (Software)

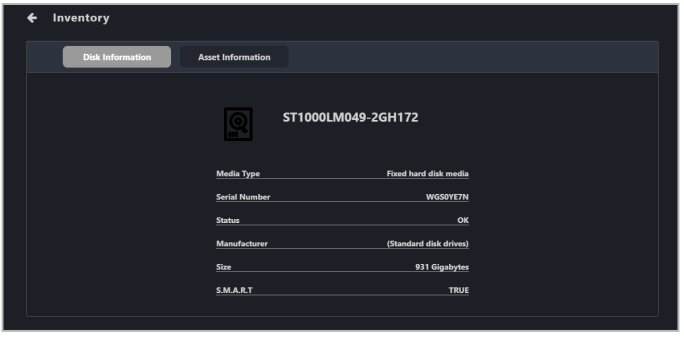
This item will not be available if your device is not logged into an OS environment, or is not connected using a management LAN port which supports a remote management controller.

This item displays more details about a single client device and disk. This item is software controlled and values may differ with the hardware version. Please refer to the following for information on **Hardware** mode:

- DASH devices: **5.7.2 Inventory**
- RTL8117 devices: **5.8.2 Inventory**
- vPro devices: **5.9.1 Inventory**
- BMC devices: **5.10.2 Inventory**

4.5.1 Disk Information

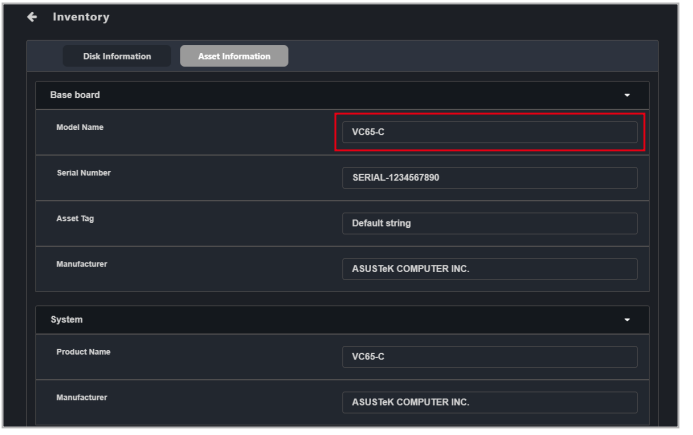
Click on **Disk Information** for more details on the disk.



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

4.5.2 Asset Information

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



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

4.6 Software

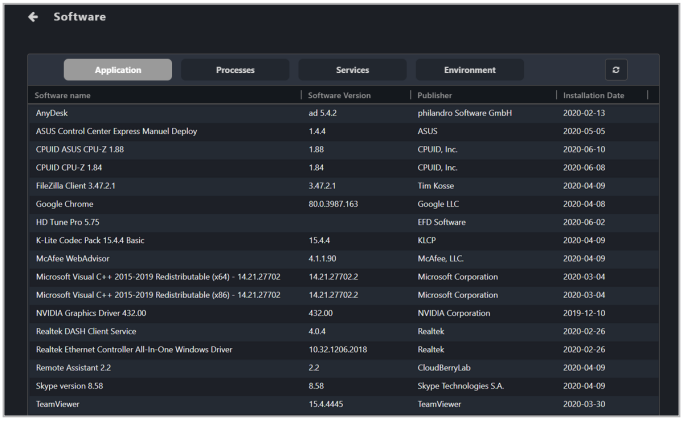
This item displays details on the software and applications of a single device with the **Application**, **Processes**, **Services**, and **Environment** tab.

- Some operating system applications, processes, and services cannot be removed, terminated, or stopped.
- Clicking on a column header will sort the information alphabetically based on the items in that column.

4.6.1 Application tab

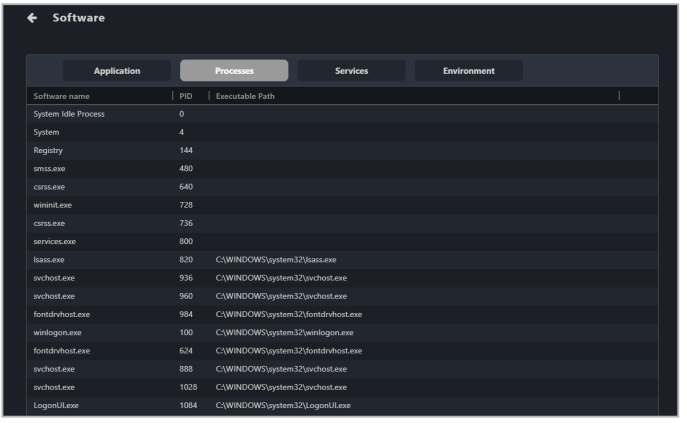
The **Application** tab allows you to view information on installed applications on the client device. You may also click on an application then select **Uninstall** to uninstall the application.

- The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.
- Click on the (Refresh) button to immediately refresh and update the software list.



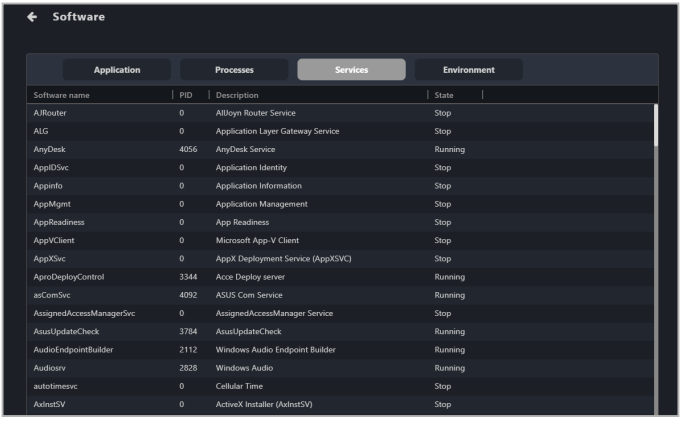
4.6.2 Processes tab

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.



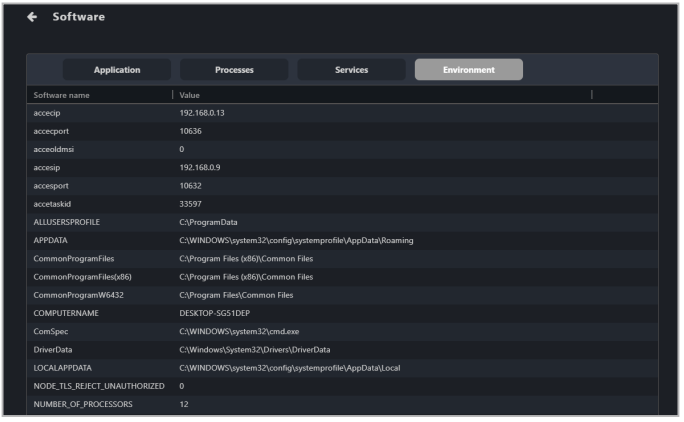
4.6.3 Services tab

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**.



4.6.4 Environment tab

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

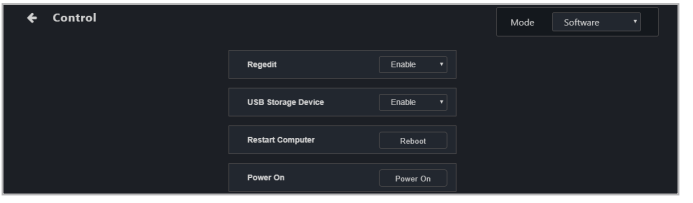


4.7 Control (software)

- This item will not be available if your device is not logged into an OS environment.
- If the below settings have not previously been configured using ASUS Control Center Express, the default value of “Not config” will be displayed.
- Use the Mission Center to check if the task was completed successfully. Refer to the **Mission Center** section for more information.

This item allows you to configure system, USB, power, and boot options. This item is software controlled and values may differ with the hardware version. Please refer to the following for information on **Hardware** mode:

- DASH devices: **5.7.3 Control**
- RTL8117 devices: **5.8.3 Control**
- vPro devices: **5.9.2 Control**
- BMC devices: **5.9.3 Control**



Enable/Disable Regedit	Enable or disable the Windows Registry Editor.
USB Storage Device	Enable or disable the USB port, or set it to Read Only.
Restart Computer	Restart the client device.
Power On	Power on the client device. If Wake on LAN is supported on the client device, the client device can be powered on using this function when the client device is powered off.
Power Off	Power off the client device.
Fast Startup	Enable or disable fast startup for the client device.
Windows Update	Enable or disable Windows Update for the client device.
Set Management Controller	Set the IP address of the vPro management controller. This function is only supported if the client device supports vPro remote management.

4.8 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**.

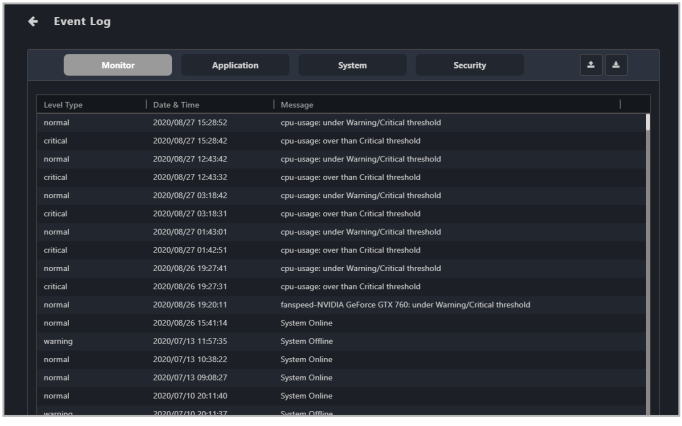
This item is software controlled and information available may differ with the hardware version. Please refer to the following for information on **Hardware** mode:

- RTL8117 devices: **5.8.9 Event Log**

Clicking on a column header will sort the information alphabetically based on the items in that column.

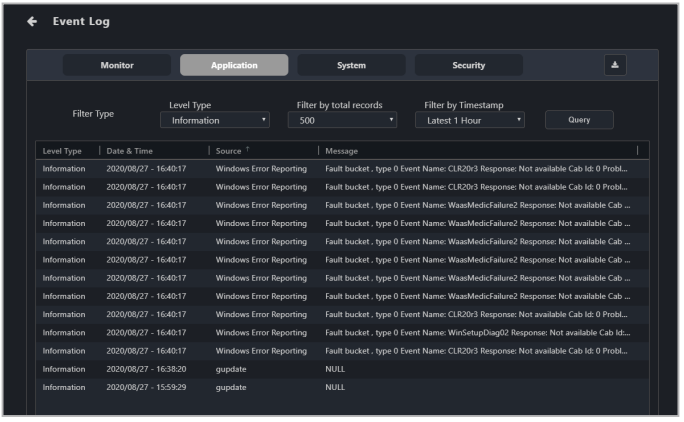
4.8.1 Monitor tab

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.



4.8.2 Application tab

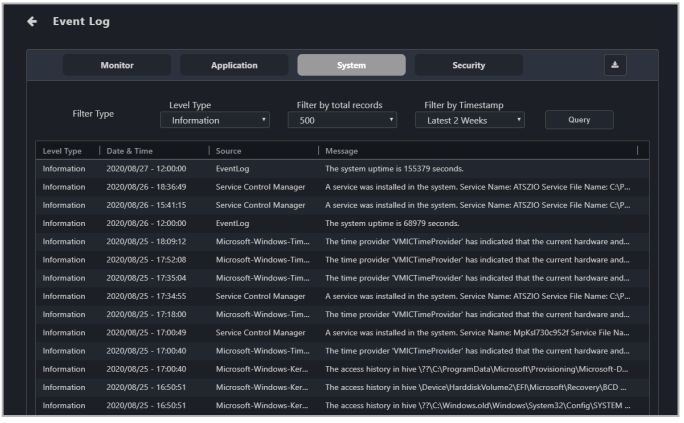
The **Application** tab allows you to filter application related events by selecting your filter criteria from the **Filter Type** block, then clicking **Query**.



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

4.8.3 System tab

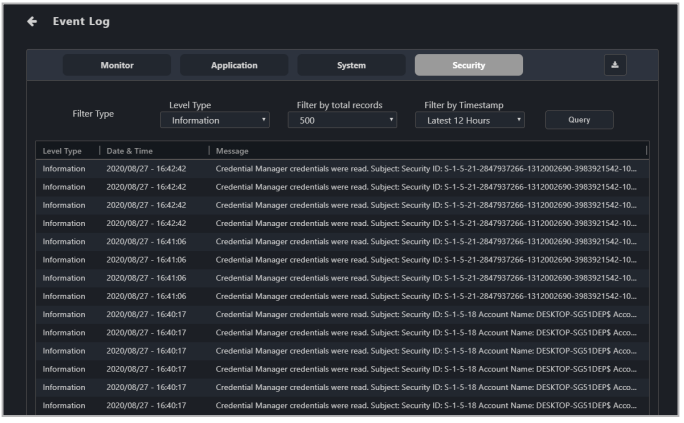
The **System** tab allows you to filter system related events by selecting your filter criteria from the **Filter Type** block, then clicking **Query**.



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

4.8.4 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**.



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

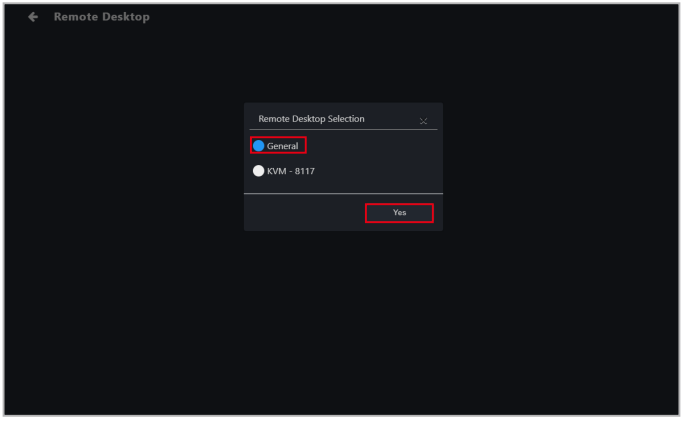
4.9 Remote Desktop (General)

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

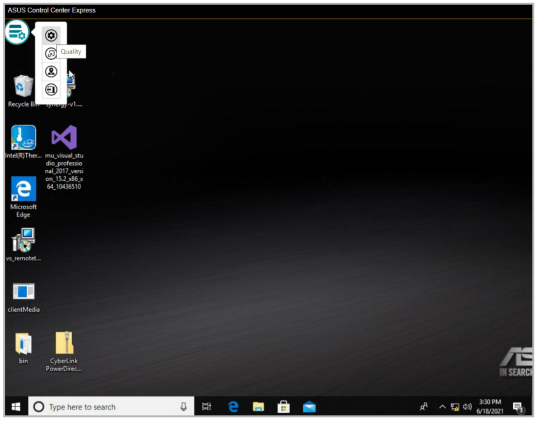
If your client device supports remote management controller (RTL8117) or vPro, a window should appear allowing you to select between **General**, **KVM - 8117**, or **KVM - vPro**. Select **General** and click on **Yes** to remotely control the client device; else it should enter the remote desktop directly. Please refer to the following for information on **Hardware** mode:

- RTL8117 devices: **5.8.4 Remote Desktop**
- vPro devices: **5.9.3 Remote Desktop**

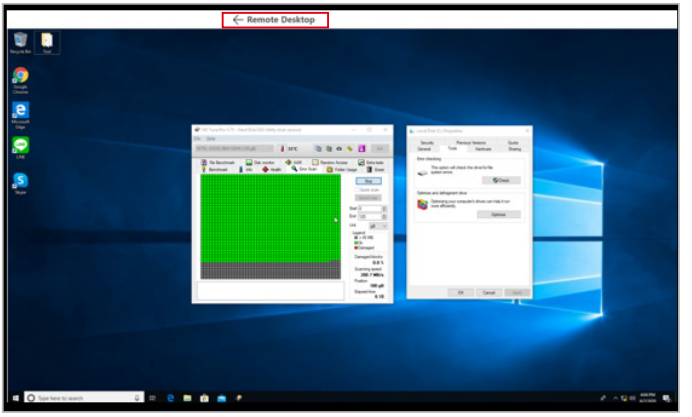
The client device should be powered on and logged into an OS environment.



After the connection is successful, you can select the remote desktop function or remotely control the connected device.



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



Remote desktop functions

You can adjust the different remote desktop functions such as image quality, screen size, and locations of function buttons.

- The remote desktop functions will differ between the **KVM - 8117** and **General** remote desktop.
- The function button for **Mouse display status** is hidden by default and only shown if there are zero displays and one or more mice connected to the client device.

Quality	Adjust the remote desktop image quality.
Resize	Select between Window Size and Screen Size.
Set button position	Adjust the default position of the remote desktop functions on the screen.
Mouse display status	Select whether to show, hide, or automatically manage the visibility of the connected client's mouse cursor.
Exit	Exit the remote desktop and return to the ASUS Control Center Express main software.

4.10 BIOS

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

If you access the BIOS page from **Device Information** you will only be able to view, manage BIOS settings, or update the BIOS of the selected device. To view, manage BIOS settings, or update the BIOS of multiple devices, please navigate back to the main menu page, then select multiple devices and select **Smart BIOS** from the **Select Function** drop down menu.

This item is software controlled and information available may differ with the hardware version. Please refer to the **Management Functions** chapter for information on the hardware mode.

4.10.1 BIOS Flash Management

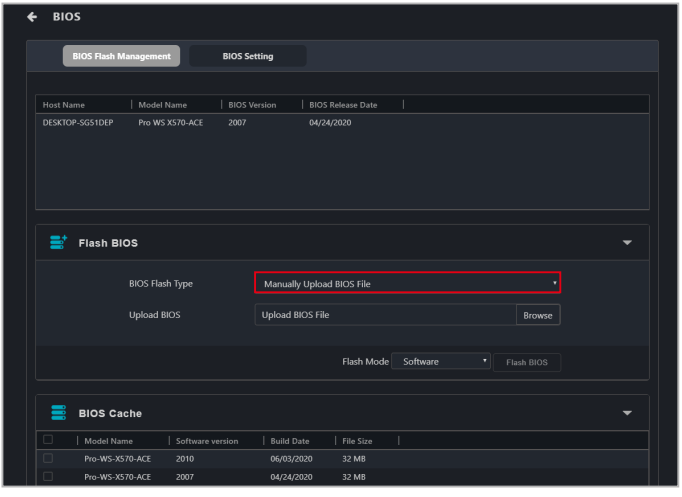
You can flash the BIOS by manually uploading a BIOS file or by selecting a previously flashed BIOS file from the BIOS cache. You may also remove BIOS files from the BIOS cache if needed.

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.

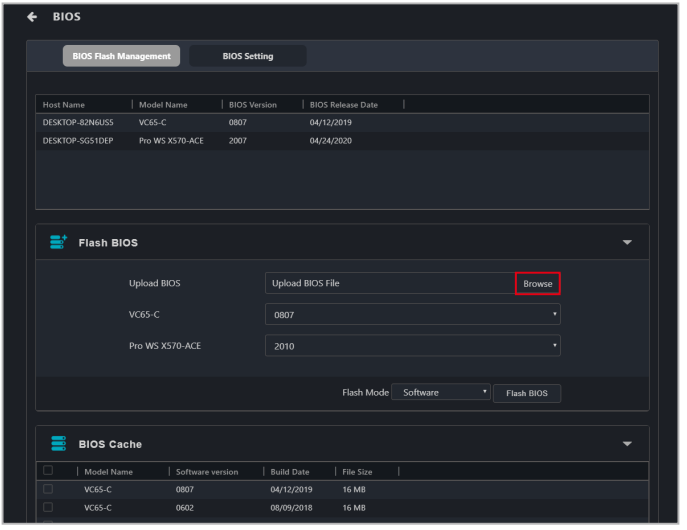
1. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.

This option will only appear if a single device was selected.

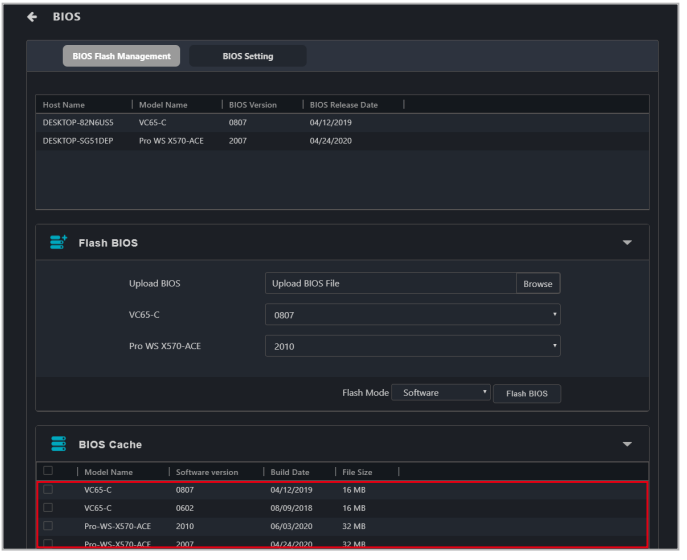


2. Click on **Browse** to select a BIOS file.

- BIOS files for multiple devices need to be uploaded separately.
- The illustration below shows the options for multiple devices selected.

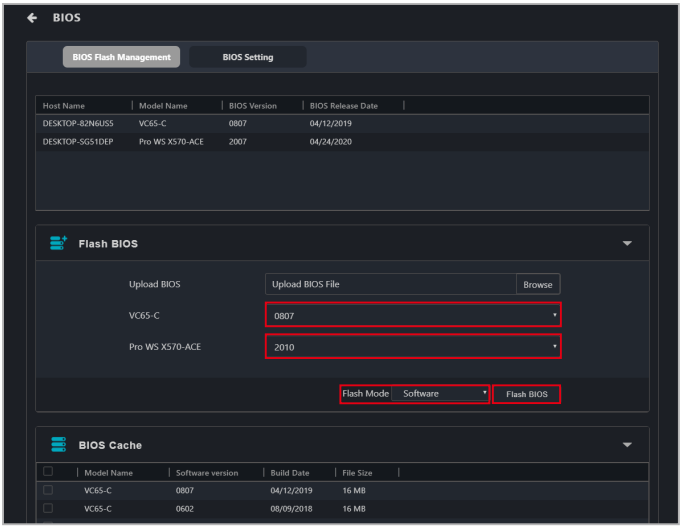


3. Confirm that the BIOS file was successfully uploaded and click **OK**. The uploaded BIOS file will also be added to the **BIOS Cache**.



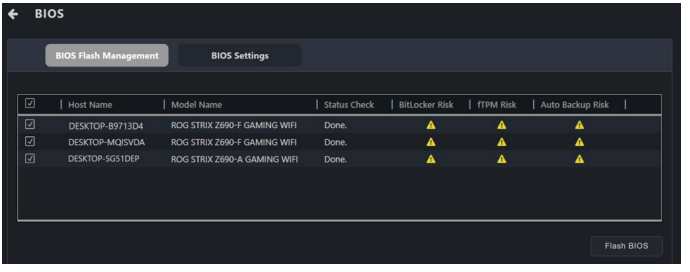
4. (for multiple devices) Select the BIOS you wish to flash on the devices selected from the drop down menu next to each model name.
5. Select your **Flash Mode**, then click on **Flash BIOS**.

Hardware Flash Mode is only available if the client device is connected using a management LAN port which supports remote management controller.



6. The client device will automatically be checked for potential issues that may affect the BIOS flashing procedure. Serious risk of data loss may occur if you proceed without resolving these issues. Carefully review the **Status Check**, **BitLocker Risk**, **Auto Backup Risk**, and **fTPM Risk** columns before proceeding.

- For **Status Check** issues, confirm if the ASUS Control Center Express agent on the client device is updated to version 1.6.3 or later.
- For **BitLocker Risk** issues, confirm if BitLocker is suspended on the client device. Proceeding anyway may trigger BitLocker encryption that is irreversible without the BitLocker recovery key.
- For **fTPM Risk** issues, confirm if fTPM is disabled on the client device. Proceeding anyway may irreversibly erase fTPM security data.
- For **Auto Backup Risk** issues, ASUS Control Center was not able to automatically backup the BitLocker recovery keys. It is strongly recommended to manually back up the BitLocker recovery keys before proceeding. Refer to Microsoft documentation on BitLocker for more information.



7. If you would like to automatically shutdown the client device when the BIOS update is completed, please click **Yes** on the pop up window. If you would like to manually shutdown the client device click **No**.

   If you selected **Yes**, the device will automatically shutdown after the update and this action will be reflected in the Mission Center.

   If you selected **No**, the device will update the BIOS and the update result will appear in the Mission Center. Click on the update result in the Mission Center and click **Shutdown** to manually shutdown the device.

Flashing BIOS from the BIOS cache

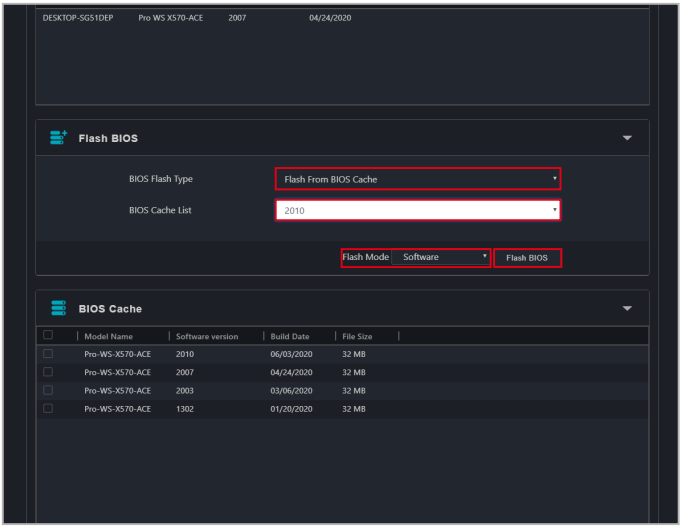
You can select a BIOS file from the BIOS cache.

1. Select **Flash from BIOS Cache** in the **BIOS Flash Type** field.

> This option will only appear if only a single device was selected.

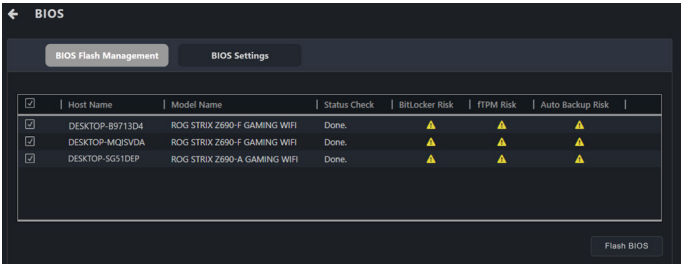
2. An applicable BIOS file should be automatically selected, if you wish to select another BIOS file, click on the **BIOS Cache List** drop down menu. Ensure to select a BIOS file for all devices if you are updating the BIOS for multiple devices.
3. Select your **Flash Mode**, then click on **Flash BIOS**.

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



4. The client device will automatically be checked for potential issues that may affect the BIOS flashing procedure. Serious risk of data loss may occur if you proceed without resolving these issues. Carefully review the **Status Check**, **BitLocker Risk**, **Auto Backup Risk**, and **fTPM Risk** columns before proceeding.

- For **Status Check** issues, confirm if the ASUS Control Center Express agent on the client device is updated to version 1.6.3 or later.
- For **BitLocker Risk** issues, confirm if BitLocker is suspended on the client device. Proceeding anyway may trigger BitLocker encryption that is irreversible without the BitLocker recovery key.
- For **fTPM Risk** issues, confirm if fTPM is disabled on the client device. Proceeding anyway may irreversibly erase fTPM security data.
- For **Auto Backup Risk** issues, ASUS Control Center was not able to automatically backup the BitLocker recovery keys. It is strongly recommended to manually back up the BitLocker recovery keys before proceeding. Refer to Microsoft documentation on BitLocker for more information.



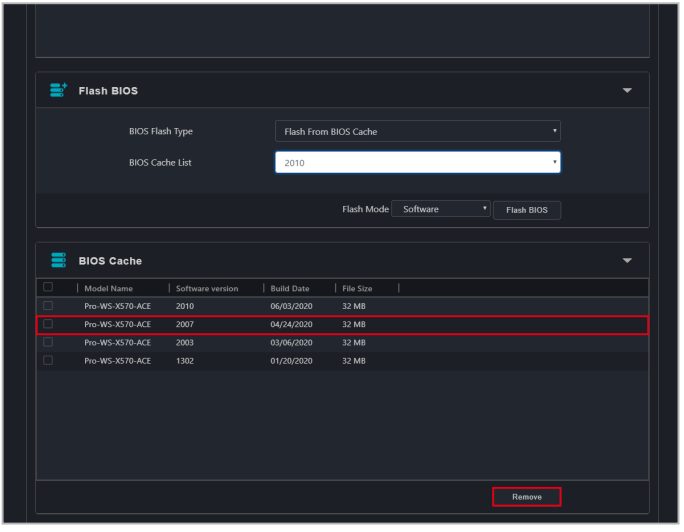
5. If you would like to automatically shutdown the client device when the BIOS update is completed, please click **Yes** on the pop up window. If you would like to manually shutdown the client device click **No**.

   If you selected **Yes**, the device will automatically shutdown after the update and this action will be reflected in the Mission Center.

   If you selected **No**, the device will update the BIOS and the update result will appear in the Mission Center. Click on the update result in the Mission Center and click **Shutdown** to manually shutdown the device.

Removing a BIOS file from the BIOS cache

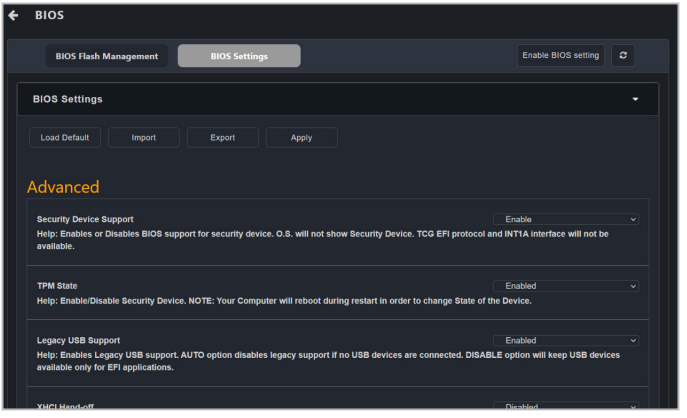
You can view the BIOS files available for the client device in the BIOS Cache block. To remove a BIOS file from the BIOS Cache, check the BIOS file you wish to remove, then click on **Remove**.



4.10.2 BIOS Setting

Adjust the BIOS **Advanced**, **Boot**, **Monitor** and **Security** settings of a single client device, or multiple client devices.

- When the BIOS Setting function is initiated, you will be prompted for the BIOS password of the client device. If a password is not set, leave the field blank and press **OK** to continue.
- On client devices that support protected BIOS system environment variables, entering an incorrect password five times will lock the BIOS settings. If this occurs, restart the client device to unlock the BIOS 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.
- When multiple devices are selected, only BIOS settings that are available on all devices will be displayed in the **BIOS Setting** tab. If there are different values or configurations between devices for the common options, the configuration will be displayed as a blank option.



BIOS Setting functions:

Please refer to the table below for the different functions you can use on the BIOS Setting page:

Enable BIOS setting	Enable the BIOS setting for a client device that has the BIOS setting disabled.
Load Default	Loads the default factory BIOS settings. When using this function, you will be required to enter the BIOS administrator password set for the client device.
Import	Import the client device's BIOS settings.
Export	Export the client device's BIOS settings.
Apply	Applies the changes made in the BIOS Setting page to the BIOS of the client device. When using this function, you will be required to enter the BIOS administrator password set for the client device.

- Ensure to restart the client device if changes were made to the BIOS, or if the default BIOS settings were loaded for the changes to take effect.
- If the BIOS administrator password has not been set on the client device, please click on **OK** on the password prompt window without entering a password when using the **Load Default** and **Apply** functions.

BIOS Setting items:

Advanced	Configure the client device's advanced BIOS settings.
Boot	Configure the client device's BIOS boot settings.
Boot Priority	Configure the client device's BIOS boot priority.
Monitor	Configure the client device's BIOS monitoring settings.
Security	Configure the client device's BIOS password.

- If the client device does not have BIOS settings enabled, ASUS Control Center Express will not be able to display the BIOS settings of the client device. Please click on Enable BIOS setting, and restart the client device to configure the BIOS settings of the client device.
- You can enable, disable, or reorder items in the Boot Priority menu, if supported by the BIOS on the client device.

4.11 Installer

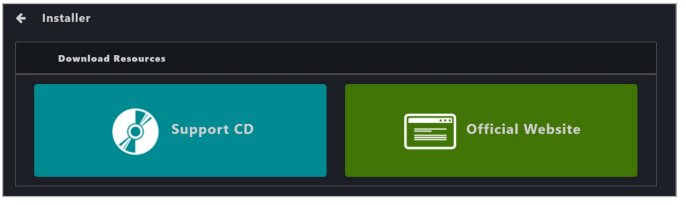
Ensure the main server is connected to the Internet and has a stable connection.

This item will allow you to download and update the driver, utility application, and BIOS for a single or multiple devices.

If you access the Installer page from **Device Information** you will only be able to download and update the driver, utility application, and BIOS of the selected device. To download and update the driver, utility application, and BIOS of multiple devices, please navigate back to the main menu page, then select multiple devices and select **Software Management** > **Installer** from the **Select Function** drop down menu.

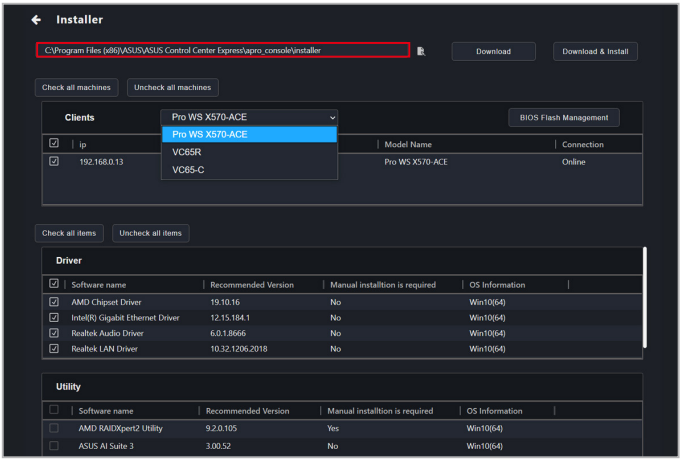
- When selecting multiple devices, ensure that most devices selected are online (some devices may be offline), as the download and install process is only applied to online devices. If all devices selected are offline, you will be prompted with a message asking you to select online devices.
- ACCE will display the versions of drivers, utility applications, and BIOS already installed only when a single device is selected.
- ACCE will automatically check for updated or recommended drivers and utility applications for download and installation only when a single device is selected.

1. On the **Installer** page, select if you would like to download from the Support CD or from the Official Website.

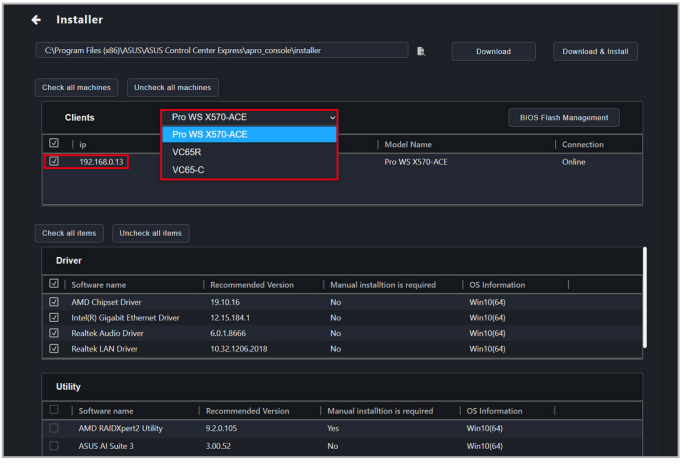


Support CD	Downloads and installs drivers, applications, and BIOS from the latest Support CD version for the selected device(s).
Official Website	Downloads the recommended version of drivers and applications from the official website for the selected device(s).

2. Click the **Edit** button to select a new download path. If unspecified, the default path will be used.



3. Select a model from the drop down menu, then select the client device(s) you wish to download software for.

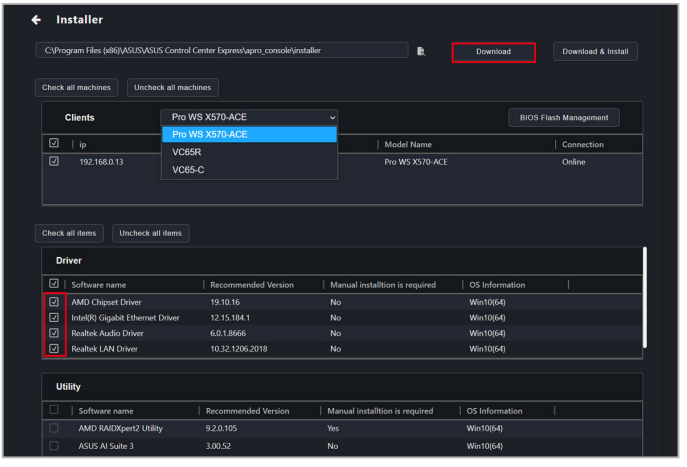


4. If you selected Official Website as the download source, use the **Operating System** dropdown list to select the operating system version.

This item only appears when Official Website is selected.

5. Select the software you would like to download, then click on **Download** or **Download & Install**.

- **Download & Install** is only available when Support CD is selected.
- Scroll down to view and select available drivers, utilities, and BIOS files. The items displayed may vary between device model.
- The **Driver**, **Utility**, and **BIOS** blocks will display items already installed, as well as recommended available updates.
- Drivers and utility applications marked **Yes** in the **Manual installation is required** column require manual installation on the client device (the installation files can be found in the download path you selected on the client device).
- Downloaded BIOS files on the main server will automatically be uploaded to the BIOS cache. Click **BIOS Flash Management** to update the BIOS after the download is complete.
- You can click **Check all items** to select all available downloads, or click **Uncheck all items** to clear the selection.
- The selected software will be downloaded to the specified download path on the ASUS Control Center Express main server.



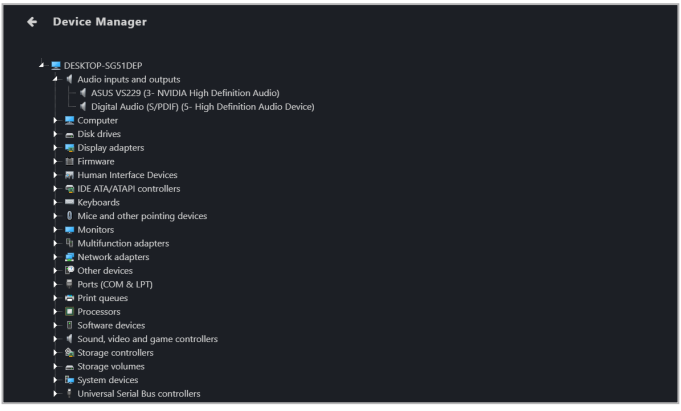
6. A status bar will display the download status. Click **OK** once the download is completed.

4.12 Device Manager

This item will allow you to view the client device's Device Manager information, allowing you to checkup on hardware, troubleshoot or locate hardware failures, system resource problems, or driver problems.

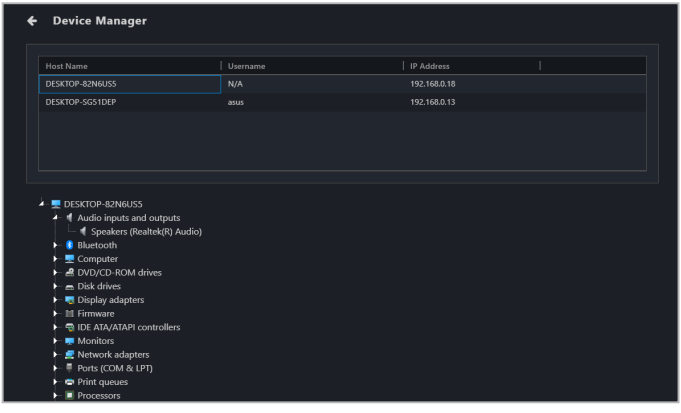
If you access the Device Manager page from **Device Information** you will only be able to view the Device Manager of the selected device. To view the Device Manager of multiple devices, please navigate back to the main menu page, then select multiple devices and select **Device Manager** from the **Select Function** drop down menu.

Single device

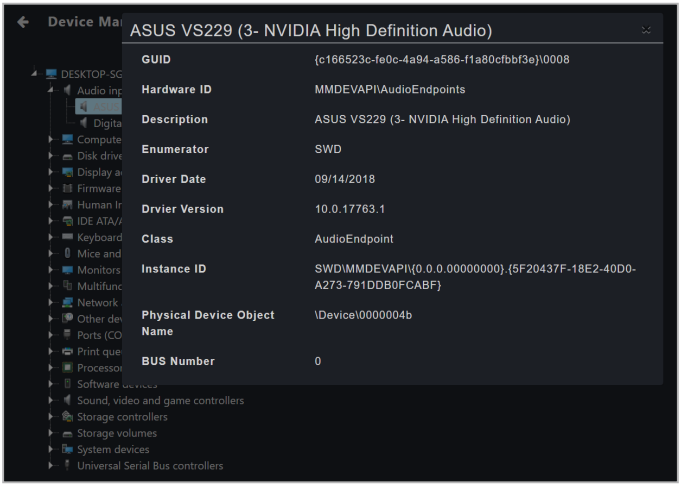


Multiple devices

Click on a device to display the Device Manager information of the device below

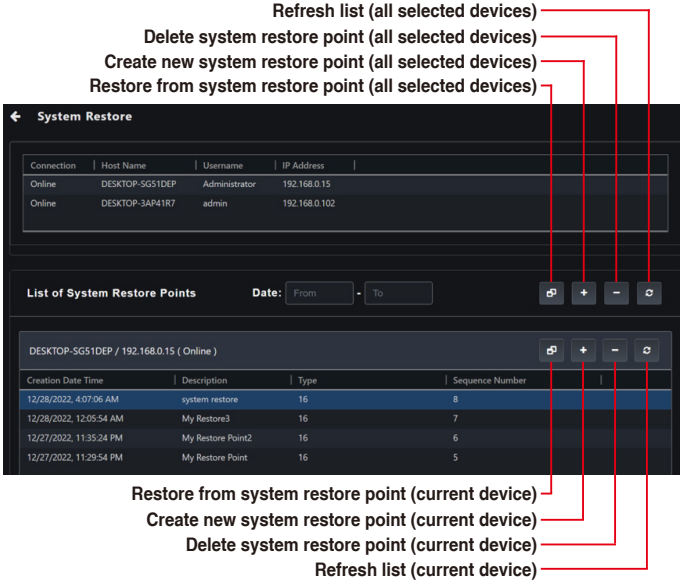


Clicking on a hardware device will allow you to view the details on the hardware device.



4.13 System Restore

Select one or more client device(s) from the device list to create, restore from, and delete system restore points.



- System restore will be enabled on the client device(s) if not already enabled.
- Create, delete, and restore functions are only available when the client device(s) are powered on and connected.
- Depending on network conditions, the list of system restore points may take some time to update. Click the Refresh button to manually initiate an update.

Creating a system restore point

1. Click the + Create button.
2. (Optional) Fill in the **Restore Point Description** field.
3. Click **Create**.

Deleting a system restore point

1. Select a system restore point from the system restore point list.
2. Click the − Delete button.
3. Click **Delete**.

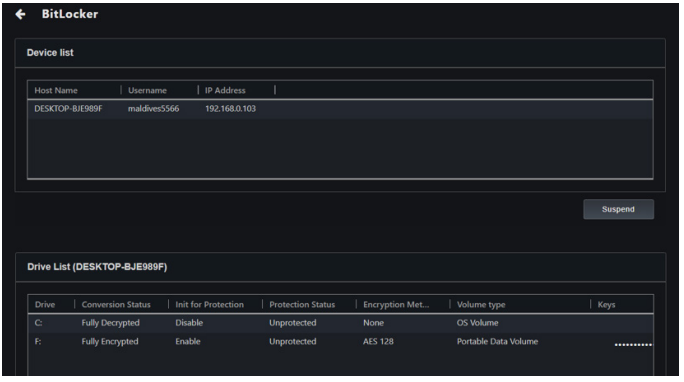
Restoring from a system restore point.

1. Select a system restore point from the system restore point list.
2. Click the Restore button.
3. Tick the checkbox to automatically restart the client device(s) after the system restore is complete, then click **Restore**.

If this checkbox is not ticked, the client device(s) should be manually restarted after the system restore is complete.

4.14 BitLocker

This item will allow you to view and configure BitLocker status and backup or restore BitLocker keys.



Suspending BitLocker encryption

1. Click **Suspend**.

Suspending BitLocker encryption will suspend encryption for the entire drive, regardless of partition.

2. Fill in the **Count** field to set the amount of client device restarts before BitLocker encryption is automatically reenabled, then click **Save**.

As an example, if the **Count** field is set to 2, BitLocker will automatically be reenabled after the client device restarts twice.

3. Use the Mission Center to check if the task was completed successfully. Refer to the **Mission Center** section for more information.

Viewing BitLocker information

You can view information about the BitLocker status of each drive in the **Drive List**.

If the operating system of the client device does not support BitLocker, the **Protection Status** field of the **Drive List** will show “Unknown”.

Drive	Displays the drive letter.
Conversion status	Displays the encryption status.
Initialize protection	Displays the protection initialization status.
Protection status	Displays the protection status.
Encryption method	Displays the encryption method.
Volume type	Displays the volume type.
Keys	Displays the encryption key.
Hide keys	Click to hide the encryption key.
Backup	Click to back up the encryption key.

Chapter 5

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

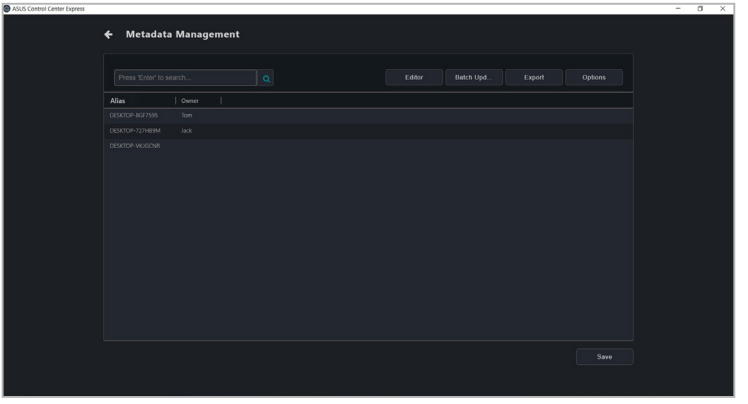
Management Control

The screenshots in this chapter are for reference only.

5.1 Metadata Management

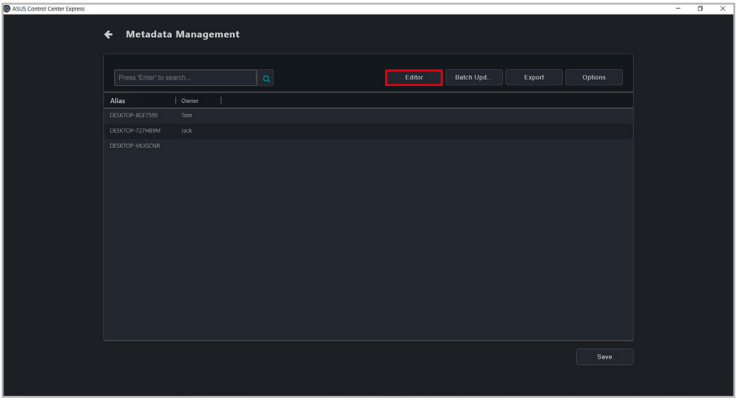
This item allows you to add or edit metadata fields and information which is displayed when viewing device information.

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



5.1.1 Adding metadata fields

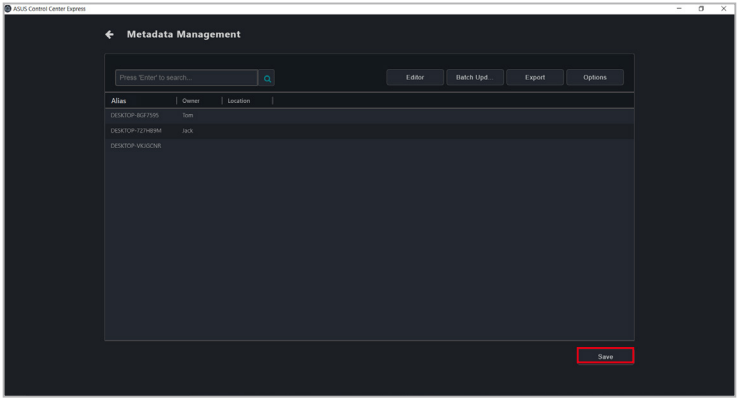
1. Click on **Editor**.



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

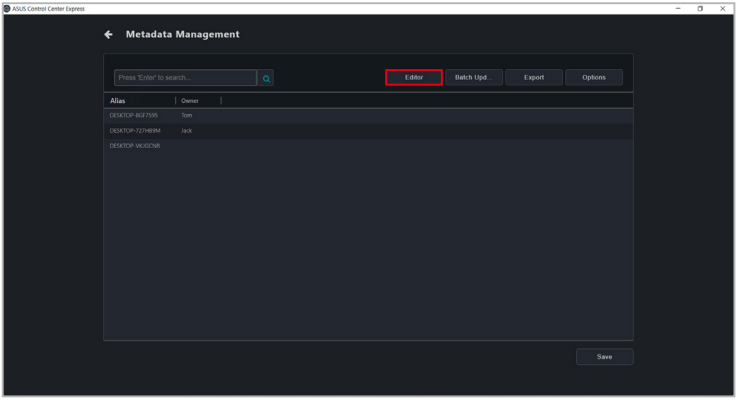
3. Your new metadata field should appear in the metadata management list, click on **Save** to save the changes done.

For this example we have added the “Location” metadata field.



5.1.2 Removing metadata fields

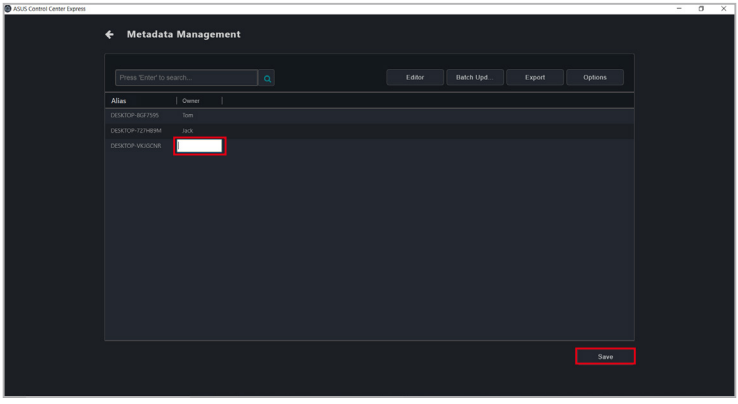
1. Click on **Editor**.



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

5.1.3 Updating the metadata manually

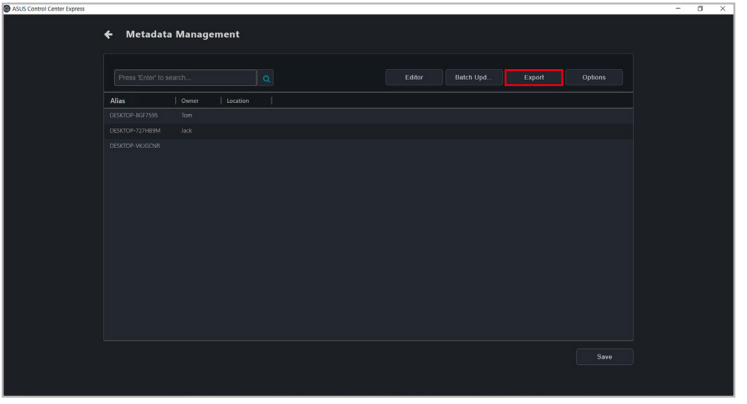
You can edit the default metadata such as Alias, or user defined metadata of each device by double clicking on the cell of the field you would like to update, then clicking on **Save** once you are finished to save the changes made. Allowing you to quickly edit the metadata of multiple devices.



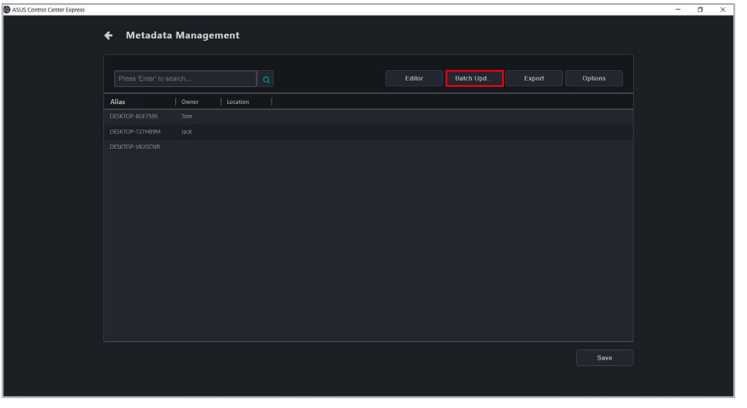
5.1.4 Updating the metadata using a batch update

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

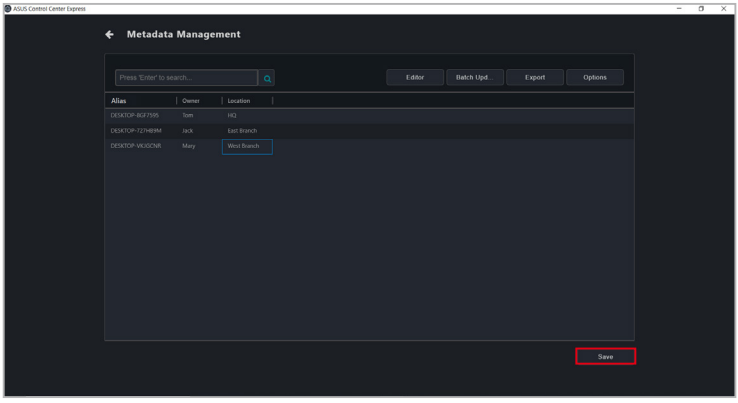
To customize which metadata fields to export, click on **Options**, then select the metadata fields you wish to export. Deselecting a metadata field will hide the metadata field and will not add that field to the exported .csv file.



2. Update the exported .csv file with the data you wish to populate the metadata fields on ASUS Control Center Express.
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.



5.2 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, blacklisting software, or setting software rules on selected client devices.

5.2.1 Software Dispatch

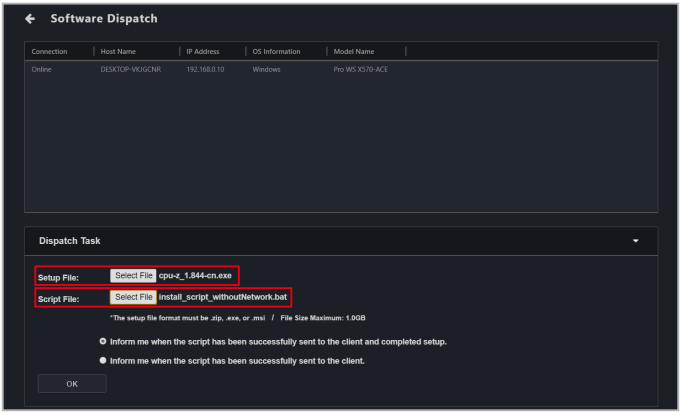
This item allows you to dispatch software setup and script files.

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

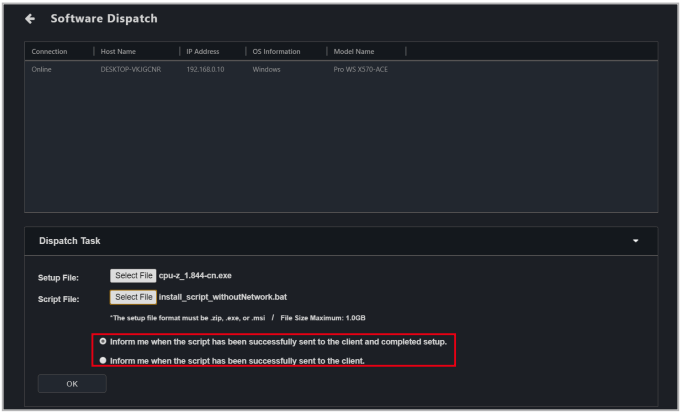
Dispatching software to client device

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

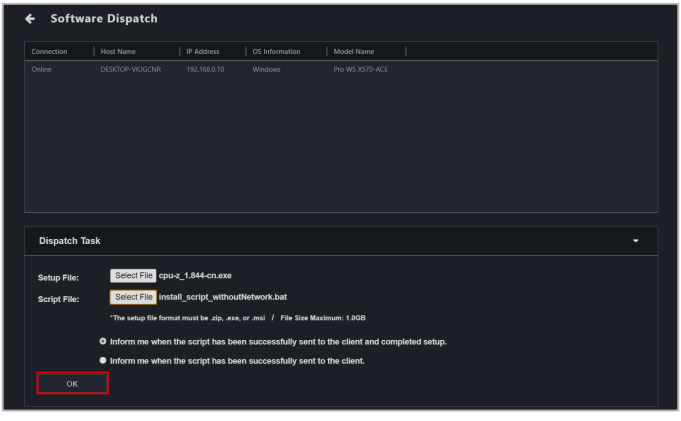
- The following setup file formats are supported: .zip, .exe, or .msi.
- The file size of the setup file should not exceed 1.0 GB.
- If you need to package the software setup file and batch file into a zip file, please ensure to rename the batch file to **install_script.bat** before packaging the files.



2. (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.

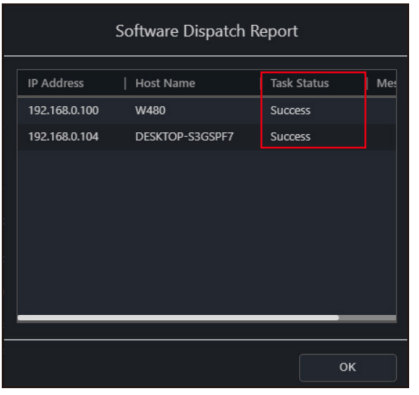


3. Click on **OK**, then wait for the software dispatch process to finish. Once it is completed you should receive a notification based on the notification scenario selected.

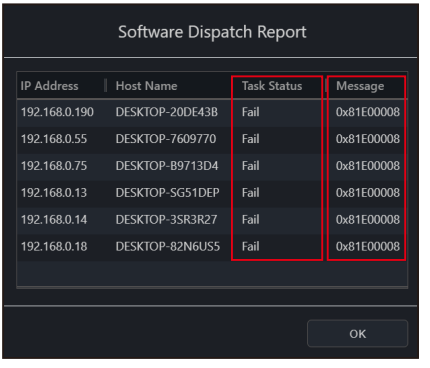


The software dispatch process will not display any software installation user interface or notices. Ensure the software you dispatch supports silent mode - an installation that requires no user interaction, and has a script file to execute the installation process in order for the software to automatically install in the background.

4. The dispatch progress and results can be viewed in the Mission Center. If the dispatch was successful, **Success** will be displayed in the **Task Status** column.

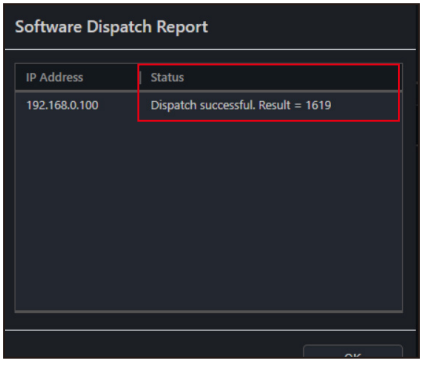


If the dispatch was unsuccessful, **Fail** will be displayed in the **Task Status** column, and a dispatch message code will be displayed in the Message column. Please refer to the table below for the dispatch message codes.



Message code	Details
0x81E00000	Unable to retrieve data returned by the server.
0x81E00004	Unable to parse data returned by the server.
0x81E00007	Unable to obtain data returned by the client device.
0x81E00008	Please check the connection status of the client device.

The setup results can also be viewed in the Software Dispatch Report



- Please refer to the MsiExec.exe and InstMsi.exe error message descriptions if the software dispatch results and message codes were returned by the Windows Installer response file script.
- Software installation may be affected by the OS anti-virus. If you are certain there are no problems with the software package and script file but the installation is still unsuccessful, you can try temporarily disabling the anti-virus on the client device during the dispatch and installation process.

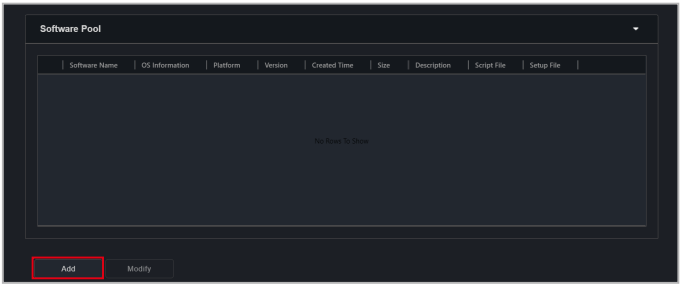
5.2.2 Software Pool

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

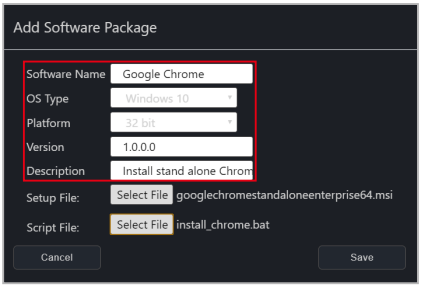
To access the software pool, select the client device(s) and click on **Select Function** > **Software Management** > **Software Dispatch**, then scroll to the bottom of the **Software Dispatch** screen.

Adding software packages to the Software Pool

1. Click on **Add**.

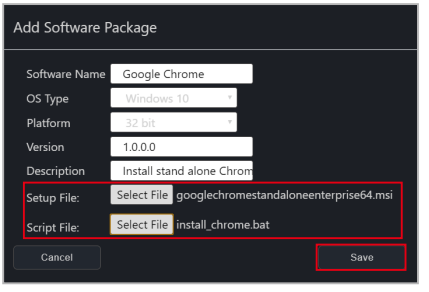


2. Enter the required information into the **Software Name**, **OS Type**, **Platform**, and **Version** fields. You may also type in a brief description of the software package into the **Description** field.

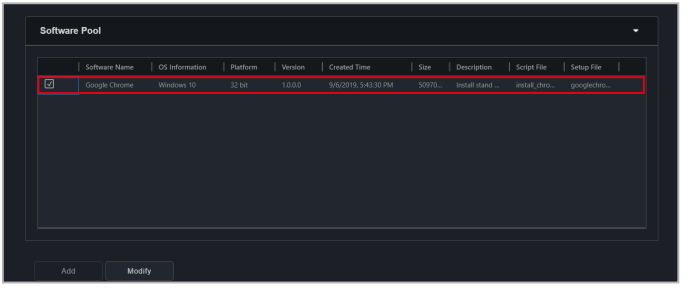


3. Select the **Setup File** and **Script File** you would like to upload. Click on **Save** once you have finished.

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

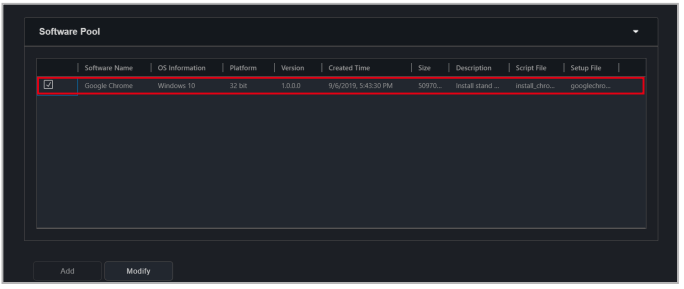


4. The added software package should appear in the Software Pool list.

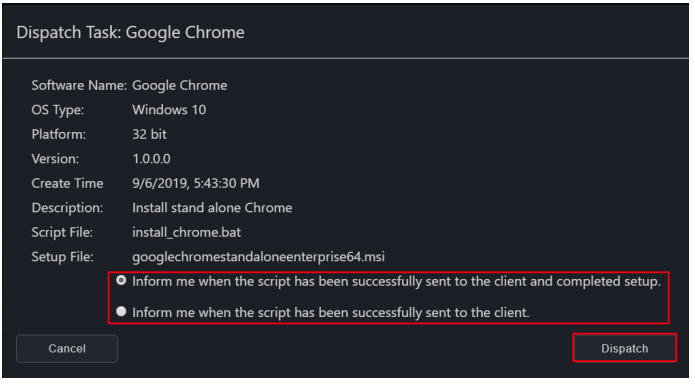


Dispatching software using the Software Pool

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

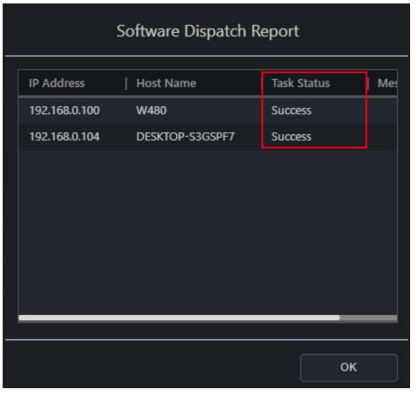


2. Select the notification scenario, then click on **Dispatch**. Once the software dispatch process is completed you should receive a notification based on the notification scenario selected.

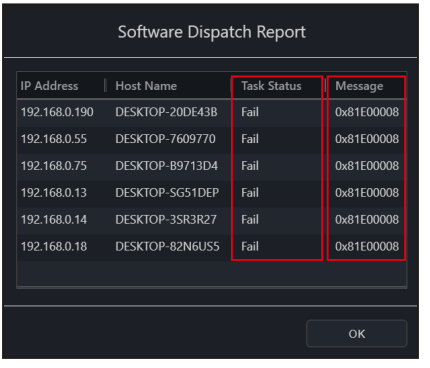


The software dispatch process will not display any software installation user interface or notices. Ensure the software you dispatch supports silent mode - an installation that requires no user interaction, and has a script file to execute the installation process in order for the software to automatically install in the background.

3. The dispatch progress and results can be viewed in the Mission Center. If the dispatch was successful, **Success** will be displayed in the **Task Status** column.



If the dispatch was unsuccessful, **Fail** will be displayed in the **Task Status** column, and a dispatch message code will be displayed in the Message column. Please refer to the table below for the dispatch message codes.

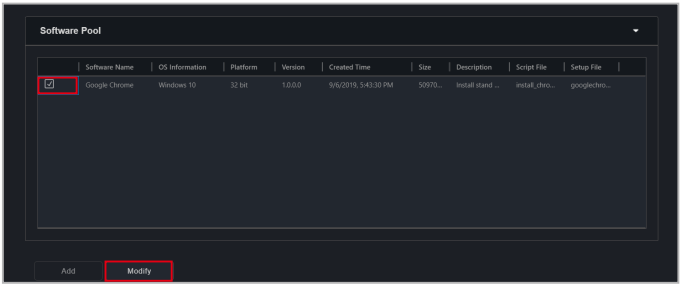


Message code	Details
0x81E00000	Unable to retrieve data returned by the server.
0x81E00004	Unable to parse data returned by the server.
0x81E00007	Unable to obtain data returned by the client device.
0x81E00008	Please check the connection status of the client device.

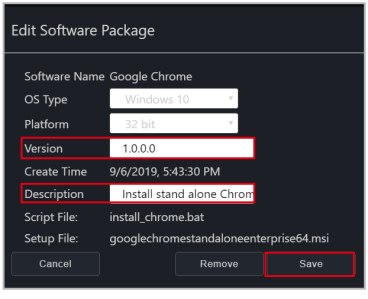
- Please refer to the MsiExec.exe and InstMsi.exe error message descriptions if the software dispatch results and message codes were returned by the Windows Installer response file script.
- Software installation may be affected by the OS anti-virus. If you are certain there are no problems with the software package and script file but the installation is still unsuccessful, you can try temporarily disabling the anti-virus on the client device during the dispatch and installation process.

Modifying a software package

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

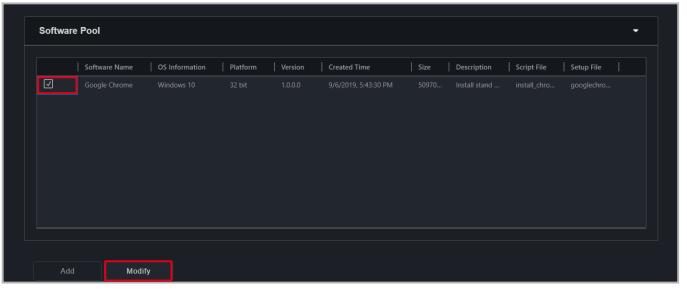


2. You can edit the **Version** and **Description**, once you have finished, click on **Save** to save the changes made.

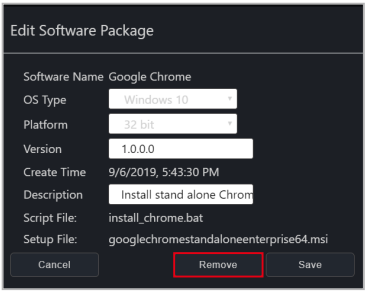


Deleting a software package

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.

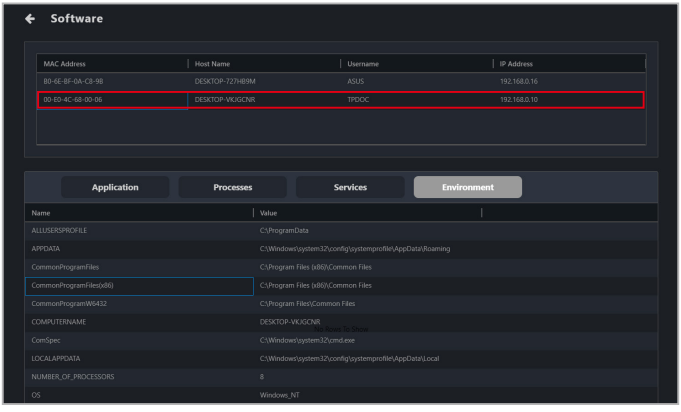


5.2.3 Software Information

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.
- Click on the (Refresh) button to immediately refresh and update the software list.

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.

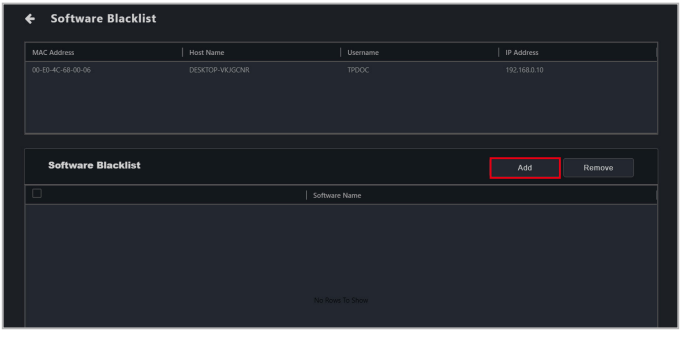
5.2.4 Software Blacklist

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**.

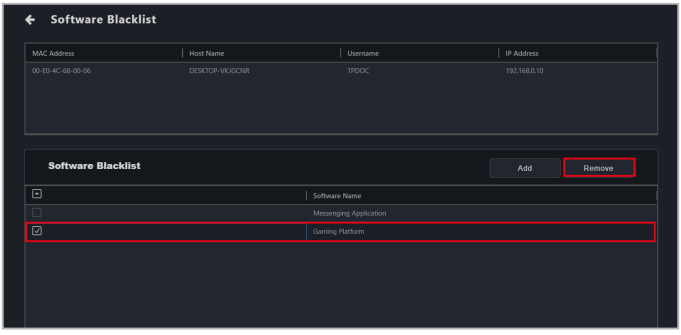


2. Enter the name of the software you wish to blacklist, then click on **Save**.

Ensure to enter the full name of the software you wish to blacklist, for example cmd.exe. You can view the full name of the software from the **Software Information** page in ASUS Control Center Express, or through the Windows command line/Task Manager. For more information on Software Information, please refer to **5.2.3 Software Information**.

Removing a software from the Software Blacklist

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



5.2.5 Installer

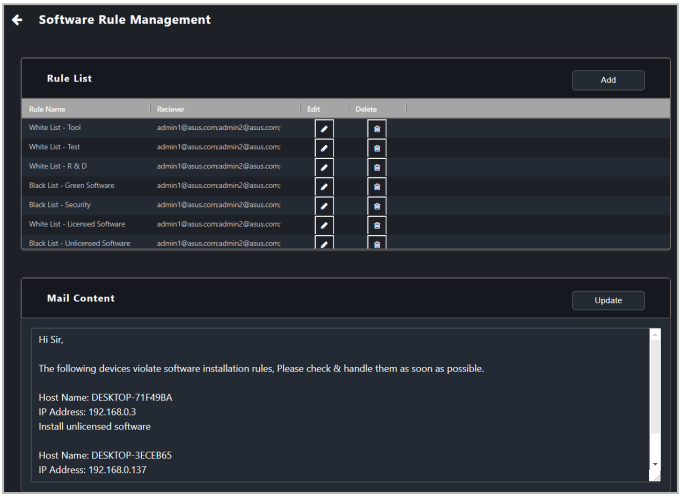
This item will allow you to download and update the driver, utility application, and BIOS for a single or multiple devices. For more information on the Installer, please refer to **4.11 Installer**.

5.2.6 Software Rule Management

The Software Rule Management allows you to manage software applications the user may install on the client device through setting software rules. You may apply whitelist and blacklist rules to software and when the user installs a software that violates the whitelist rule or complies to the blacklist rule, an email notification will be sent to user-defined receivers notifying them of this software installation.

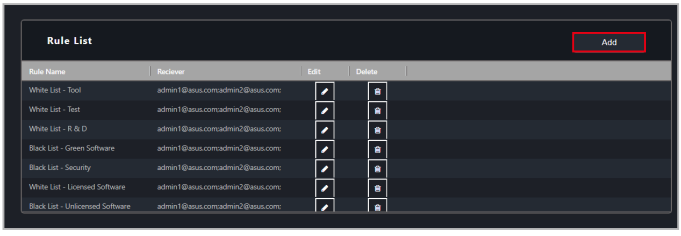
To access the **Software Rule Management**, select the client device(s) and click on **Select Function** > **Software Management** > **Software Rule Management**.

- Ensure the SMTP settings are set and can receive the test email before using the Software Rule Management function. For more information please refer to **8.1.1 SMTP Settings**.
- A notification email will be sent for each violated/met condition which would send a notification email, for example, if a software was installed on the client device, and it met a blacklist condition and violated a whitelist condition at the same time, two notification emails would be sent.
- If a software that does not comply to the software rules was installed on a client device that is offline, the system will check for violations and send notification emails once the device is online.

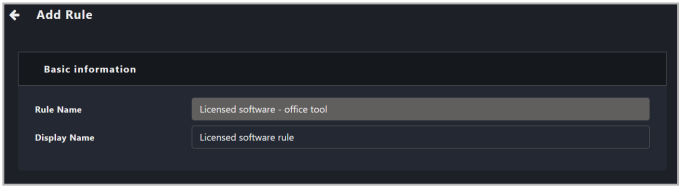


Adding a new rule to the Rule List

1. Click on **Add**.



2. Enter the required information into the Basic Information block.

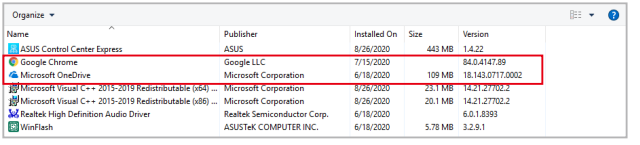


Rule Name	Enter the rule name.
Display Name	Enter the email title of the notification email for this rule.

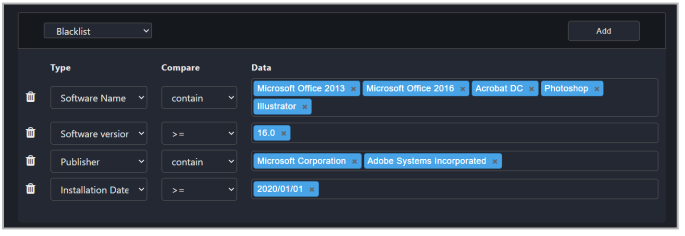
3. Select whether to add a **Blacklist** or **Whitelist** condition, then select the **Type** and **Condition** and enter keywords for the rule into the **Data** field. Click **Add** to add the blacklist or whitelist condition.

- If a blacklist condition and a whitelist condition contradict with each other, the system will prioritize the blacklist condition.
- If multiple keywords are entered for a single blacklist/whitelist condition, if any one of the keywords meet the condition or violate the condition set, the blacklist/whitelist condition will be valid.
- If multiple blacklist/whitelist conditions are set within a single rule, all conditions have to be valid for the rule to take effect.

- When entering multiple keywords, press <Enter> after each keyword to separate the keywords.
- The information displayed for may differ between softwares, we recommend referring to the software information displayed in **Control Panel** > **Programs** > **Programs and Features**.



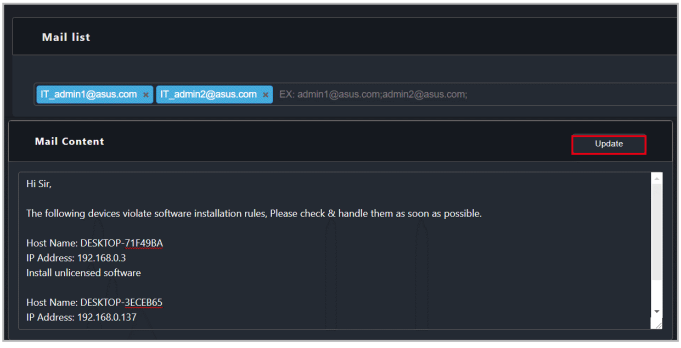
- For a full list of the whitelist and blacklist conditions, please refer to the **Whitelist conditions** and **Blacklist conditions** section.



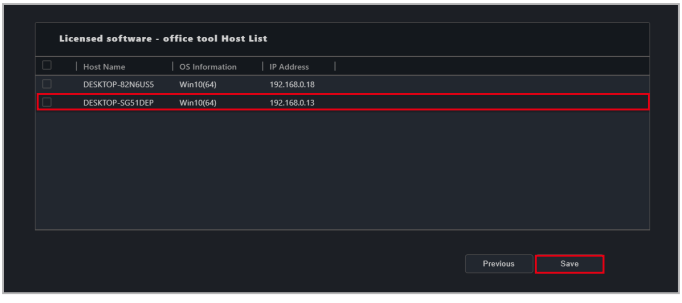
Blacklist / Whitelist	Set the rule as a Blacklist or Whitelist condition.
Type	Select the type of data (**Software Name**, **Software Version**, **Publisher**, **Installation Date**) you would like to enter into the **Data** field as blacklist or whitelist keywords.
Compare	Select the comparison condition, the options available may vary according to the **Type** selected.
Data	Enter keywords which correspond to the **Type** selected as the keywords to compare.

4. Repeat step 3 to add more blacklist or whitelist conditions.
5. Enter the email addresses the notifications should be sent to, then enter the email content for the notification email and click **Update** once you are finished with the email content.

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



6. Click on **Next** once you are finished.
7. Select the client devices you want to apply this software rule to, then click **Save** to finish adding the software rule.



Whitelist conditions

Type	Compare	Data
Software Name	Contains	If a software installed on the client device matches a software name entered, no notification email will be sent.
		If a software installed on the client device does not match a software name entered, a notification email will be sent.
	Does not contain	If a software installed on the client device does not match a software name entered, no notification email will be sent.
		If a software installed on the client device matches a software name entered, a notification email will be sent.
Version	>	If a software installed on the client device is a higher version than a version entered, no notification email will be sent.
		If a software installed on the client device is a lower version than a version entered, a notification email will be sent.
	<	If a software installed on the client device is a lower version than a version entered, no notification email will be sent.
		If a software installed on the client device is a higher version than a version entered, a notification email will be sent.
	=	If a software installed on the client device is the same version as a version entered, no notification email will be sent.
		If a software installed on the client device is not the same version as a version entered, a notification email will be sent.
	!=	If a software installed on the client device is not the same version as a version entered, no notification email will be sent.
		If a software installed on the client device is the same version as a version entered, a notification email will be sent.
	>=	If a software installed on the client device is a higher version or equal to a version entered, no notification email will be sent.
		If a software installed on the client device is a lower version than a version entered, a notification email will be sent.

(continued on the next page)

Version	**<=**	If a software installed on the client device is a lower version or equal to a version entered, no notification email will be sent.
		If a software installed on the client device is a higher version than a version entered, a notification email will be sent.
Developer	**Contains**	If a software installed on the client device matches a developer entered, no notification email will be sent.
		If a software installed on the client device does not match a developer entered, a notification email will be sent.
	Does not contain	If a software installed on the client device does not match a developer entered, no notification email will be sent.
		If a software installed on the client device matches a developer entered, a notification email will be sent.
Installation Date	**>**	If a software's installation date on the client device is later than a date entered, no notification email will be sent.
		If a software's installation date on the client device is earlier than a date entered, a notification email will be sent.
	<	If a software's installation date on the client device is earlier than a date entered, no notification email will be sent.
		If a software's installation date on the client device is later than a date entered, a notification email will be sent.
	=	If a software's installation date on the client device is equal to a date entered, no notification email will be sent.
		If a software's installation date on the client device is not equal to a date entered, a notification email will be sent.
	!=	If a software's installation date on the client device is not equal to a date entered, no notification email will be sent.
		If a software's installation date on the client device is equal to a date entered, a notification email will be sent.

(continued on the next page)

Installation Date	>=	If a software's installation date on the client device is later or equal to a date entered, no notification email will be sent.
		If a software's installation date on the client device is earlier than a date entered, a notification email will be sent.
	<=	If a software's installation date on the client device is earlier or equal to a date entered, no notification email will be sent.
		If a software's installation date on the client device is later than a date entered, a notification email will be sent.

Blacklist conditions

Type	Compare	Data
Software Name	Contains	If a software installed on the client device matches a software name entered, a notification email will be sent.
		If a software installed on the client device does not match a software name entered, no notification email will be sent.
	Does not contain	If a software installed on the client device does not match a software name entered, a notification email will be sent.
		If a software installed on the client device matches a software name entered, no notification email will be sent.
Version	>	If a software installed on the client device is a higher version than a version entered, a notification email will be sent.
		If a software installed on the client device is a lower version than a version entered, no notification email will be sent.
	<	If a software installed on the client device is a lower version than a version entered, a notification email will be sent.
		If a software installed on the client device is a higher version than a version entered, no notification email will be sent.
	=	If a software installed on the client device is the same version as a version entered, a notification email will be sent.
		If a software installed on the client device is not the same version as a version entered, no notification email will be sent.

(continued on the next page)

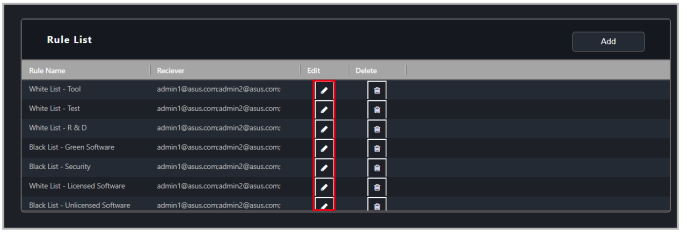
Version	**!=**	If a software installed on the client device is not the same version as a version entered, a notification email will be sent.
		If a software installed on the client device is the same version as a version entered, no notification email will be sent.
	>=	If a software installed on the client device is a higher version or equal to a version entered, a notification email will be sent.
		If a software installed on the client device is a lower version than a version entered, no notification email will be sent.
	<=	If a software installed on the client device is a lower version or equal to a version entered, a notification email will be sent.
		If a software installed on the client device is a higher version than a version entered, no notification email will be sent.
Developer	**Contains**	If a software installed on the client device matches a developer entered, a notification email will be sent.
		If a software installed on the client device does not match a developer entered, no notification email will be sent.
	Does not contain	If a software installed on the client device does not match a developer entered, a notification email will be sent.
		If a software installed on the client device matches a developer entered, no notification email will be sent.
Installation Date	**>**	If a software's installation date on the client device is later than a date entered, a notification email will be sent.
		If a software's installation date on the client device is earlier than a date entered, no notification email will be sent.
	<	If a software's installation date on the client device is earlier than a date entered, a notification email will be sent.
		If a software's installation date on the client device is later than a date entered, no notification email will be sent.

(continued on the next page)

Installation Date	=	If a software's installation date on the client device is equal to a date entered, a notification email will be sent.
		If a software's installation date on the client device is not equal to a date entered, no notification email will be sent.
	!=	If a software's installation date on the client device is not equal to a date entered, a notification email will be sent.
		If a software's installation date on the client device is equal to a date entered, no notification email will be sent.
	>=	If a software's installation date on the client device is later or equal to a date entered, a notification email will be sent.
		If a software's installation date on the client device is earlier than a date entered, no notification email will be sent.
	<=	If a software's installation date on the client device is earlier or equal to a date entered, a notification email will be sent.
		If a software's installation date on the client device is later than a date entered, no notification email will be sent.

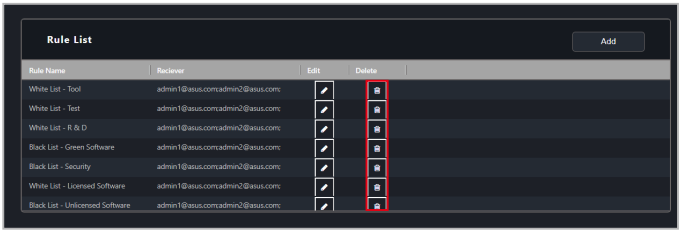
Modifying a software rule

1. Click on next to the rule you wish to modify.
2. Click on **Next** once you are finished modifying the rule.
3. Select the client devices you want to apply this software rule to, then click **Save** to finish modifying the software rule.

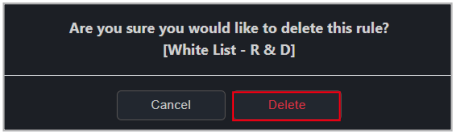


Deleting a software rule

1. Click on next to the rule you wish to delete.



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

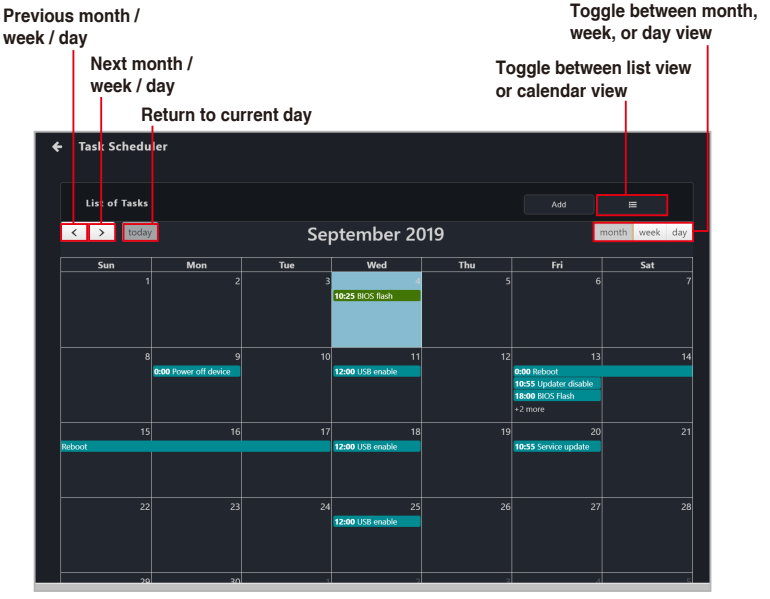


5.3 Task Scheduler

You can set scheduled tasks for client devices to execute on set dates, or set them to repeat periodically. To begin setting tasks, please select the device(s) you would like to schedule tasks for from the Devices list, then select the **Task Scheduler** function from the Select function drop down list of functions.

5.3.1 Task scheduler calendar overview

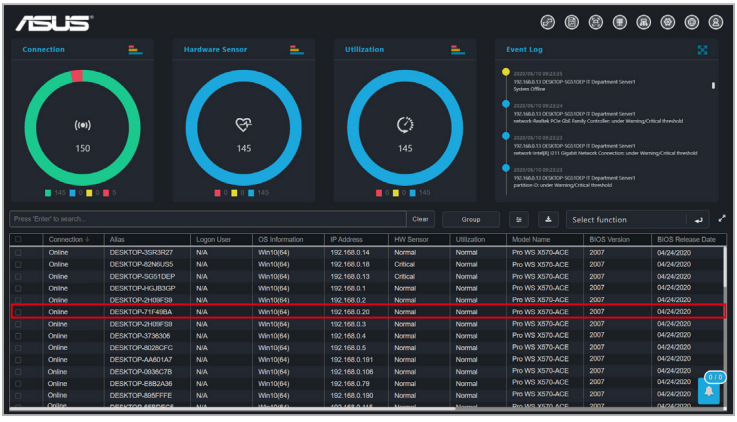
You can view the tasks already set on the task scheduler calendar.



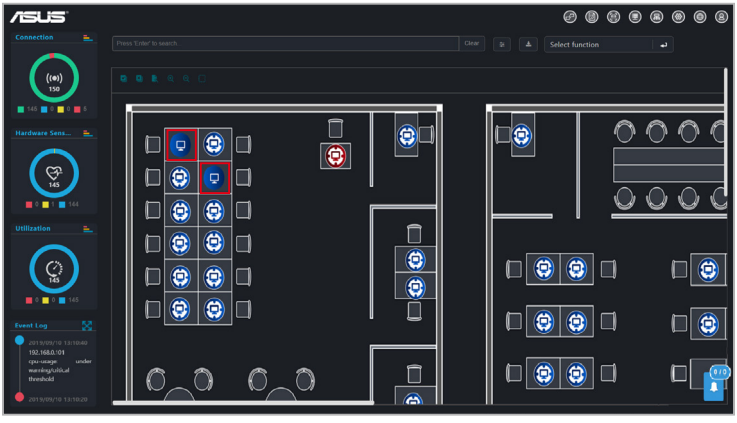
5.3.2 Setting a new task

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

Classic dashboard

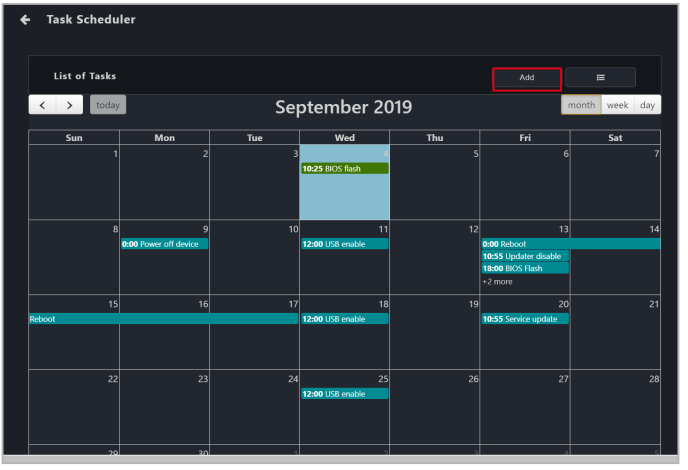


Graphic dashboard



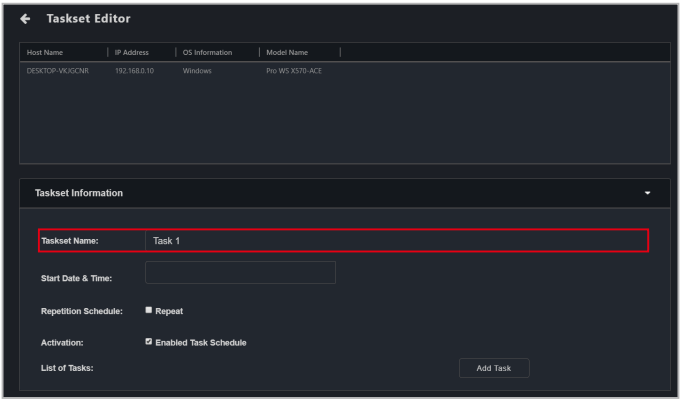
2. Click on **Select function**, then select **Task Scheduler** from the drop down menu.

3. Click on **Add.**



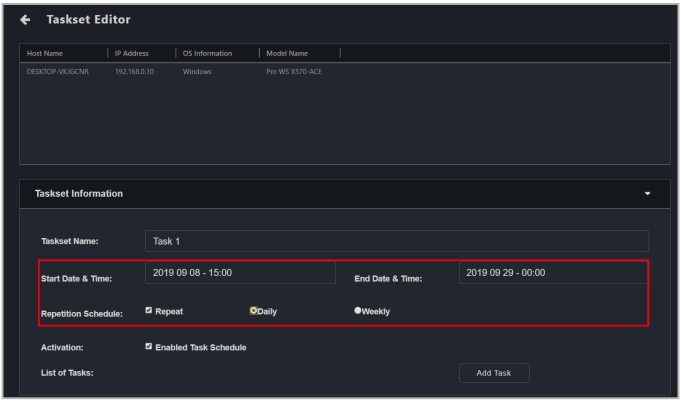
4. Enter the Taskset name**.**

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

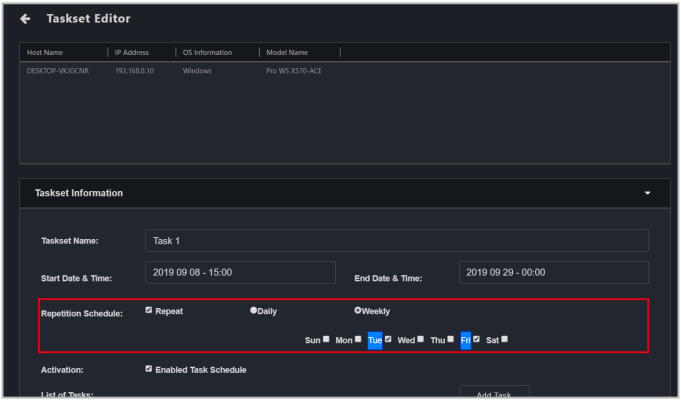


5. Select a **Start Date & Time**. If you want the task to repeat for a set period of time, check **Repeat**, then select the **End Date & Time**.

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

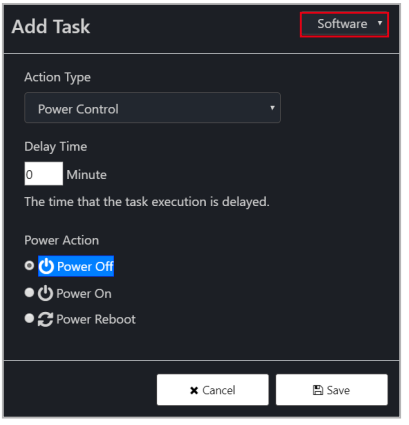


6. (optional) If you checked **Repeat** in the previous step, select if you want the task to repeat **Daily** or **Weekly**. Selecting **Weekly** will allow you to choose the day you wish to repeat the task each week.

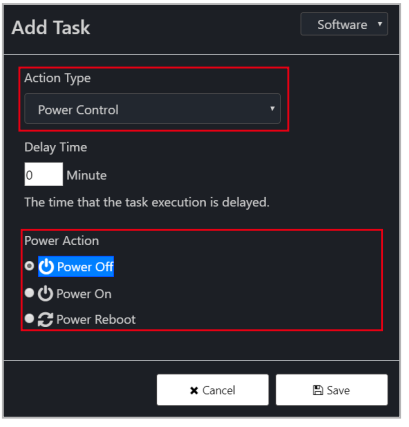


7. Click on **Add Task** and select **Software** for software based functions, **Hardware** for management functions, or **DASH** or **vPro** for power control functions.

Hardware functions are only available on client devices connected using a management LAN port which supports remote management controller.



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



Software

Action type	Action options		Description
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 and Boot	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
	Fast Startup	Enable	Enable Fast Startup
		Disable	Disable Fast Startup
	Windows Update	Enable	Enable Windows Update
		Disable	Disable Windows Update
BIOS Cache	BIOS Cache List		Select a BIOS file from the BIOS cache list

- BIOS Cache tasks may fail to complete if a BitLocker or fTPM risk is detected. It is strongly recommended to resolve these risks before proceeding. Refer to the **BIOS** section in the **Device Information** chapter for more information.
- If you understand the risks involved, check **Allow updating BIOS when BitLocker is unsuspended or unknown**, **Allow updating BIOS when BitLocker automatic backup of recovery key failed**, and **Allow erasing fTPM security data when updating BIOS** when creating a BIOS Cache task to ignore these risks and proceed anyway.

Hardware

Action type	Action options	Description
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

*** These Action Categories are only supported on motherboards which support remote management controllers.**

DASH

Action type	Action options	Description
Power Control	Power On (G0/S0)	Power on device
	Power Off - Soft (G2/S5)	Power off device
	Power Off - Hard (G3)	Force device to power off .
	Power Cycle - Soft off (G2/S5)	Restart device after shutting down the OS
	Sleep - Deep (G1/S3)	Enter sleep mode (G1/S3)
	Master Bus Reset	Reset the hardware
	Hibernate (G1/S4)	Enter hibernate mode (G1/S4)
	Restart Computer to BIOS	Enter BIOS after restarting device
	Power On to BIOS	Enter BIOS after powering on device
	Restart Computer to IDE-R Floppy	Enter IDE-R floppy drive after restarting device
	Power On to IDE-R Floppy	Enter IDE-R floppy drive after powering on device
	Restart Computer to IDE-R CDROM	Enter IDE-R ODD after restarting device
	Power On to IDE-R CDROM	Enter IDE-R ODD after powering on device
	Sleep - Light (G1/S2)	Enter sleep mode (G1/S2)
	Power Cycle - Hard Off (G3)	Restart device after forcing device to power off.
	Diagnostic Interrupt (NMI)	Print error report and restarting device
	Power Off - Soft Graceful (G2/S5)	Normal shut down via the OS
	Power Off - Hard Graceful (G3)	Normal shut down via the hardware
	Master Bus Reset Graceful	Normal shut down and resetting the hardware
	Power Cycle (Graceful Soft Off) (G2/S5)	Normal shut down via the OS then restarting the device
	Power Cycle (Graceful Hard Off) (G3)	Normal shut down via the hardware then restarting the device

* **These Action Categories are only supported on motherboards which support remote management controllers.**

vPro

Action type	Action options	Description
Power Control	Power On (G0/S0)	Power on device
	Power Cycle - Soft off (G2/S5)	Restart device after shutting down the OS
	Master Bus Reset	Reset the hardware
	Sleep - Deep (G1/S3)	Enter sleep mode (G1/S3)
	Hibernate (G1/S4)	Enter hibernate mode (G1/S4)
	Power Off - Soft (G2/S5)	Power off device
	Power Off - Soft Graceful (G2/S5)	Normal shut down via the OS
	Master Bus Reset Graceful	Normal shut down and resetting the hardware
	Restart Computer to BIOS	Enter BIOS after restarting device
	Power On to BIOS	Enter BIOS after powering on device
	Restart Computer to IDE-R Floppy	Enter IDE-R floppy drive after restarting device
	Power On to IDE-R Floppy	Enter IDE-R floppy drive after powering on device
	Restart Computer to IDE-R CDROM	Enter IDE-R ODD after restarting device
	Power On to IDE-R CDROM	Enter IDE-R ODD after powering on device

* **These Action Categories are only supported on motherboards which support remote management controllers.**

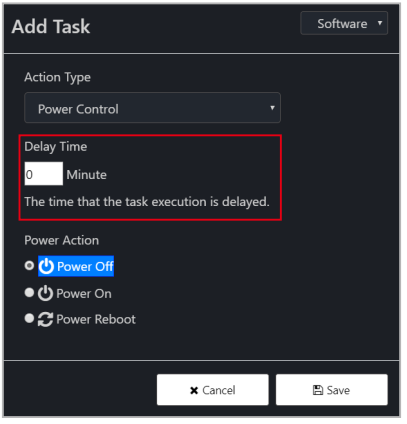
BMC

Action type	Action options	Description
Power Control	Power On (G0/S0)	Power on device
	Power Off - Soft (G2/S5)	Power off device
	Power Off - Hard (G2/S5)	Force device to power off
	Power Cycle - Soft Graceful (G2/S5)	Restart device after shutting down the OS.
	Power Cycle - Hard Off (G3)	Restart device after forcing device to power off.

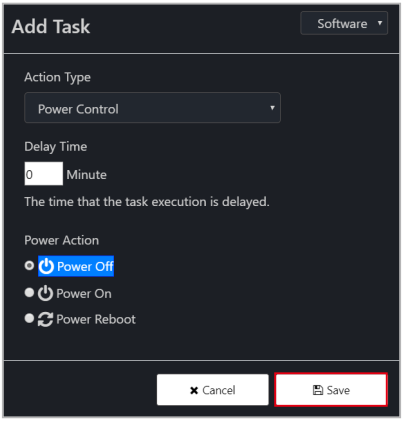
* **These Action Categories are only supported on motherboards which support remote management controllers.**

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.



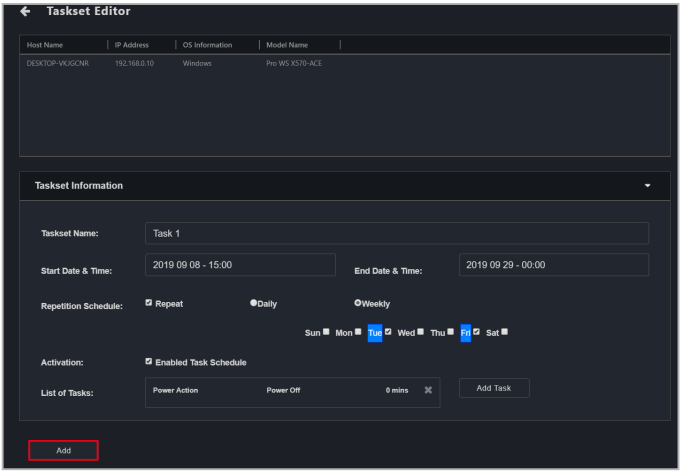
10. Click on **Save** to save this task



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**.

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

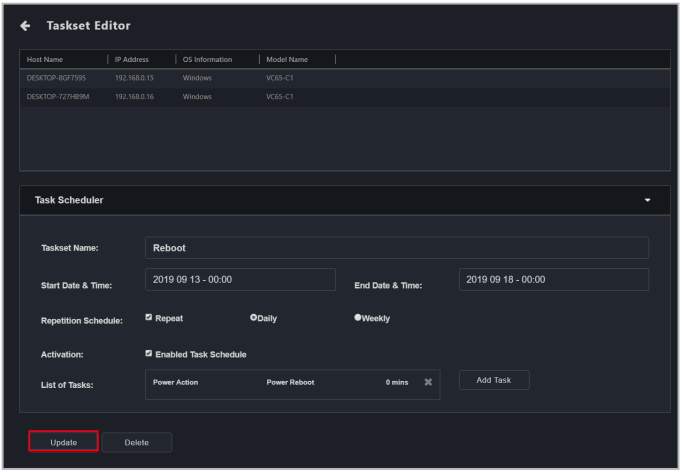


5.3.3 Editing a task

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

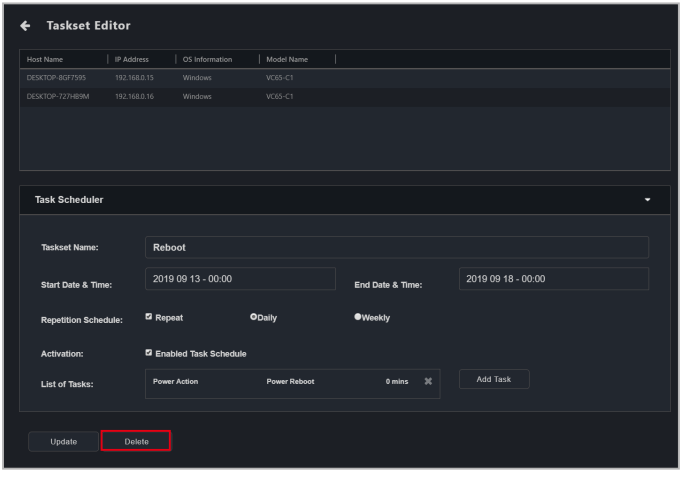
To delete a task, click on the **X** next to the task in the **List of Tasks**.

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



5.3.4 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.



5.4 OOB Control

The OOB (Out of band) Control function ASUS Control Center Express provides allows one-to-many management of devices and also supports control of client device(s) with BMC, DASH, RTL8117, or vPro remote management controllers.

- To use the OOB Control functions, ensure the client device's motherboard supports BMC, DASH, RTL8117, or vPro remote management controller.
- Before using the OOB function on the client device, ensure that the remote management controller settings have been set in the client device's BIOS.

5.4.1 Setting remote management controller credentials

Before using the client device's OOB functions, please set up the login account and password ASUS Control Center Express will use to log into the client device's remote management controller. This will ensure the OOB remote functions are secure.

Please refer to the following methods for setting up the login information ASUS Control Center Express will use to log into the client device's remote management controller:

Setting the account and password in Settings (BMC, DASH, and vPro)

1. Click on , then navigate to **Options** > **General Configuration**, and scroll down to **vPro Account**, **DASH Account** and **BMC Account**.
   - To set up a vPro controller, enter the account and password for the client device's remote management controller under **vPro Account**, then click **Save**.

MEBx is an Intel BIOS extension option and setting for Intel client devices. The account and password set for MEBx is not the Intel vPro remote management controller account and password.

- The password for **vPro Account** must be at least 8 characters long, and must contain one uppercase letter (A-Z), number (0-9), and one special character.
- The account and password entered should match the account and password already set on the client device.

- To set up a DASH controller, enter the account and password for the client device's remote management controller under **DASH Account**. You may choose to enter the port used for DASH, or enable/disable the TLS (Transport Layer Security). Click **Save** when you are finished.

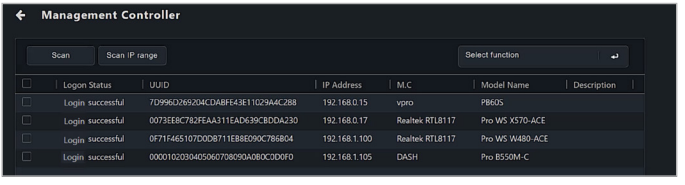
- The account and password for **DASH Account** is limited to 15 characters.
- The account and password entered should match the account and password already set on the client device.

- To set up a BMC controller, enter the account and password for the client device's remote management controller under **BMC Account**. You may choose to enter the port used for BMC. Click **Save** when you are finished.

- The account for **BMC Account** must start with a letter (A-z), must contain at least one number (0-9), and is limited to 16 characters. The password must be at least 8 characters long.
- The account and password entered should match the account and password already set on the client device.

2. After setting up the BMC Account, **vPro Account**, and/or **DASH Account** information, ASUS Control Center Express will automatically log into the client device's remote management controller. You can perform a scan in the Management Controller page to check the remote management controller login status for the client device(s).

If the default login account and password matches the client device's remote management controller match, the login status will be displayed as **Login successful** on the Management Controller page after executing a scan.



The default account and password entered can be used to log into multiple client devices which have the same remote management controller account and password.

Setting the account and password through Management Controller

You can set the remote management controller log in account for ASUS Control Center Express for multiple client devices through the Management Controller page.

If a client device(s) with a remote management controller already has an agent deployed to it, you can also select the client device(s) from the devices list on the main menu page, then: click on **Select Function** > **OOB - Control** > **Account Management** > **Set password** for RTL8117 and vPro, or click on **Select Function** > **OOB - Control** > **Account Management** > **Login** for BMC and DASH.

1. Click on then perform a **Scan** or **Scan IP Range**.
2. After the scan is completed, you can check if ASUS Control Center Express has successfully logged into the client device's remote management controller. If the account and password entered in ASUS Control Center Express does not match the client device's remote management controller account and password, **Login failed** will be displayed in the **Login Status** column.

3. Select the client devices for which you would like to set the account and password ASUS Control Center Express will use to log into the client device's remote management controller.

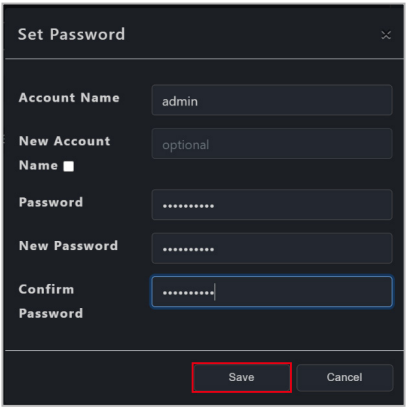
When selecting multiple client devices to set the account and password, ensure that the selected client devices have the same remote management controller.

4. Depending on the remote management controller type, the steps for setting the account and password may differ slightly.

   For RTL8117 and vPro

   a. Click on **Select Function** > **Account Management** > **Set password**.

   b. Enter the account and password ASUS Control Center will use to log into the client device's remote management controller, then click **Save**.



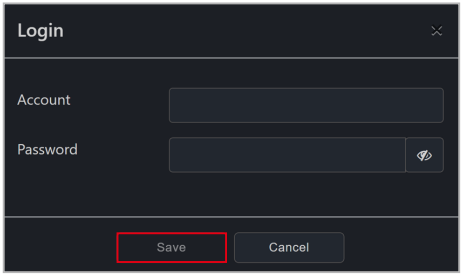
MEBx is an Intel BIOS extension option and setting for Intel client devices. The account and password set for MEBx is not the Intel vPro remote management controller account and password.

- The password for vPro Account must be at least 8 characters long, and must contain one uppercase character (A-Z), numbers (0-9), and one special character.
- The password for RTL8117 must be at least 8 characters long, and must contain uppercase characters (A-Z), lower case characters (a-z), and numbers (0-9).

For BMC and DASH

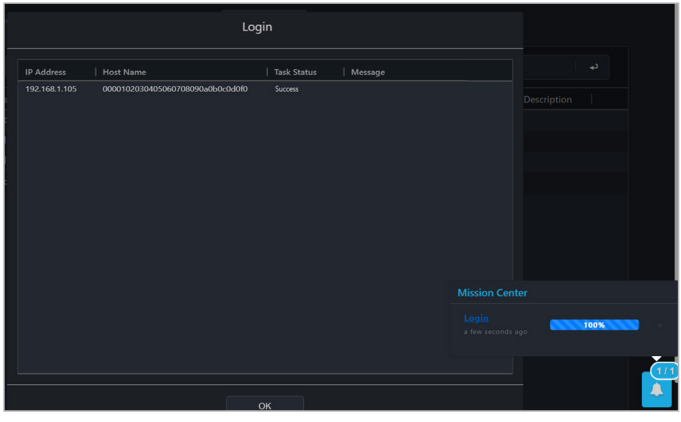
a. Click on **Select Function** > **Account Management** > **Login**.

b. Enter the account and password ASUS Control Center will use to log into the client device's remote management controller, then click **Save**.

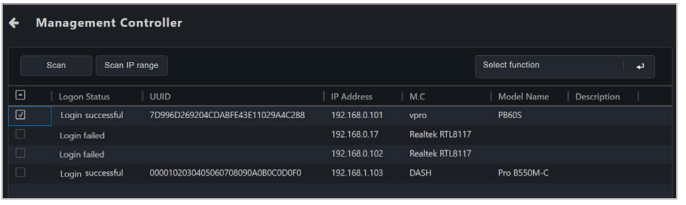


- You can also set the account and password for a single device with DASH remote management controller through **Account Management** on the **Device Management Information** page. For more information on Account Management please refer to **5.7.7 Account Management**.
- If the client device selected has multiple BMC or DASH remote management controller accounts you can switch accounts through **OOB - Control** > **Account Management** > **Login**.

5. You can view the status and results of setting the account and password in the Mission Center.



6. After the account and password has been set, ASUS Control Center Express will log into the client device's remote management controller. If the login is successful, **Login successful** will be displayed in the **Login Status** column and the client device's remote management controller and device name will also be displayed.



7. For client devices with BMC or DASH remote management controllers, you can also check which account has been logged in on the **Device Management Information** page.

Setting the account and password through Management Control Information of a single device

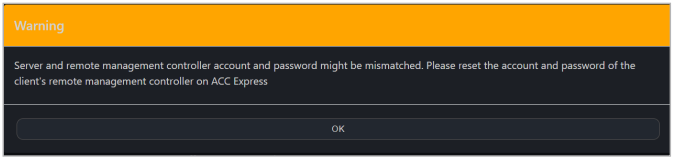
You can set the remote management controller log in account for ASUS Control Center Express for a single client device through the Management Control Information page.

If a client device(s) with a remote management controller already has an agent deployed to it, you can also select the client device(s) from the devices list on the main menu page, then click on **Select Function** > **OOB - Control** > **Account Management** > **Set password** for RTL8117 and vPro, or click on **Select Function** > **OOB - Control** > **Account Management** > **Login** for BMC and DASH.

1. To enter the Management Control Information page you can either
   - On the main menu page, click on in the M.C. column of the device you would like to enter the **Management Control Information** of.

     To use this method, the client device should already have an agent deployed to it.

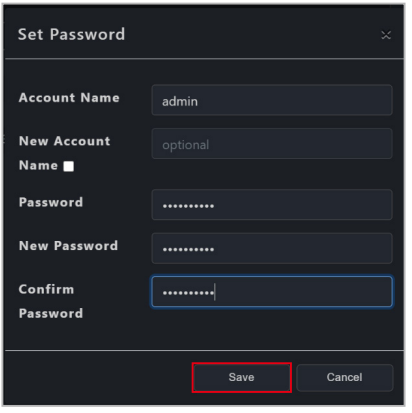
   - Click on then perform a **Scan** or **Scan IP Range**, then click on in the M.C column of the device you would like to enter the Management Control Information of.
   - Enter the **Device Information** page of a device, then toggle the **Mode** to **Hardware**.
2. If the login account and password ASUS Control Center Express is using to log into the client device's remote management controller do not match, a pop-up message should show up:



3. Depending on the remote management controller type, the pop up window for setting the account and password may differ slightly.

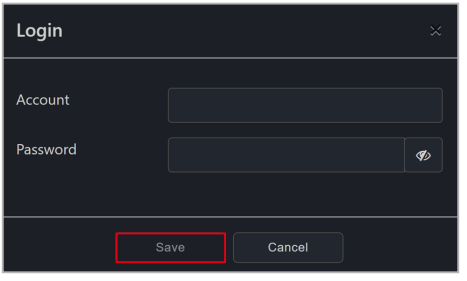
For RTL8117 and vPro

Enter the account and password ASUS Control Center will use to log into the client device's remote management controller, then click **Save**.



For BMC and DASH

Enter the account and password ASUS Control Center will use to log into the client device's remote management controller, then click **Save**.



4. You can view the status and results of setting the account and password in the Mission Center. If the account and password setting was successful and the account and password match, ASUS Control Center should automatically log into the client device's remote management controller, and also allow you to begin using the **OOB - Control** functions.

- You can also set the account and password for a single device with DASH remote management controller through **Account Management** on the **DASH Device Management Information** page. For more information on Account Management please refer to **5.7.7 Account Management**.
- MEBx is an Intel® BIOS extension option and setting for Intel® client devices. The account and password set for MEBx is not the Intel® vPro remote management controller account and password.

- The password for vPro Account must be at least 8 characters long, and must contain one uppercase character (A-Z), numbers (0-9), and one special character.
- The password for RTL8117 must be at least 8 characters long, and must contain uppercase characters (A-Z), lower case characters (a-z), and numbers (0-9).

5.4.2 Using OOB - Control functions

To use the OOB - Control functions you can either:

- Select the client device(s) you would like to execute OOB - Control functions on, then click on **Select Function** > **OOB - Control** and select a function to use.
- Click on then perform a **Scan** or **Scan IP Range**, select the client device(s) you would like to execute OOB - Control functions on, then click on **Select Function** and select a function to use.

Please see the table below for the list of the OOB - Control functions available for the different remote management controllers:

Functions List		BMC	DASH	RTL 8117	vPro
Power Control	Power On (G0/S0)	V	V	V	V
	Power Off - Soft (G2/S5)	V	V	V	V
	Power Off - Hard (G3)	V	V	V	
	Power Cycle - Soft off (G2/S5)	V	V	V	V
	Sleep - Deep (G1/S3)		V		V
	Master Bus Reset		V		V
	Hibernate (G1/S4)		V		V
	Restart Computer to BIOS				V
	Power On to BIOS				V
	Restart Computer to IDE-R Floppy				V
	Power On to IDE-R Floppy				V
	Restart Computer to IDE-R CDROM				V
	Power On to IDE-R CDROM				V
	Sleep - Light (G1/S2)		V		
	Power Cycle - Hard Off (G3)	V	V		
	Diagnostic Interrupt (NMI)		V		
	Power Off - Soft Graceful (G2/S5)		V		
	Power Off - Hard Graceful (G3)		V		
	Master Bus Reset Graceful		V		
	Power Cycle (Graceful Soft Off) (G2/S5)		V		
	Power Cycle (Graceful Hard Off) (G3)		V		
WatchDog	WatchDog Enable			V	
	WatchDog Disable			V	
BIOS	Smart BIOS - BIOS update management	V		V	
	Smart BIOS - User profile	V			
	Clear CMOS	V		V	
Account Management	Set Password			V	V
	Login	V	V		

(continued on the next page)

Functions List		BMC	DASH	RTL 8117	vPro
System	Restart service			V	
	Sync OEM port	V			
KVM	KVM Remote Multi-display			V	
	KVM Local Multi-display			V	
	KVM Remote Single-display			V	
	KVM Enable				V
	KVM Disable			V	V
	KVM Password				V
USB Redirection	USB Redirection		V	V	V
	Enable USB Redirection				V
	Disable USB Redirection				V
Firmware Update		V		V	
Trust Zone				V	
Certificate Management					V
System Trap Alert	Enable Trap Alert		V		V
	Enable Trap Alert - Info		V		V
	Enable Trap Alert - Warning		V		V
	Enable Trap Alert - Error		V		V
	Disable Trap Alert		V		V
IPMI	IPMI Tool Lanplus Command Redirect	V			
	FRU Info. Write	V			
Settings		V			
Configuration		V			
OOB - Control Help		V	V	V	V

Function descriptions

Power Control	Execute power actions on the selected device(s) through the remote management controller.
WatchDog	Enable or disable WatchDog of selected RTL8117 device(s).
BIOS	Use the Smart BIOS function, clear CMOS through BMC, or manage BIOS user profile data for supported device(s).
Account Management	Set the login account and password ASUS Control Center Express will use to login into the RTL8117, vPro, BMC, or DASH remote management controller for selected device(s).
System	Set the port used for BMC; or restart the RTL8117 services of the selected device(s).
KVM	Set the RTL8117 KVM display mode; vPro KVM enable, disable, or password setting for selected device(s).

(continued on the next page)

Function descriptions

USB Redirection	Use the USB redirection function of the selected RTL8117, DASH, or vPro device(s); or enable or disable the USB redirection function for selected RTL8117 and vPro device(s).
Firmware Update	Update the BMC or RTL8117 firmware for selected device(s).
Trust Zone	Set the main server IP addresses which are allowed to perform RTL8117 function operations on client devices.
Certificate Management	Manage the certificates for selected vPro device(s).
System Trap Alert	Set the system Trap Alert level, or enable or disable Trap Alert for DASH and vPro device(s).
IPMI	Configure command redirection; or write information from the FRU(s) on selected BMC device(s).
Settings	Configure settings for selected BMC device(s).
Configuration	Backup, restore, or factory reset configuration settings for selected BMC device(s).
OOB - Control Help	View information about OOB functions supported by the selected device(s).

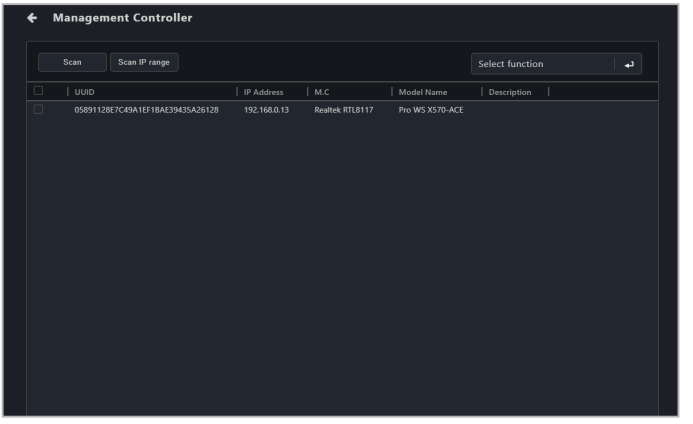
- OOB - Control functions are a collection of BMC, DASH, RTL8117, and vPro remote management controller functions. If a selected device does not support a selected OOB - Control function, you can view the details and results of the action in the Mission Center.
- Selected OOB - Control functions may not be able to be executed together due to differences between the remote management controllers, for example, USB Redirection function for vPro cannot be executed at the same time as the USB Redirection function for DASH or RTL8117.
- The USB redirection function for DASH and vPro does not support NTFS format USB devices.
- When using the USB redirection function for vPro, the client device will be displayed as Floppy Disk A, CD Drive (drive code) when successfully mounted.
- When using the KVM remote desktop function of a vPro device, the border of the client device screen will flash red and yellow to indicate that the client device is currently running the KVM remote desktop function.
- Ensure that port 162 is opened before enabling system trap alerts.
- You can add or edit remote management controller notifications in Notification Rule. The Event Log on the dashboard will display the system Trap Alert notifications you have set.

- When selecting multiple client devices to set the account and password, ensure to select client devices with the same remote management controller.
- The KVM password must contain 8 characters, and must contain uppercase characters (A-Z), lowercase characters, numbers (0-9), and special characters.
- Ensure the client device's RTL8117 is enabled if it uses RTL8117 for remote management control, and this is a new machine which is used for the first time or has been reset to factory settings. In the device's BIOS, navigate to **Advanced** > RTL8117 setting, then enable RTL8117.
- If an agent has been deployed to the client device, you can also enable the client device's RTL8117 management controller through the BIOS setting function of ASUS Control Center Express.
- You cannot update the RTL8117 remote management controller firmware if KVM is enabled. If you wish to update the RTL8117 remote management controller firmware please disable KVM first.

5.5 Management Control Overview

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

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



5.5.1 Scanning for devices

You can scan for client devices which support the Management Control functions by clicking on **Scan** or **Scan IP range**. Clicking on a device from the scan results will redirect you to the **Management Control Information** page.

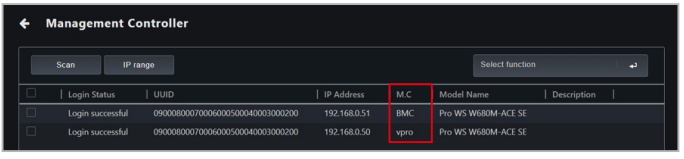
For more information on scanning an IP range, please refer to **3.2.2 Scanning an IP range**.

5.5.2 Managing devices with multiple remote management controllers

If the client device supports multiple remote management controllers, you can use ASUS Control Center Express to quickly switch between remote management controllers.

Selecting a management controller via Management Control

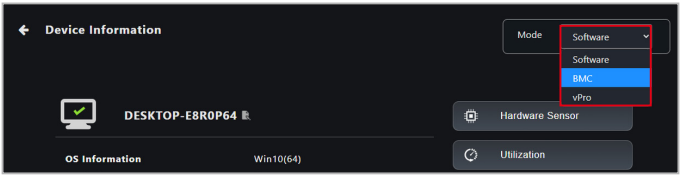
1. Click on **Management Control** in the menu bar of the main control panel, then click Scan. The detected remote management controller type will be displayed in the **M.C** column.
2. Select the entry corresponding to the desired remote management controller to open the Management Control Information page, or click **Select function** to execute an OOB - Control function.



If the Login Status field shows “Login failure”, please refer to **5.4.1 Setting remote management controller credentials** to set the account and password or log into the remote management controller of the indicated device.

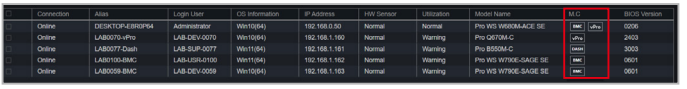
Selecting a management controller via Device Information

Select a device from the device list on the main menu to open the **Device Information** screen, then select the desired remote management controller from the **Mode** drop down menu.



Selecting a management controller via the device list

Select the icon corresponding to the desired remote management controller in the **M.C** column of the device list on the main menu, or click **Select function** to execute an OOB - Control function.

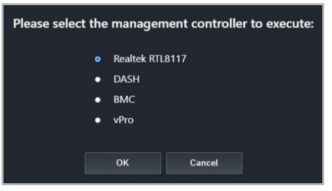


	Connection	Alias	Login User	OS Information	IP Address	HW Sensor	Utilization	Model Name	M.C	BIOS Version
	Online	DESKTOP-E8R9P64	Administrator	Win10(64)	192.168.0.50	Normal	Normal	Pro WS W680M-ACE SE	BMC vPro	0206
	Online	LAB0070-vPro	LAB-DEV-0070	Win10(64)	192.168.1.160	Normal	Warning	Pro Q670M-C	vPro	2403
	Online	LAB0077-Dash	LAB-SUP-0077	Win11(64)	192.168.1.161	Normal	Warning	Pro B550M-C	DASH	3003
	Online	LAB0105-BMC	LAB-USR-0100	Win11(64)	192.168.1.162	Normal	Warning	Pro WS W790E-SAGE SE	BMC	0601
	Online	LAB0059-BMC	LAB-DEV-0059	Win10(64)	192.168.1.163	Normal	Warning	Pro WS W790E-SAGE SE	BMC	0601

The vPro icon may not be visible if the IP address of the vPro remote management controller has been changed. To update the vPro IP address, click **Device Information > Control > Set Management Controller**, then restart the device.

Selecting a remote management controller for an offline device

Select a device from the device list on the main menu to open the **Device Information** screen, then select the desired function and management controller.



- Hardware Sensor requires a BMC, DASH, or RTL 8117 controller.
- USB Redirection requires a DASH, RTL 8117, or vPro controller.
- Power requires a vPro controller.
- Remote Desktop requires a BMC, RTL 8117, or vPro controller.

5.6 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 for devices which do not have an OS installed yet.

The Management Control Information for DASH, vPro, RTL8117, and BMC may differ from each other.

- For DASH, please refer to **5.7 DASH Management Control Information**.
- For RTL8117, please refer to **5.8 RTL8117 Management Control Information**.
- For vPro, please refer to **5.9 vPro Management Control Information**.
- For BMC, please refer to **5.10 BMC Management Control Information**.

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

- Classic view: Click on a client device in the device list, then select **Hardware** in the **Mode** dropdown menu, or click on in the M.C column of the Devices List.
- Graphic 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 scan results of the **Management Control** screen.

- Some options are only available when the client device is online and logged into the OS.
- You will not be able to toggle between **Hardware** and **Software** mode if you accessed the **Management Control Information** page through **Management Control** or by clicking on in the M.C column of the Devices List on the main menu page.
- This chapter is only for the **Hardware Mode** options, for **Software Mode** options, please refer to **Chapter 4 Device Information**.

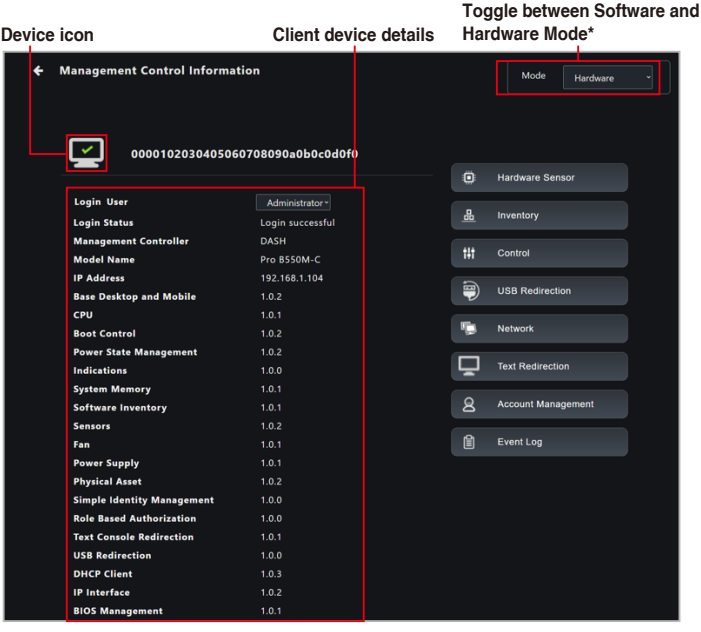
Remote Management Controller support on the motherboard is required for Management Control Information.

5.7 DASH Management Control Information

The **DASH Management Control Information** allows you to monitor the hardware status, remote power control, USB redirection, console redirection, or view the hardware assets while the client device is offline.

The functions in this section are hardware controlled and values may differ with the software version. Please refer to Chapter 4 for more information on Software mode.

The client device needs to support DASH remote management controller, and DASH function needs to be enabled in the client device's BIOS settings.



* **This item will not be available if you accessed the Management Control Information page through Management Control.**

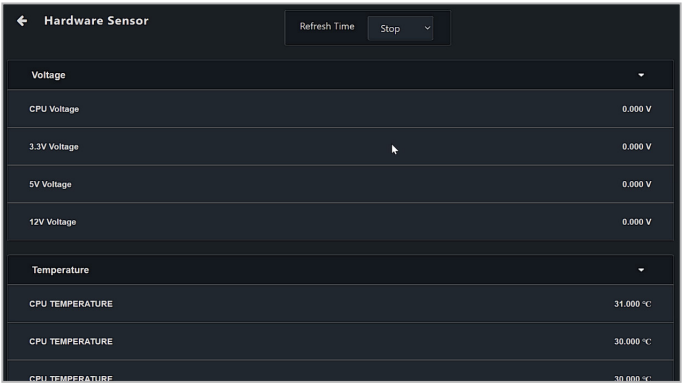
Device icon	Displays the connection status of the client device's DASH remote management controller.
Login user	Displays the user account currently logged into the client device's DASH remote management controller. The login user can be switched.
Login Status	Displays the current login status to the client device's DASH remote management controller.

(continued on the next page)

Management Controller	Displays the remote management controller of the client device.
Model Name	Displays the model name of the client device.
IP Address	Displays the IP address of client device.
Profile versions	Displays the version information for the different profiles of the client device's DASH. This information may vary depending on the support of the client device's DASH remote management controller.

5.7.1 Hardware Sensor

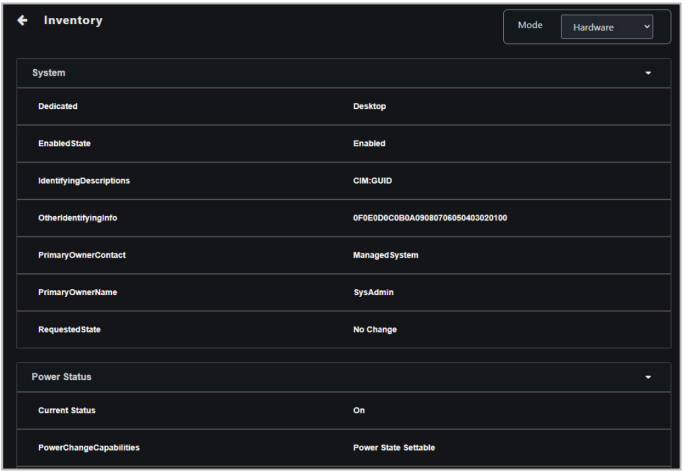
This item allows you to view the voltage, temperature, and fan rotation information of the client DASH device.



Refresh Time	Set the refresh time interval for the Hardware Sensor.
Voltage	Displays the voltage of the device hardware.
Temperature	Displays the temperature of the device hardware.
Fan	Displays the fan rotation speed of the device hardware.

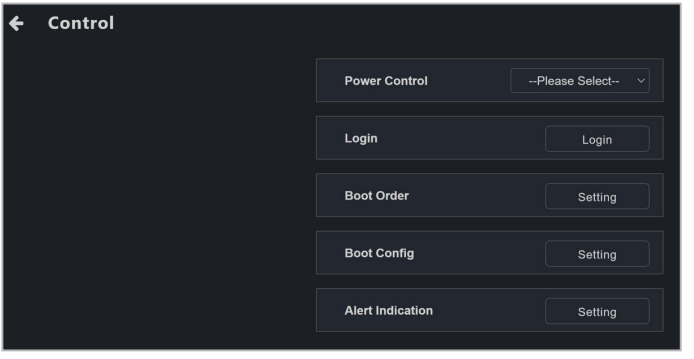
5.7.2 Inventory

This item allows you to view system product, model, CPU version, BIOS version, memory, and other hardware information.



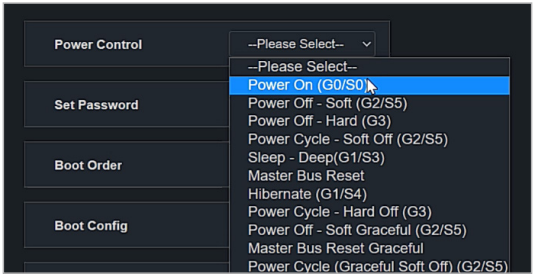
5.7.3 Control

This item allows you to set or change the client DASH device's password, and also allow you to execute power control operations.



Power Control

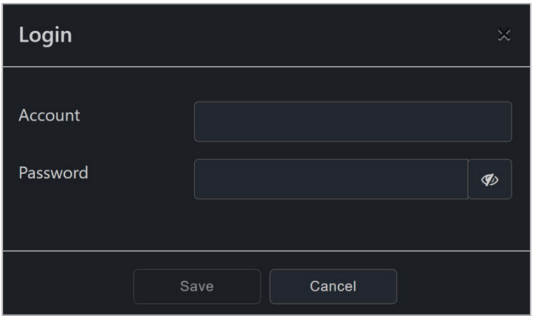
Allows you to remotely execute power control functions on the client device through the DASH remote management controller, such as a system restart.



Power On (G0/S0)	Power on the client device through the DASH remote management controller.
Power Off - Soft (G2/S5)	Power off the client device through the DASH remote management controller.
Power Off - Hard (G3)	Force the client device to power off through the DASH remote management controller when the OS is unresponsive.
Power Cycle - Soft off (G2/S5)	Restart the client device after shutting down from the OS through the DASH remote management controller.
Sleep - Deep (G1/S3)	Set the client device to enter sleep mode (G1/S3) through the DASH remote management controller.
Master Bus Reset	Resetting the hardware of the client device through the DASH remote management controller.
Hibernate (G1/S4)	Set the client device to enter hibernate mode (G1/S4) through the DASH remote management controller.
Power Cycle - Hard Off (G3)	Powering off and restarting the client device through the DASH remote management controller.
Power Off - Soft Graceful (G2/S5)	Normal shut down via the OS of the client device through the DASH remote management controller.
Master Bus Reset Graceful	Normal shut down and resetting the hardware of the client device through the DASH remote management controller.
Power Cycle (Graceful Soft Off) (G2/S5)	Normal shut down via the OS then restarting the client device through the DASH remote management controller.

Login

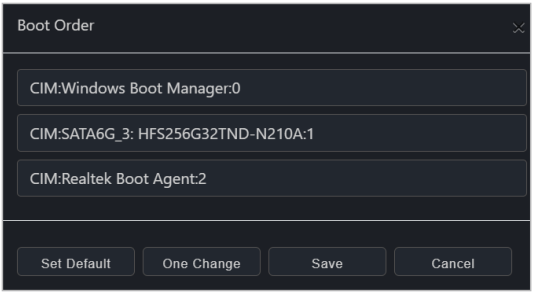
Allows you to set the account and password ASUS Control Center Express will use to log into the client device's DASH remote management controller. After successfully logging in, the DASH remote management controller will automatically switch to the newly logged in account.



Boot Order

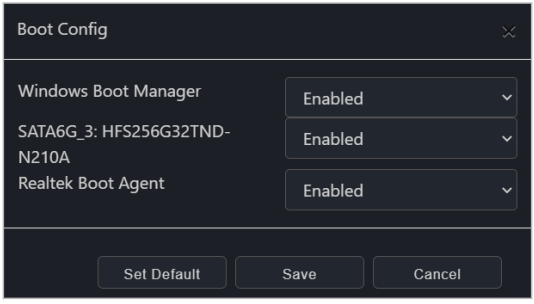
Allows you to set the client device's boot order through the DASH remote management controller.

You can readjust the ordering by left-clicking and holding the item you wish to adjust the order of, then dragging it up or down to readjust the boot order.



Boot Config

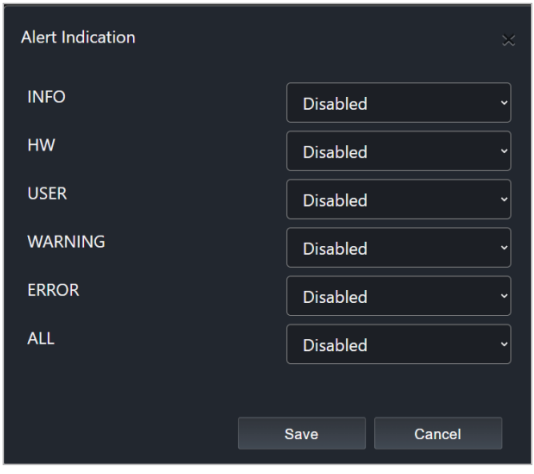
Allows you to set the client device's boot settings through the DASH remote management controller.



Alert Indication

Allows you to set the client device's DASH platform event alert indications.

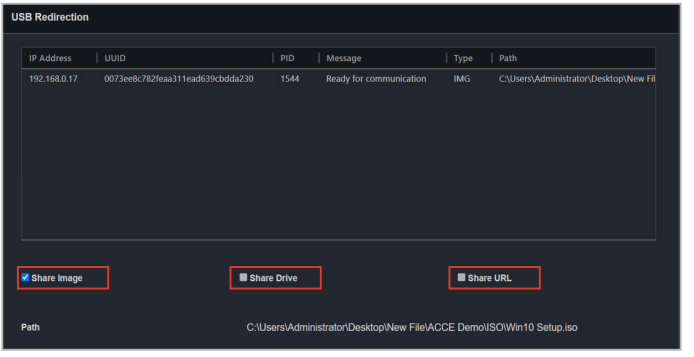
- The Alert Indication categories you can set may vary depending on the support of the client device's DASH remote management controller.
- You can add or edit remote management controller notification rules from **Rule Management**, for more information on **Rule Management**, please refer to **8.1.2 Rule Management**. Once the rule has been set, the Event Log on the Dashboard will show the event log.



5.7.4 USB Redirection

This item allows you to redirect a USB storage device or image file of a client DASH device.

- Before using the USB Redirection function, ensure the USB storage device function has been enabled on the client device.
- The USB redirection function for DASH does not support NTFS format USB devices.



USB and device information	The USB Redirection list displays the IP address and other information about the device the USB is connected to.
Share Image	Select an image file you wish to mount onto the client device.
Share Drive	Allow the client device access to a selected USB storage device connected to the main server device.
Share URL	Copy the path or link to an image file you wish to mount onto the client device.
Image Path	The path of your redirected USB device or image file

Share Image

Allows you to share an Image file.

1. Check **Share Image**.
2. Select the image file you wish to mount, then click **Mount** in the File Picker window.
3. If the image file is successfully mounted, **Ready for communication** will be displayed in the **Message** column.

Share Drive

Allows you to share a USB storage device.

1. Check **Share Drive**, and ensure the remote device's USB function is enabled.
2. Select the USB storage device you wish to mount.
3. If the USB storage device is successfully mounted, **Ready for communication** will be displayed in the **Message** column.

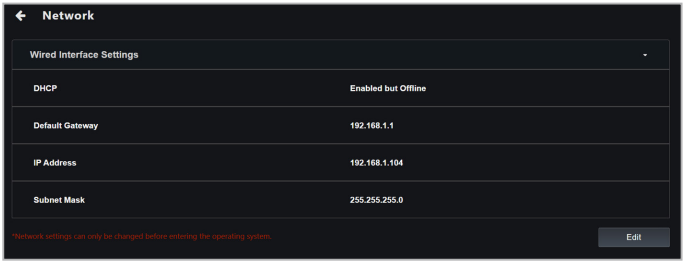
Share URL

Allows you to share an image file URL.

1. Check **Share URL**.
2. Enter the URL of the image file, then click **Mount**.
3. If the image file is successfully mounted, **Ready for communication** will be displayed in the **Message** column.

5.7.5 Network

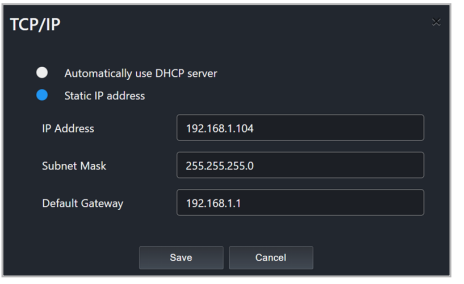
This item allows you to set the wired and wireless network settings of the client DASH device.



DHCP	Displays the Dynamic Host Configuration Protocol (DHCP) state.
Default Gateway	Displays the default gateway.
IP Address	Displays the IP address.
Subnet Mask	Displays the subnet mask.

Network Settings

You can only configure the network settings if the client device has not booted into OS. Once the client device has booted into OS, you can only view the network settings and will not be able to configure the settings.

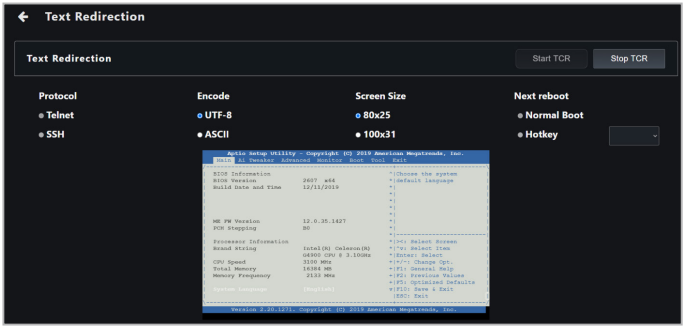


Client IP	Select to use **Static IP address**, or **Automatically use DHCP server** for the client device's IP.
IP Address	Allows you to set the IP address.
Subnet Mask	Allows you to set the subnet mask.
Default Gateway	Allows you to set the default gateway.

5.7.6 Text Redirection

This item allows you to redirect a keyboard or console of a client DASH device through the BIOS settings.

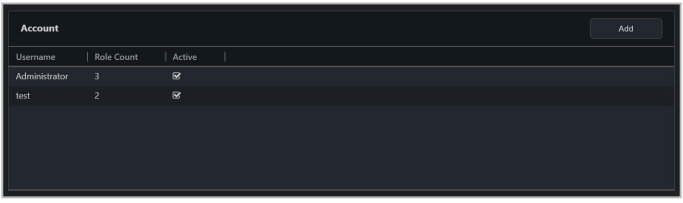
Before using the Text Redirection function, ensure to complete the COM Port settings for Serial Port Console Redirection connection in the client device's BIOS.



Protocol	Select the connection method between Telnet or SSH.
Encode	Select the character encryption between UTF-8 or ASCII.
Screen Size	Select the resolution of the console.
Next Reboot	Select if the next reboot will be a normal boot, or set a hotkey for powering on.

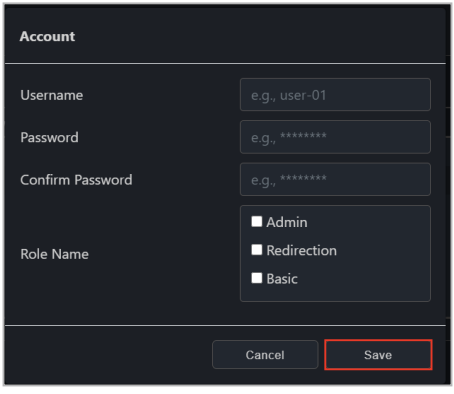
5.7.7 Account Management

This item allows you to add, delete, enable, or disable a DASH remote management controller account.



Adding a new account

1. Click on **Add**.
2. Enter the information of the new account, then click **Save**.



Username	Enter the username.
Password	Enter the password.
Confirm Password	Re-enter the password.
Role Name	Select the role for the account.

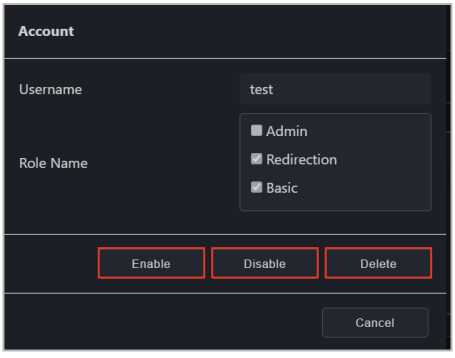
The account and password for the DASH remote management controller is limited to 15 characters.

After setting the account and password, ASUS Control Center will log into the client device's remote management controller. If the login is successful, **Login successful** will be displayed in the **Login Status** on the **Management Controller Information** page.

Enabling, disabling, or deleting a new account

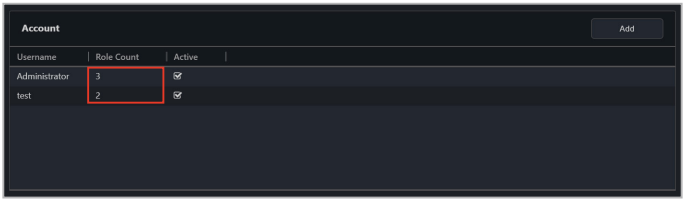
Only newly added accounts can be deleted. The default administrator account can only be edited and cannot be deleted.

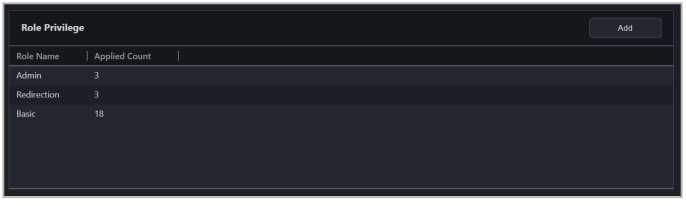
1. Click on the account you would like to enable, disable or delete from the Account list.
2. Click on **Enable**, **Disable**, or **Delete**.
3. You can view the results of your action (**Enable**, **Disable**, or **Delete**) in the Mission Center.



5.7.8 Role privileges

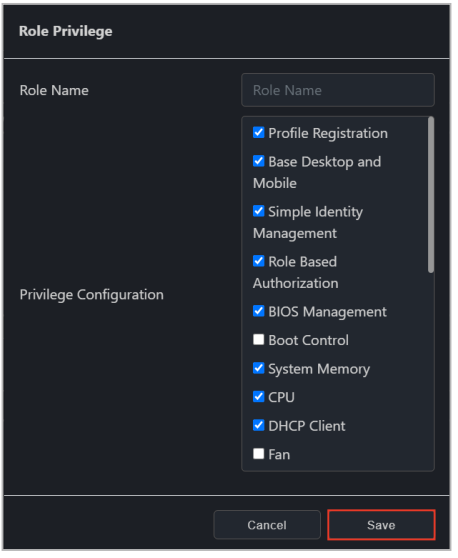
This item allows you to manage role privileges of a DASH account. To access Role privileges, click on the **Role Count** of the account you would like to manage role privileges of.





Adding a new role

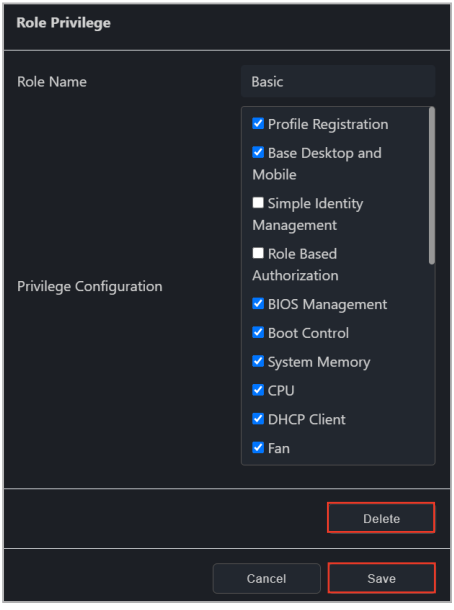
1. Click on **Add** located at the top right of the **Role Privilege** page.
2. Enter the **Role Name**.
3. Check the privileges the new role will have from the **Privilege Configuration** list.
4. Click **Save** once you are finished.



Editing or deleting a role

Only newly added roles can be deleted. The default administrator role can only be edited and cannot be deleted.

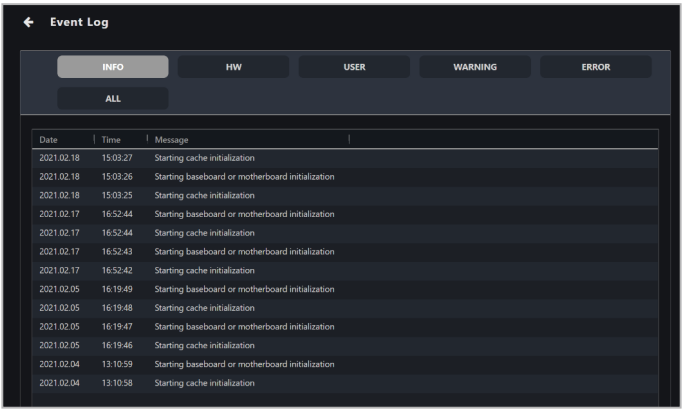
1. Click on the role you would like to edit or delete.
2. You may edit the role name and role privileges, or click **Delete** to delete the role.
3. If you chose to edit the role, click on **Save** once you are finished.



5.7.9 Event Log

This item allows you to view system issues or problems of the client DASH device.

- The event categories displayed will vary depending on support of the DASH remote management controller.
- You can add or edit remote management controller notification rules from **Rule Management**. For more information on **Rule Management**, please refer to **8.1.2 Rule Management**. Once the rule has been set, the Event Log on the Dashboard will show the event log.

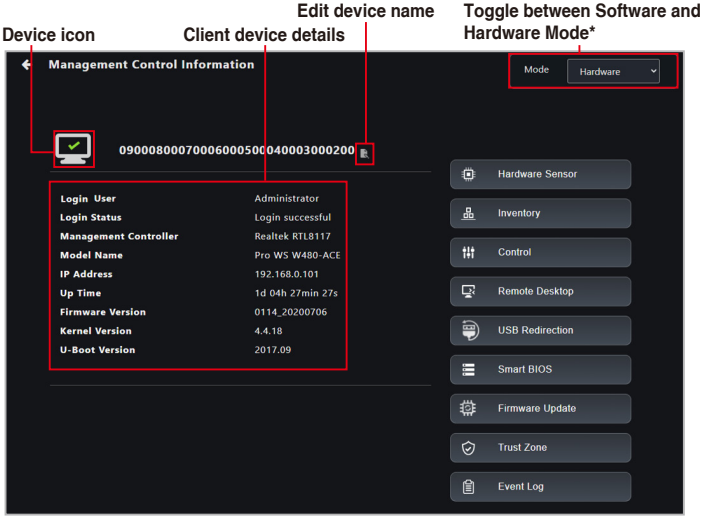


5.8 RTL8117 Management Control Information

The **RTL8117 Management Control Information** allows you to monitor the hardware status, and perform functions through the RTL8117 remote management controller when there is no OS installed on the client device, or when you cannot enter the OS of the client device.

The functions in this section are hardware controlled and values may differ with the software version. Please refer to Chapter 4 for more information on Software mode.

- The client device needs to support RTL8117 remote management controller.
- Ensure the client device's RTL8117 is enabled if this is a new machine which is used for the first time or has been reset to factory settings. In the device's BIOS, navigate to **Advanced** > RTL8117 setting, then enable RTL8117.



* **This item will not be available if you accessed the Management Control Information page through Management Control.**

Machine Name	Displays the machine name. Click on to edit the machine name (max. character limit of 32 characters).
Device icon	Click on the device icon to view the event log of this device.
Login User	Displays the user account currently logged into the client device's RTL8117 remote management controller.

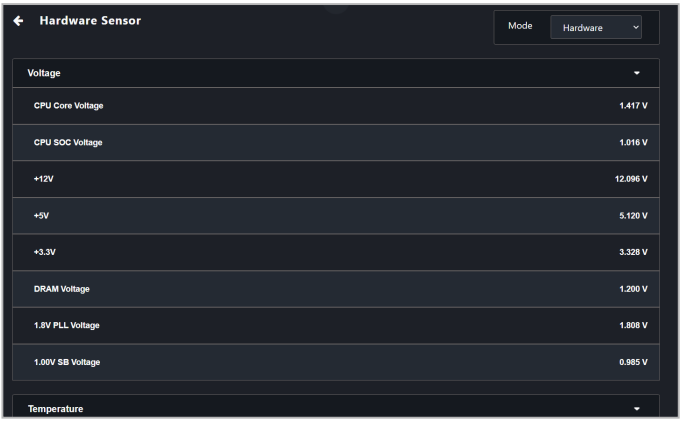
(continued on the next page)

Login Status	Displays the current login status to the client device's RTL8117 remote management controller.
Management Controller	Displays the remote management controller of the client device.
Model Name	Displays the model name of the client device.
Up Time	Displays the up time of the client device the previous session.
Firmware Version	Displays the firmware version of client device's RTL8117 remote management controller.
Kernel Version	Displays the kernel version of client device's RTL8117 remote management controller.
U-Boot Version	Displays the U-Boot version of client device's RTL8117 remote management controller.

5.8.1 Hardware Sensor

This item allows you to view threshold value for items such as voltage, temperature, and fan values of the previous time the device was powered on.

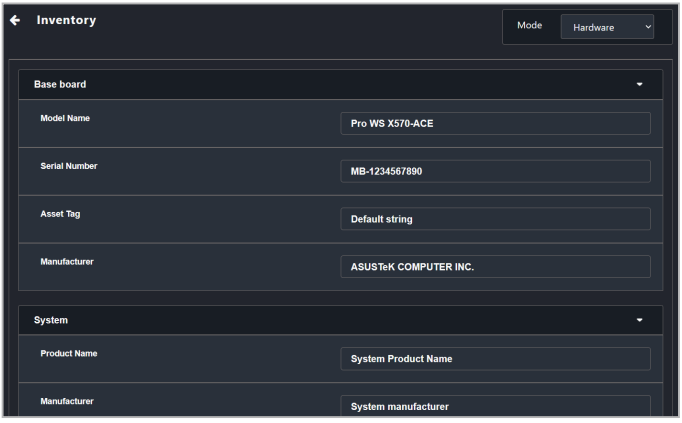
The RTL8117 hardware sensor will only update the data while the client device is in the powering on process (when the client device is restarting).



Voltage	Displays the voltage of the device hardware.
Temperature	Displays the temperature of the device hardware.
Fan	Displays the fan rotation speed of the device hardware.

5.8.2 Inventory

This item displays the client device's hardware details from the previous time the client device was powered on.

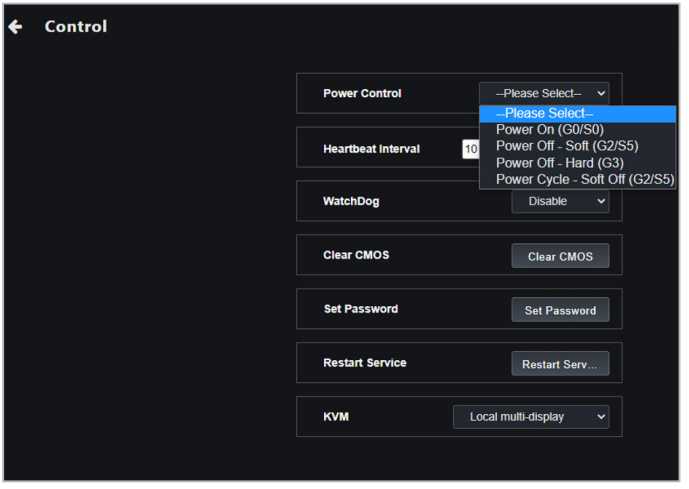


Base board	Displays the motherboard model, serial number, asset tag, and manufacturer information.
System	Displays the product name and manufacturer information.
Memory	Displays the memory location and capacity.
BIOS	Displays the BIOS issue date, version, and manufacturer information
Processor	Displays the processor name and clock information.

5.8.3 Control

This item allows you to manage and control hardware level functions for scenarios where the client may not have an OS installed or cannot enter the OS.

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



Power On (G0/S0)	Power on the client device through the RTL8117 remote management controller.
Power Off - Soft (G2/S5)	Power off the client device through the DASH remote management controller.
Power Off - Hard (G3)	Force the client device to power off through the DASH remote management controller when the OS is unresponsive.
Power Cycle - Soft off (G2/S5)	Restart the client device after shutting down from the OS through the DASH remote management controller.
Heartbeat Interval*	Allows you to set the time interval in seconds for which the hardware signals are checked.

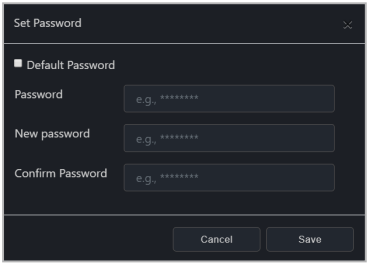
(continued on the next page)

Watchdog*	Enable or disable the Watchdog monitoring function. If the Watchdog function is enabled and the client device triggered the Watchdog function causing the client device to restart, the Watchdog function will be reverted to the default disabled state. Ensure to re-enable the Watchdog function for the client device.
Clear CMOS	Clears the BIOS setup information through RTL8117 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.
Set Password	Set an RTL8117 encryption password. Restart the client device once you have set the new password for the changes to take effect.
Restart Service	Restart service through RTL8117.
KVM	Enable or disable KVM.

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

Setting the password for RTL8117

You can set an encryption password for RTL8117 using the **Set Password** function.



Default Password	Check this item to load a previously set password to the **Password** field. If no RTL8117 password was previously set, checking Default Password will load the system's default password.
Password	Enter the current password , or you may check **Default Password** to load a previously set password.
New Password	Enter the new password.
Confirm Password	Re-enter the password.

- The password should be a minimum of 8 characters and should only consist of uppercase characters, lowercase characters, and numbers.
- Restart the client device once you have set the new password for the changes to take effect.

5.8.4 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. 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 RTL8117 LAN IC.
- The main server will save the current KVM status, if this status has been changed, ensure to reboot the system to ensure the changes are saved.

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** > **OOB-Control** > **KVM** > **KVM Enable** to enable KVM.

If you need to disable the KVM, click **Select function** > **OOB-Control** > **KVM** > **KVM Disable**, then restart the client device.

2. Next, click **Select function** > **OOB-Control** > **KVM**, and select the KVM Display Mode you would like to use. You may refer to the table below for more information.

Remote Mulit-Display	BIOS screen will be mirrored on both server remote desktop and client devices. OS screen will only be displayed on the server remote desktop.
Local Multi-Display	BIOS screen will be mirrored on both server remote desktop and client devices. OS screen will only be displayed on the client device.
Remote Single-Display	BIOS and OS screen will only be displayed on the server remote desktop.
Disable	BIOS and OS screen will only be displayed on the client device.

3. Reboot the client device and enter BIOS setup, then navigate to **Advanced** > **RTL8117 setting** and set **RTL8117 Manager Controller** to **[Enabled]**.

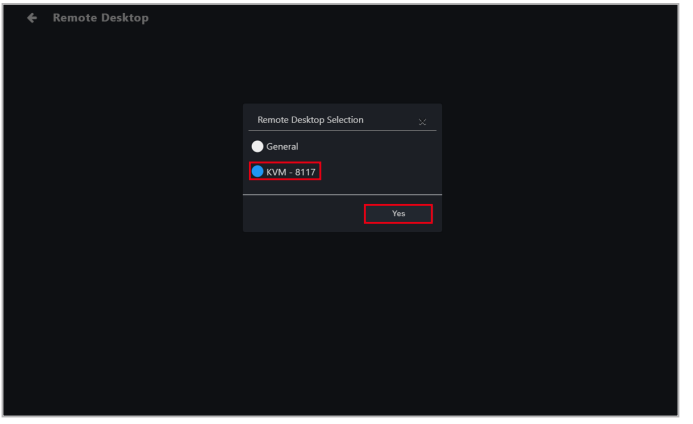
The BIOS settings may differ between client devices. Please refer to your client device's motherboard user manual for more information about navigating the BIOS and BIOS settings.

4. Click on the drop down menu of the **KVM Display Mode** option, and select the same display mode as the one selected in step 1.

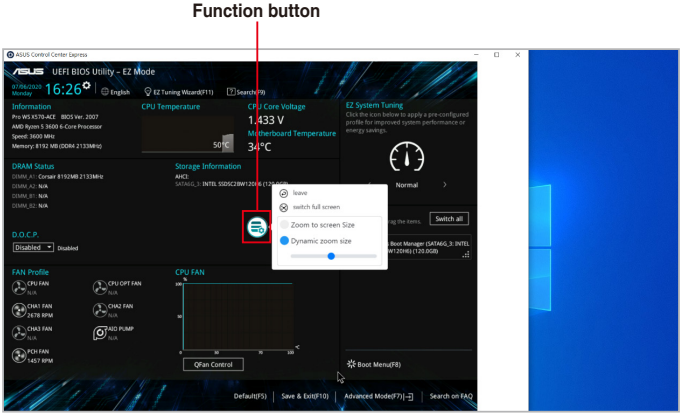
Using the out-of-band management Remote Desktop

On the Management Control Information page of the RTL8117 device, click **Remote Desktop**, select **KVM - 8117** then click on **Yes** to remotely control your client device even if it is not in an OS environment.

- If you accessed **Remote Desktop** through a client device's **Management Control Information** by clicking on **Management Control**, then clicking on a client device, then **Remote Desktop** will automatically enter **KVM - 8117** mode.
- KVM remote desktop is a hardware mode function. The functions between KVM remote desktop and software mode remote desktop may differ.



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

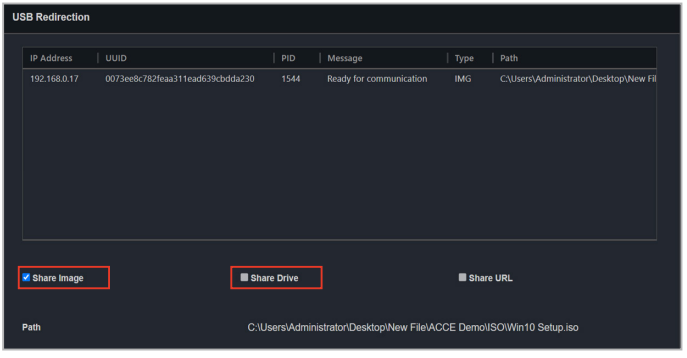


	Leave	: Return to the previous options
	Display remote mouse cursor	: When there is no mouse connected to the client, there may not be a mouse cursor available for the remote screen, click to display a remote mouse cursor on the remote desktop screen.
	Leave	: Return to the previous options
	Switch full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

5.8.5 USB Redirection

This item 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 client device is connected using a management LAN port which supports RTL8117 LAN.
- Before using the USB Redirection function, ensure the USB storage device function has been enabled on the client device.
- The USB redirection function for RTL8117 does not support the **Share URL** function.



USB and device information	The USB Redirection list displays the IP address and other information about the device the USB is connected to.
Share Image	Select an image file you wish to mount onto the client device.
Share Drive	Allow the client device access to a selected USB storage device connected to the main server device.
Share URL	Copy the path or link to an image file you wish to mount onto the client device.
Image Path	The path of your redirected USB device or image file

Share Image

Allows you to share an Image file.

1. Check **Share Image**.
2. Select the image file you wish to mount, then click **Mount** in the File Picker window.
3. If the image file is successfully mounted, **Ready for communication** will be displayed in the **Message** column.

Share Drive

Allows you to share a USB storage device.

1. Check **Share Drive**, and ensure the remote device's USB function is enabled.
2. Select the USB storage device you wish to mount.
3. If the USB storage device is successfully mounted, **Ready for communication** will be displayed in the **Message** column.

5.8.6 Smart BIOS

This item allows you to update the BIOS of a device by uploading a BIOS file manually or from the BIOS Cache if the device cannot be powered on to perform a BIOS update or repair.

The client device will begin updating the BIOS after shutting down. The update process may take a while, please wait for the update to be finished. Once the BIOS flash is finished the client device will restart.

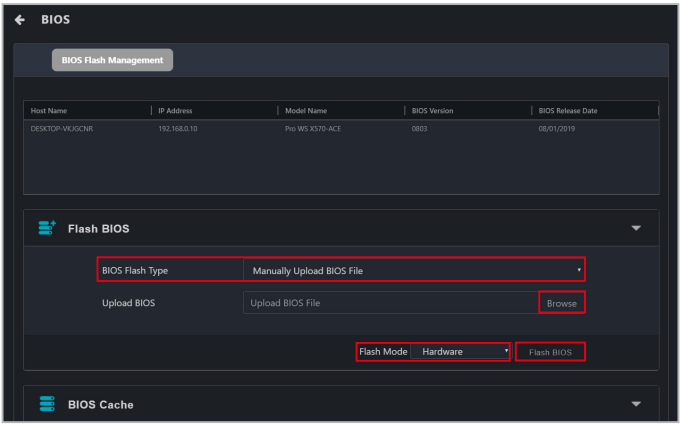
DO NOT disconnect the power supply during the BIOS flash.

Flashing BIOS by manually uploading a 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.

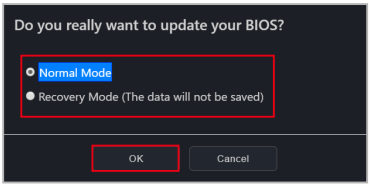
1. Select **Manually Upload BIOS File** in the **BIOS Flash Type** field.
2. Click on **Browse** to select a BIOS file, then click **OK** to confirm the BIOS file was uploaded successfully. The uploaded BIOS file will also be added to the **BIOS Cache**
3. Click on **Flash BIOS**.

Flash Mode will default to **Hardware Mode**.



5. 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.

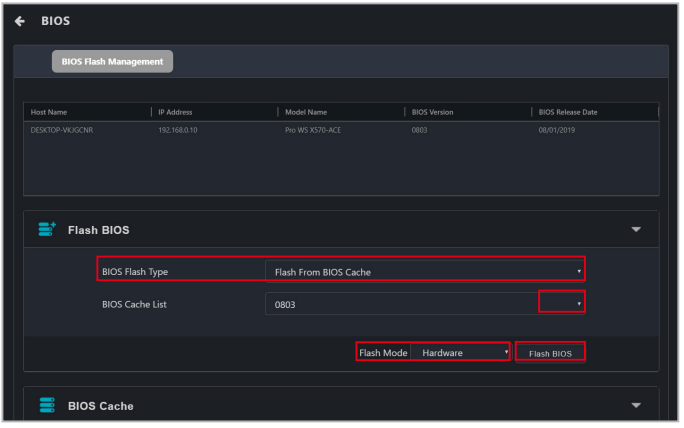


Flashing BIOS from the BIOS cache

You can select a BIOS file from the BIOS cache.

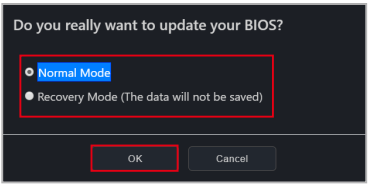
1. Select **Flash from BIOS Cache** in the **BIOS Flash Type** field.
2. Select a BIOS file from the **BIOS Cache List** drop down menu.
3. Click on **Flash BIOS**.

Flash Mode will default to **Hardware Mode**.



5. 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**.

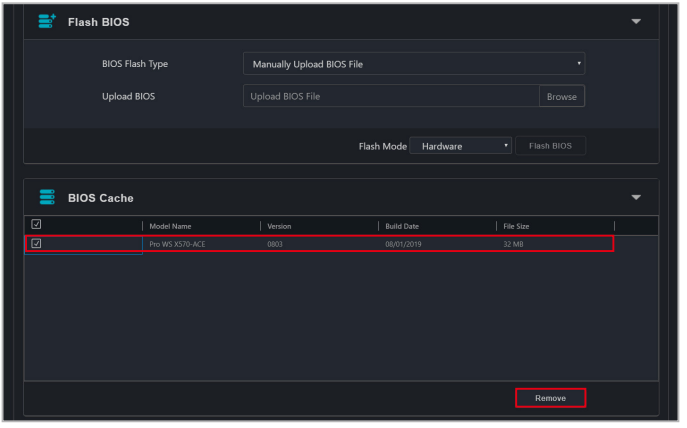
Performing a **Recovery Mode** BIOS Flash will reset all BIOS configurations, and remove all previous configurations.



6. (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**.



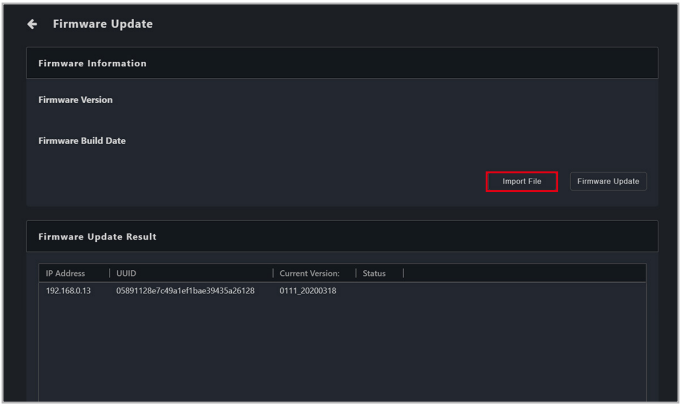
5.8.7 Firmware Update

This item allows you to update the firmware of the RTL8117 LAN IC, and also displays the results of the firmware update.

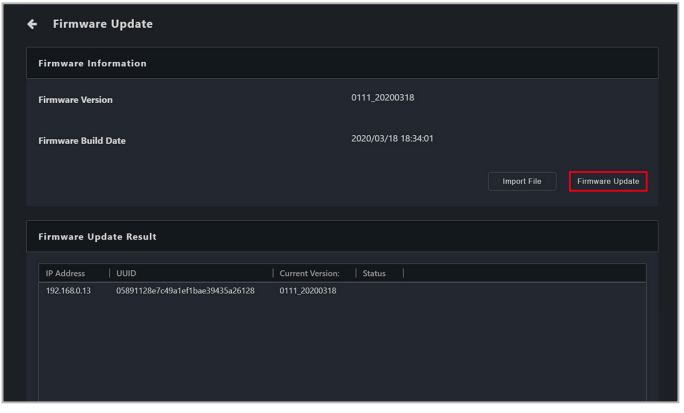
Firmware Update will be disabled when KVM is set to enabled. To update firmware please set KVM to disabled.

Uploading and updating firmware

1. Click on **Import File**, then select you 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.

5.8.8 Trust Zone

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.

The **Trust Zone** function provides a method of protecting your client devices from being accessed by unauthorized or non-trusted connections. This item will allow you to set main server IP addresses to a client device's trust zone , and only main server IP addresses added to the Trust Zone are allowed to perform remote management control functions on the client device.

If you access the Trust Zone page using the following methods:

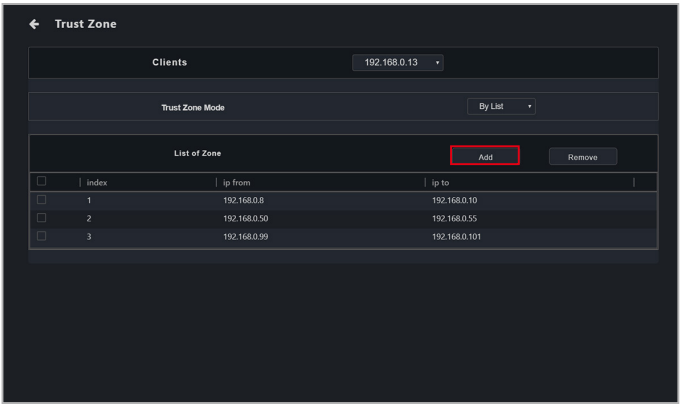
- Clicking on in the M.C column of the Devices List.
- Scanning, then selecting a device from the Management Controller page.

You will only be able to set the Trust Zone of the selected device. To view the Trust Zone of multiple devices, please navigate back to the main menu page, then select multiple devices and select **OOB-Control** > **Trust Zone** from the **Select Function** drop down menu.

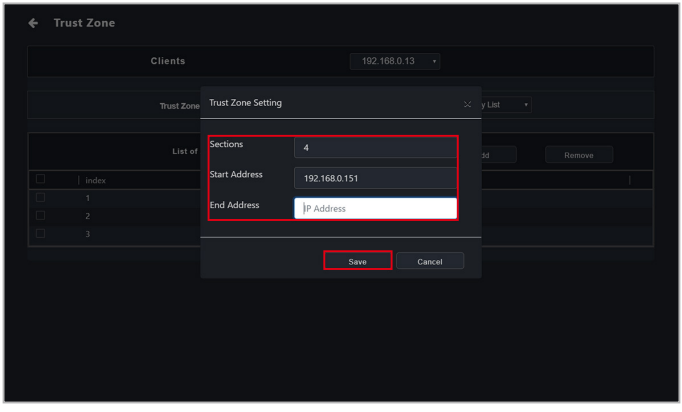
Adding a trust zone

Up to 8 sets of main server IP address ranges may be added to a client device, if you already have 8 sets and wish to add more, please remove an existing set of IP address range from the trust list before adding the new IP address range.

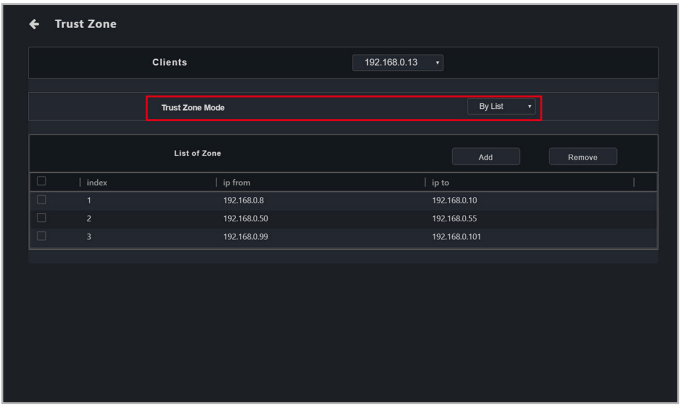
1. Click on **Add**.



2. Enter the IP address range of a main server you wish to add to the client device's trust zone, then click **Save**.

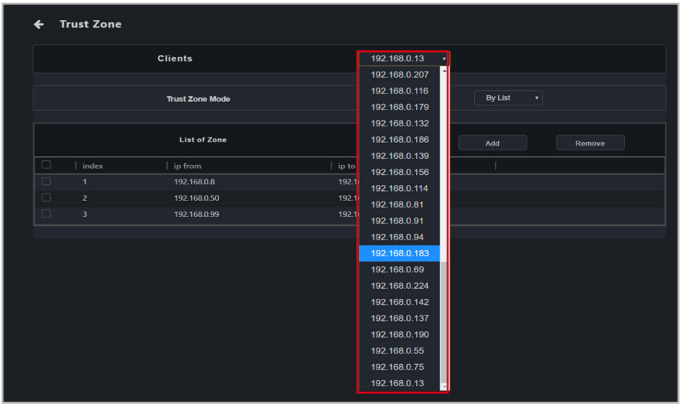


3. Repeat steps 1 and 2 to add more IP address ranges to the trust zone.
4. Select **By List** in the **Trust Zone Mode** field drop down menu to activate the IP addresses added to the trust zone list.



5. (optional) Select another device from the **Clients** drop down list to set the trust zone for the selected device.

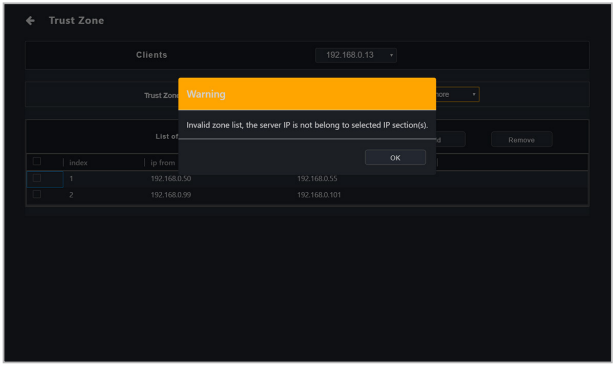
Only follow this step if you selected multiple devices to set the trust zone.



6. (optional) Repeat steps 1 to 4 to add main server IP address ranges to the trust zone of the newly selected device.

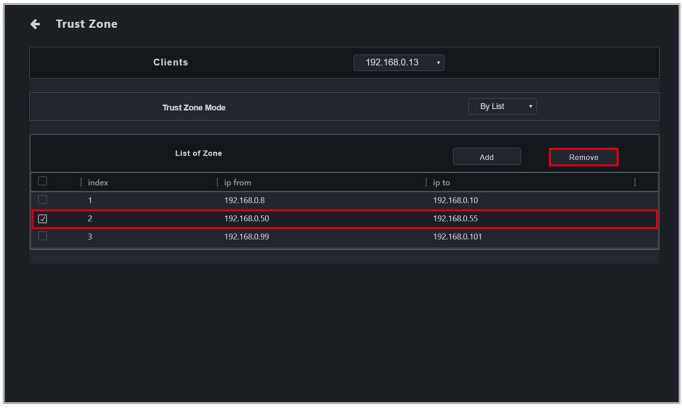
Only follow this step if you selected multiple devices to set the trust zone.

Ensure that the trust zone list contains a main server IP address, if the trust zone list does not contain a main server IP address, the trust zone cannot be activated.



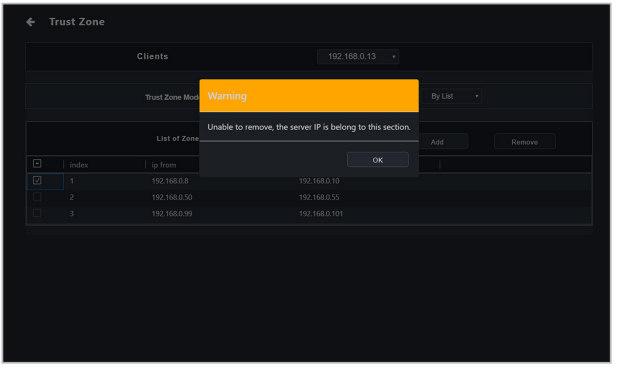
Deleting a trust zone

Check the IP addresses you would like to delete from the trust zone list, then click on **Remove**.



If you wish to disable an activated trust zone list, select **Disable** from the Trust Zone Mode field drop down menu.

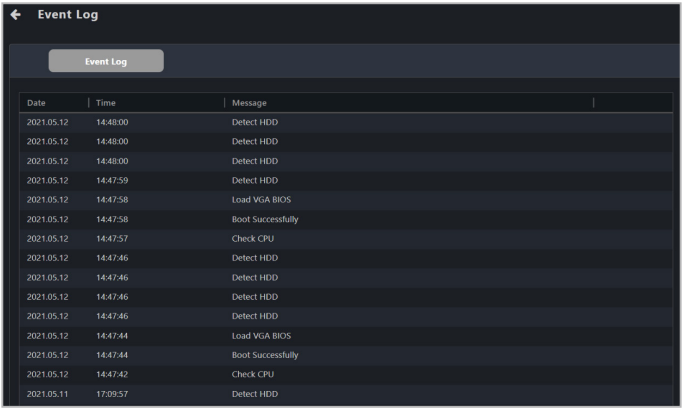
- The main server IP address cannot be removed from an activated trust zone list, ensure that the main server IP address is not included in the IP sections you would like to remove.



- If a main server's IP address was changed due to other reasons, and is already included in an activated trust zone of a client device, you will not be able to perform remote management control functions on the client device through the main server with the new IP address as it is not included in the client device's trust zone. You can set the new main server IP address on the client device through BIOS > **Advanced** > **RTL8117 Settings**.

5.8.9 Event Log

This item allows you to view the event log of the last time the client device was powered on, giving you more information to analyze the reason for the problem or issue.

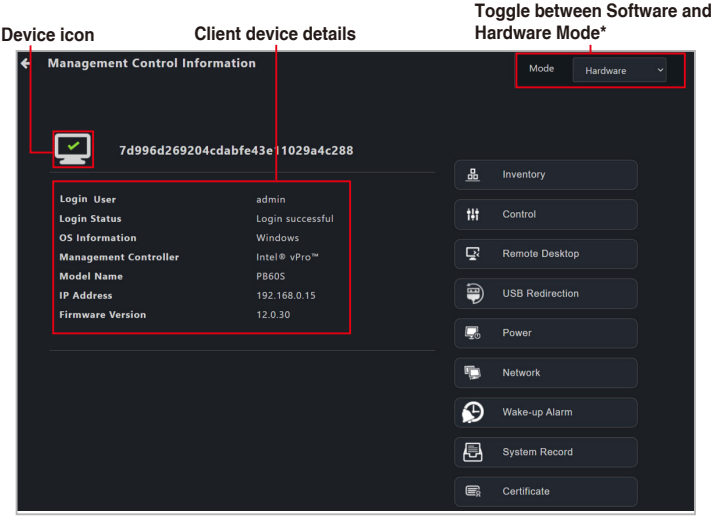


5.9 vPro Management Control Information

The **vPro Management Control Information** allows you to remotely perform repairs when an error occurs on the client OS, check the hardware assets when the device powered off, pin point system errors using the event log and trap alert system, and provide network management and network protection for client devices.

The functions in this section are hardware controlled and values may differ with the software version. Please refer to the **Device Information** chapter for more information on Software mode.

- The client device needs to support Intel vPro remote management controller.
- Availability of certain functions may vary depending on whether the client device supports Intel Standard Manageability (ISM), Active Management Technology (AMT), or Small Business Technology (SBT). Use Intel MEBx to check which functions are supported on the client device.
- Ensure that the client device's BIOS AMT and Intel MEBx settings are set to enable the client device's vPro functions before using these functions through the management controller.
- Any mention of the trademark Intel or Intel vPro, are trademarks of Intel Corporation or its subsidiaries.



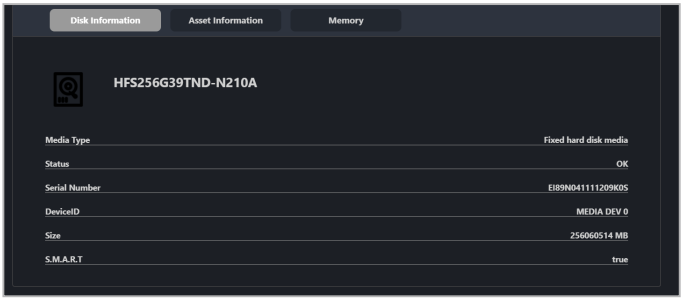
* **This item will not be available if you accessed the Management Control Information page through Management Control.**

Device Icon	Displays the connection status of the client device's vPro remote management controller.
Login user	Displays the user account currently logged into the client device's vPro remote management controller.
Login Status	Displays the current login status to the client device's vPro remote management controller.
Management Controller	Displays the remote management controller of the client device.
Model Name	Displays the model name of the client device.
IP Address	Displays the IP address of client device.
Firmware Version	Displays the firmware version of client device's vPro remote management controller.

5.9.1 Inventory

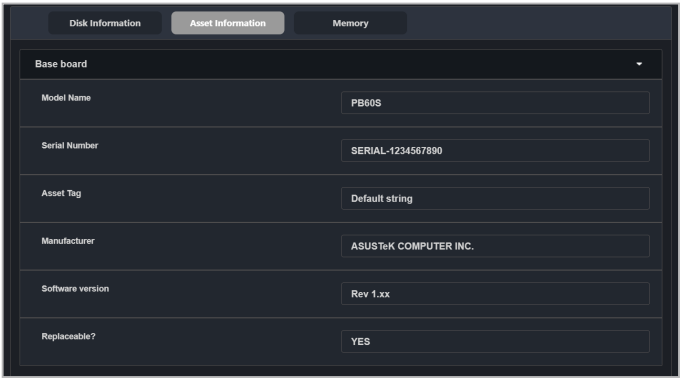
This item displays the client device's disk, hardware asset, and memory information.

Disk Information



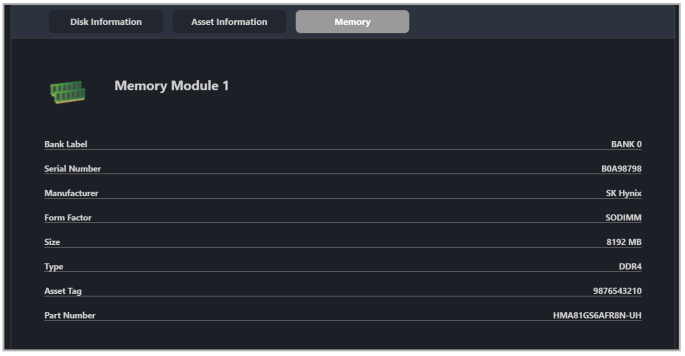
Device Name	Displays the name of the disk device.
Media Type	Displays media type of the disk device.
Status	Displays the current status of the disk device.
Serial Number	Displays the serial number of the disk device.
DeviceID	Displays the ID of the disk device.
Size	Displays the capacity size of the disk device.
S.M.A.R.T	Displays the S.M.A.R.T attribute status.

Asset Information



Base board	Displays the model name, serial number, asset tag, manufacturer and other information of the base board.
Platform	Displays the product name, serial number, manufacturer and other information.
BIOS	Displays the release date, version, manufacturer, and other information of the BIOS.
Processor	Displays the manufacturer, family, model, clock speed, and other information of the processor.

Memory



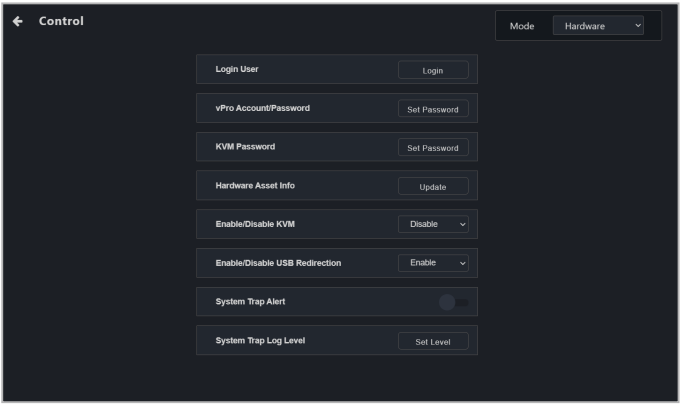
Bank Label	Displays the bank label of the memory module.
Serial Number	Displays the serial number of the memory module.
Manufacturer	Displays the manufacturer of the memory module.
Form Factor	Displays the form factor of the memory module.
Size	Displays the capacity of the memory module.
Type	Displays the type of the memory module.
Asset Tag	Displays the asset tag of the memory module.
Part Number	Displays the part number of the memory module.

5.9.2 Control

This item allows you to set the account and password, KVM, USB redirection, system trap alert, and system trap log level functions of the vPro device.

You can add or edit remote management controller notifications in Notification Rule. The Event Log on the dashboard will display the system Trap Alert notifications you have set.

- The password for vPro Account must be at least 8 characters long, and must contain one uppercase character (A-Z), numbers (0-9), and one special character.
- The KVM password must contain 8 characters, and must contain uppercase characters (A-Z), lowercase characters, numbers (0-9), and special characters.
- Ensure that port 162 is opened before enabling system trap alerts.



vPro Account/Password	Set the account and password of the vPro device.
Hardware Asset Information	Update the hardware asset information of the client device.
KVM Password	Update and set the vPro device's KVM password.
Enable/Disable KVM	Enable or disable the KVM of the device.
Enable/Disable USB Redirection	Enable or disable the USB redirection function.
System Trap Alert	Enable or disable the system trap alert.
System Trap Log Level	Set the log level of system trap (Information, Warning, Error)

5.9.3 Remote Desktop

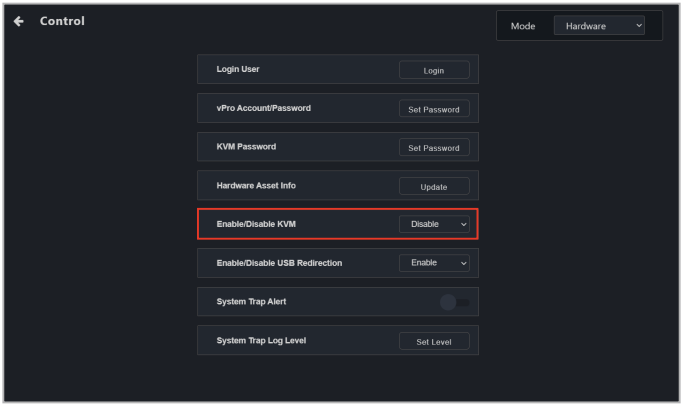
The **Remote Desktop** function allows you to control a vPro client device through KVM. This is useful for remotely monitoring and repairing the client device, should the client device's OS encounter an error.

- Availability of certain functions may vary depending on vPro support and ME version. Remote desktop is not supported by Intel Standard Manageability (ISM).
- If the client device is operating from the Intel MEBx, you will not be able to connect using KVM.
- The device will not be able to enter the Intel MEBx settings page if the client device was restarted whilst using KVM.
- When using the KVM remote desktop function of a vPro device, the border of the client device screen will flash red and yellow to indicate that the client device is currently running the KVM remote desktop function.

Setting up KVM before using Remote Desktop

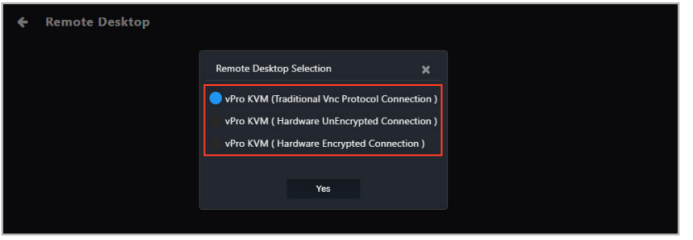
Before using the Out-of-band Management Remote Desktop function for the first time, ensure that KVM is enabled. On the Management Control Information page of the vPro device, click **Control**, then click the drop down menu of the **Enable/ Disable KVM** field and select **Enable**.

To disable KVM, select the **Disable** option and restart the client device.



Using the out-of-band management Remote Desktop

On the Management Control Information page of the vPro device, click **Remote Desktop**, then select the desired connection method



Traditional VNC protocol connection	Establish an encrypted connection using the VNC protocol.
Hardware unencrypted connection	Establish an unencrypted connection.
Hardware encrypted connection	Establish an encrypted connection using the TLS protocol.

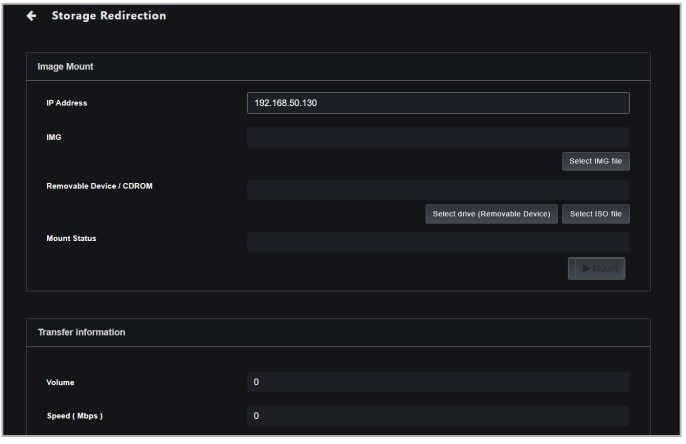
- The default quality for hardware encrypted connections is set to Low. Use the Function button after establishing a connection to adjust the quality. Quality options may vary depending on vPro and ME support.
- Ensure that a KVM password is set before attempting to establish a traditional VNC protocol connection. To set the KVM password, open the **Control** page, then click **KVM Password**. The KVM password must be at least eight characters and must include at least one upper case, one lower case, and one special character.

Once a connection is established, clicking the Function button offers more options for navigating the remote desktop screen. Refer to **4.9 Remote Desktop (General)** for more information on the Function button.

5.9.4 Storage Redirection

This item allows your vPro device to redirect USB-R/IDE-R storage.

- The USB redirection function for vPro does not support NTFS format USB devices.
- When using the USB redirection function for vPro, the client device will be displayed as Floppy Disk A, CD Drive (drive code) when successfully mounted.

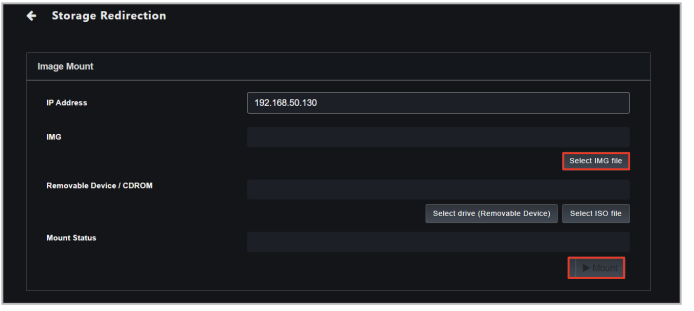


IP Address	Displays the IP address of the client device.
IMG	Select the image file (.img) to transfer.
Removable Device / CDROM	Select the removable storage device or ISO file (.iso) to transfer.
Mount Status	Displays the mount status of the device and files.
Volume	Displays the amount of data transferred.
Speed(Mbps)	Displays the transfer speed of the data.

Mounting an image file

After enabling USB Redirection on the Control page, please follow the steps below to mount an image file.

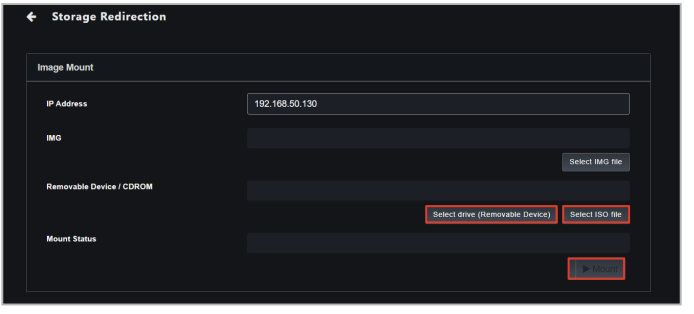
1. Click **Select IMG file**, then select the image file you wish to mount in the File picker and click **OK**.
2. Click **Mount**.



Mounting a removable device or CDROM (ISO file)

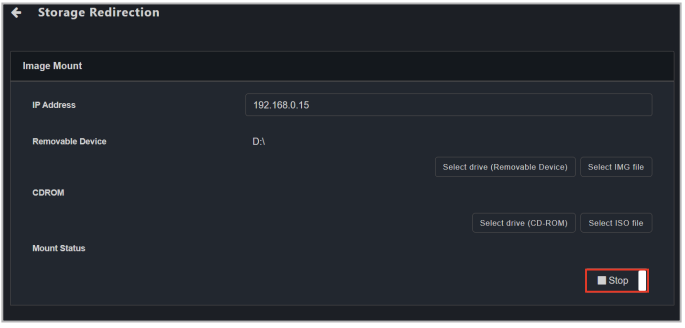
Follow the steps below to mount a removable device or ISO file.

1. Click **Select drive (Removable device)**, or **Select ISO file**, then select the device or ISO file you wish to mount in the File picker and click **OK**.
2. Click **Mount**.



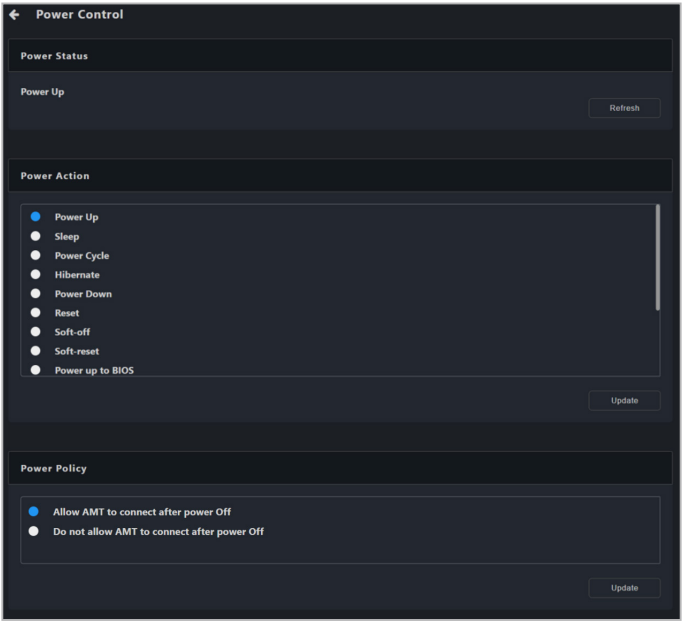
Ending storage redirection

Click **Stop** to end storage redirection.



5.9.5 Power

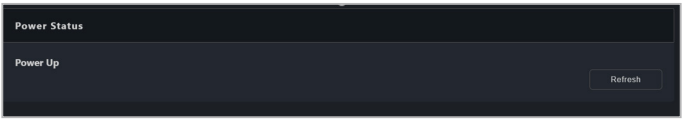
This item allows you to view the client vPro device's power status, and also allows you to execute power control functions.



Power Status

This item allows you to view the client device's current power status.

Clicking on **Refresh** will update the information shown on the Power Status page to the latest information.

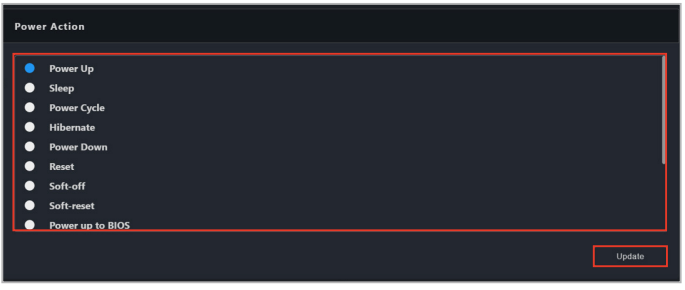


Power Action

This item allows you to select the power action the client device should execute.

The power actions available may differ depending on the client device's power and operating system status. Please refer to the actual options available on your screen.

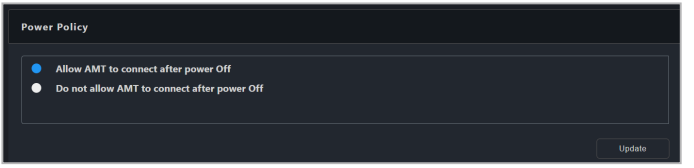
1. Select a power action from the **Power Action** list.
2. Click on **Update**.



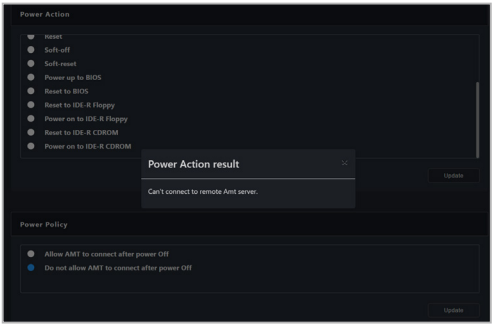
3. Check if the power action is correct in the confirmation window, then click **OK**.
4. You can check if the power action has been executed by checking if the **Power Status** has been updated to the power action you selected.

Power Policy

This item allows you to select whether to allow AMT to connect after powering off.



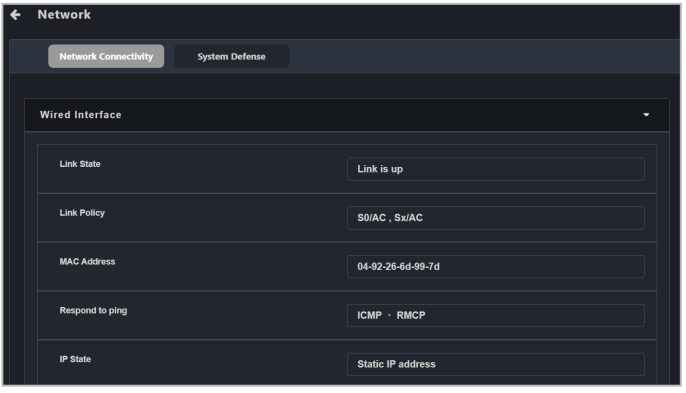
If you selected **Do not allow AMT to connect after power Off**, you will not be able to execute power control functions, refresh the power status, or change power policy while the client device is powered off. If you wish to execute power control functions, please set the power policy to **Allow AMT to connect after power Off** once the client device has been woken up or powered on.



5.9.6 Network

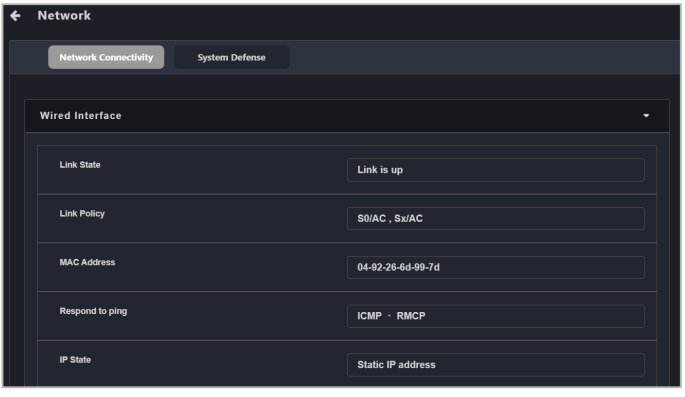
This item allows you to set the wired and wireless network settings of the client vPro device, and also allows you to use the **System Defense** function to implement Internet safety precautions.

Wireless interface settings may be unavailable on vPro client devices with Intel Standard Manageability (ISM).



Network Connectivity

This item allows you view and manage the wired/wireless network status and settings.

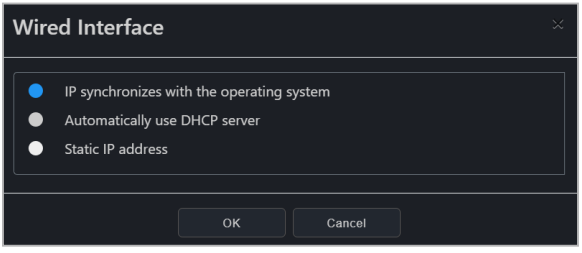


- **Wired Interface Settings**
  Displays and allows you to configure wired network settings of the client device.

Link State	Displays the wired network link state.
Link Policy	Displays the wired network link policy.
MAC Address	Displays the wired network MAC address.
Respond to ping	Displays the wired network ping response protocol.
IP State	Displays the wired network IP state.
IP Address	Displays the wired network IP address.
IP Default Gateway	Displays the wired network IP default gateway.
IP Subnet Mask	Displays the wired network IP subnet mask.
IP Domain Name Server	Displays the wired network IP Domain Name Server.

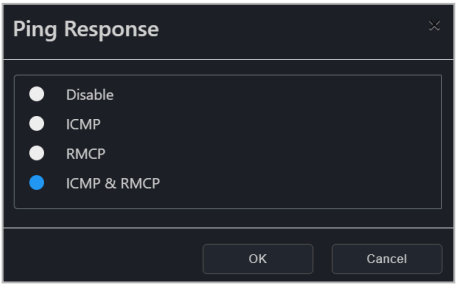
Editing wired interface IP

Click on **Edit** in the Wired Interface Settings block to set the client device's IP from either **IP synchronizes with the operating system**, **Automatically use DHCP server**, or **Static IP address**.



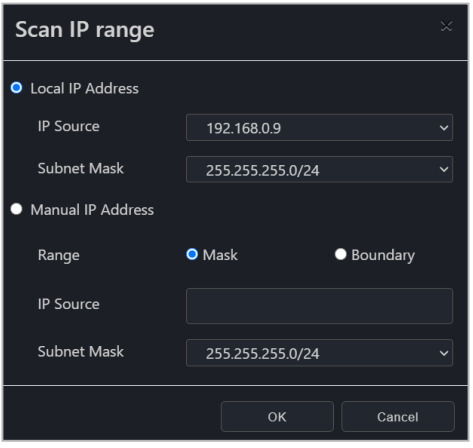
Setting ping packet response

Click on **Set ping packet response** in the Wired Interface block to set the client device's wired network pin packet response from either **Disable**, **ICMP**, **RMCP**, or **ICMP & RMCP**.



Searching for device

Click on **Search for device** in the Wired Interface block to search for a device within a given IP range. For more information on scanning an IP range, please refer to **3.2.2 Scanning an IP range**.

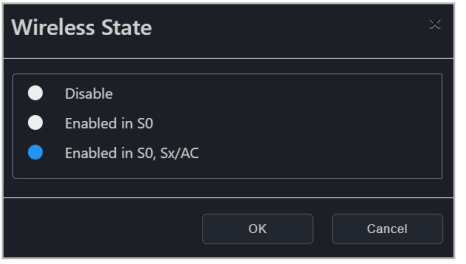


- **Wireless Interface Settings**
  Displays and allows you to configure wireless network settings of the client device.

Link State	Displays the wireless network link state.
Link Policy	Displays the wireless network link policy.
MAC Address	Displays the wireless network MAC address.
State	Displays the wireless network settings state.
Radio State	Displays the wireless network radio state.
IP Address	Displays the wireless network IP address.
IP Default Gateway	Displays the wireless network IP default gateway.
IP Subnet Mask	Displays the wireless network IP subnet mask.
IP Domain Name Server	Displays the wireless network IP Domain Name Server.

Setting wireless state:

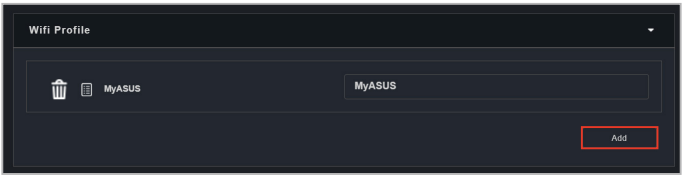
Click on **Edit** in the Wireless Interface Settings block to set the client device's wireless state from either **Disable**, **Enabled in S0**, or **Enabled in S0, sX/AC**. The wireless network's connection will proceed according to the wireless state selected.



- **Wi-Fi Profile**
  This item allows you to add or edit the Wi-Fi profile(s) of the client device. The client device will connect/disconnect according to the Wi-Fi profile and wireless state selected.

  Adding a new Wi-Fi profile

  1. Click on **Add**.



2. Enter the information for the Wi-Fi profile.
3. Click on OK once you are finished. The newly added Wi-Fi profile should appear in the profile list.

Editing a Wi-Fi profile

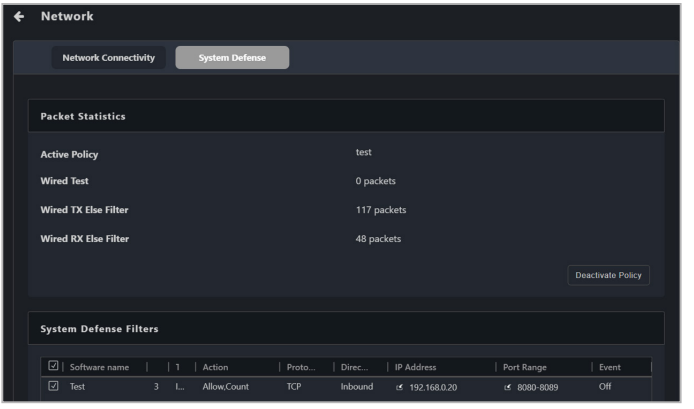
To edit an existing Wi-Fi profile click on the edit icon ( ) next to the profile name.

Deleting a Wi-Fi profile

To delete an existing Wi-Fi profile click on the delete icon ( ) next to the profile name.

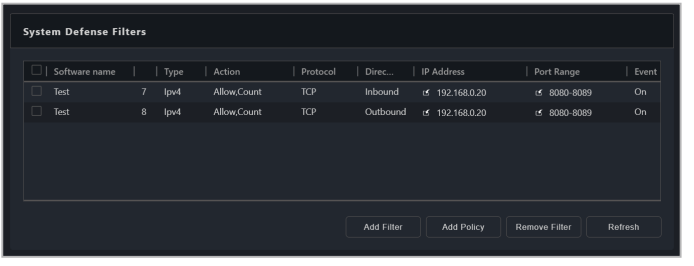
System Defense

This item allows you to define and execute Internet safety measures on the client device, allowing you to isolate the network and also providing you with an intrusion test function.



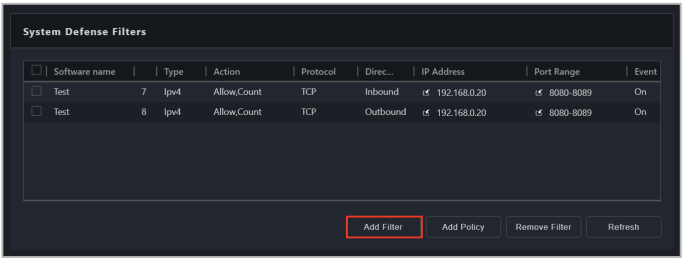
- **System Defense Filters**
  This item allows you set the outgoing and incoming packets for the isolated network, allow or ban specific IP addresses, and set network traffic filters to calculate and record data transfer.

Click on **Refresh** to refresh the System Defense Filters list to the latest updated state.

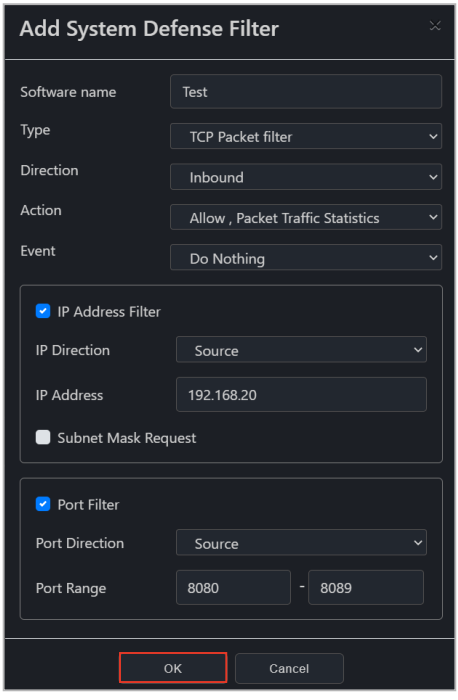


Adding a system defense filter

1. Click on **Add Filter**.



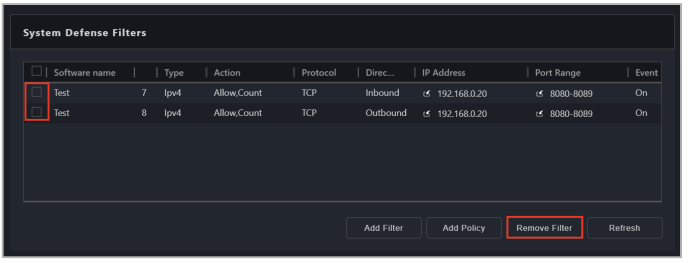
2. Select and enter the settings for the new system defense filter, then click **OK**.



3. Repeat steps 1 and 2 to add more system defense filters.
4. The newly added system defense filter(s) will be displayed in the System Defense Filters list.

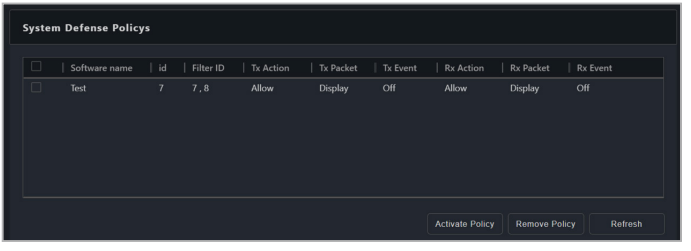
Removing a system defense filter

To remove a system defense filter(s), select the system defense filter(s) you would like to remove, then click **Remove Filter**.



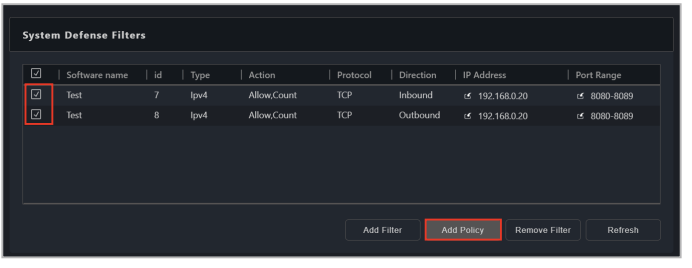
- **System Defense Policy**
  This item will check incoming and outgoing packets to see if they match or do not match the conditions set in the filter, then act according to the settings of the policy.

Click on **Refresh** to refresh the System Defense Policy list to the latest updated state.

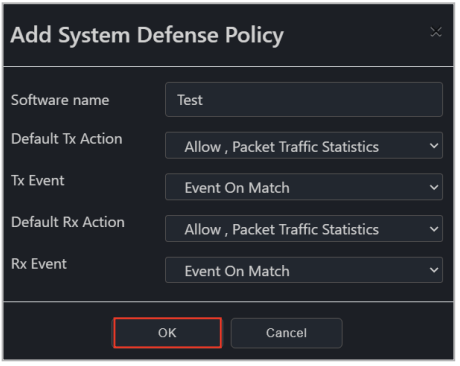


Adding a system defense policy

1. Select the system defense filters you would like to add a policy to in the System Defense Filters list, then click **Add Policy**.



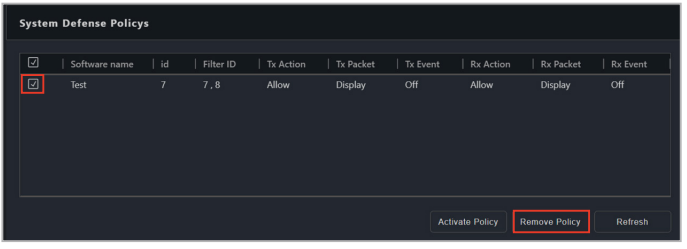
2. Select and enter the settings for the system defense policy, then click **OK**.



3. The newly added system defense policy will be displayed in the System Defense Policys list.

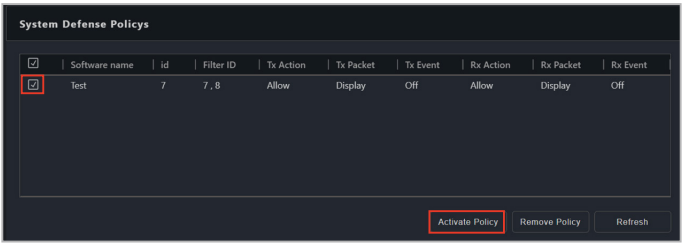
Removing a system defense policy

Select the system defense policy you would like to remove in the System Defense Policys list, then click **Remove Policy**.

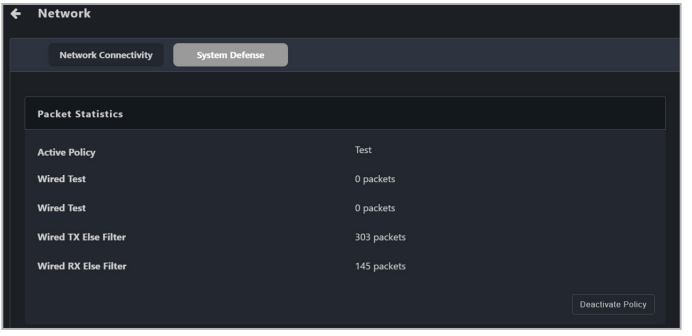


Activating a system defense policy

Select the system defense policy you would like to activate in the System Defense Policys list, then click **Activate Policy**.



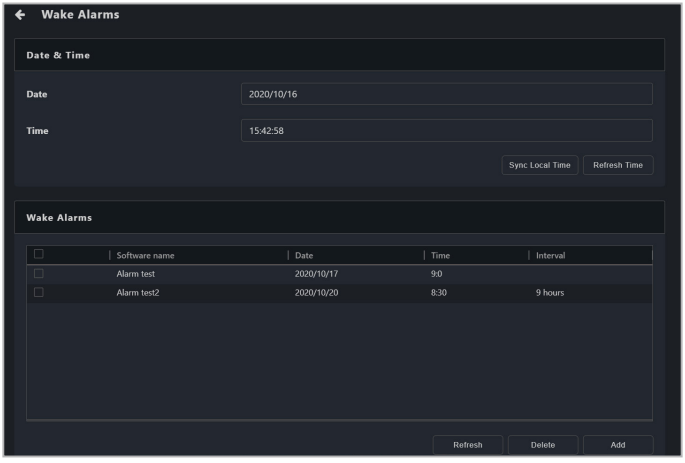
You can view packets statistics if you scroll to the top of the **System Defense** page, under the Packet Statistics block.



Only one System Defense Policy may be active at a time, if you wish to use a different System Defense Policy, click on **Deactivate Policy** in the Packet Statistics block to deactivate the currently active policy, then activate the new policy.

5.9.7 Wake-up Alarm

This item allows you to set an alarm to wake up the client vPro device when the client device is in sleep mode or powered down.

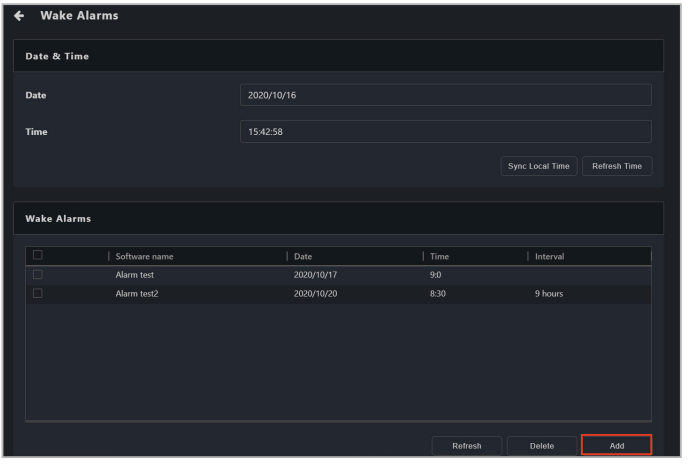


Date	Date on the client vPro device.
Time	Time on the client vPro device.
Sync Local Time	Synchronizes the client vPro device's time to match the main server's.
Refresh Time	Updates the client vPro device's time to the latest updated state.

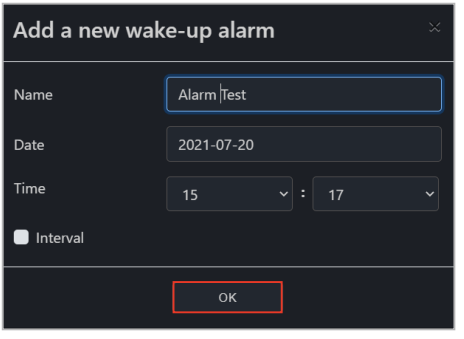
Adding a new wake alarm

- Up to five (5) wake alarms can be added to a single client vPro device, if you have reached the maximum limit of wake alarms allowed on a device, please delete an unused wake alarm first.
- Click on **Refresh** to refresh the Wake Alarms list to the latest updated state.

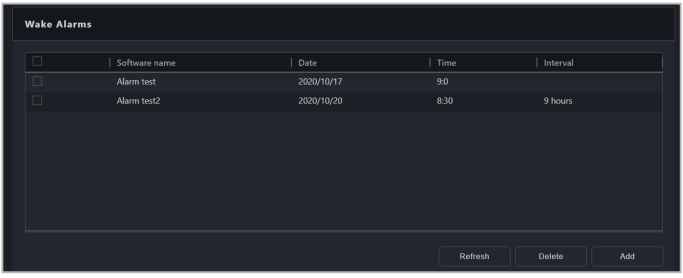
1. Click on **Add**.



2. Enter the settings for your new wake alarm, then click **OK**.

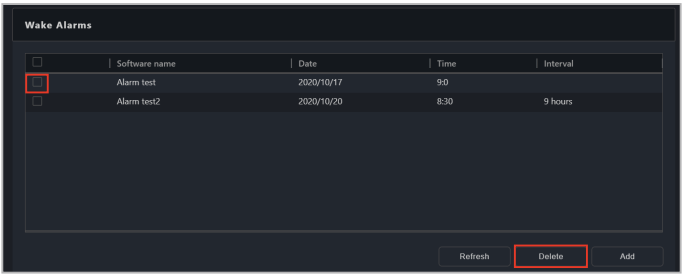


3. The newly added wake alarm will be displayed in the Wake Alarms list.



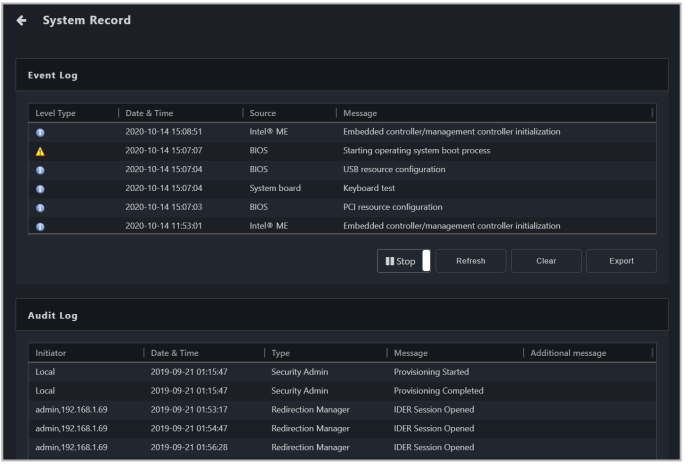
Removing a wake alarm

Select the wake alarm you would like to remove in the Wake Alarms list, then click **Delete**.



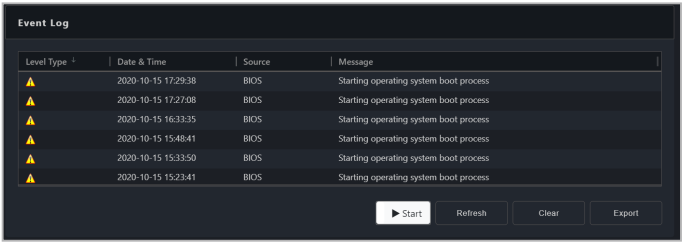
5.9.8 System Record

This item allows you to quickly detect the problems or issues on a client vPro device through the event log and alert records.



Event Log

View the client vPro device's event log records and analyze and detect device issues or problems.

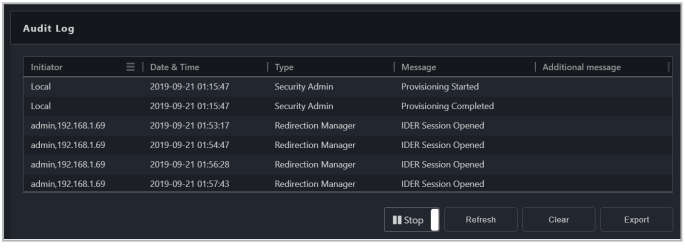


Start / Stop	Start or stop recording the event log.
Refresh	Refresh the event log to the latest updated state.
Clear	Clear the event log records.
Export	Export the event log records.

Audit Log

Records specified device system operations and unauthorized visits into the Audit Log. Through tracking the audit log, you can detect various sources of problems, security breaches, or illegal usage.

- Ensure to periodically export and clear the client vPro device's audit log.
- When you receive an alert about the storage space for the audit log, please export then clear the audit log. Once the audit log's storage space is full, you will not be able to execute any important or events defined as severe issues on the client device.

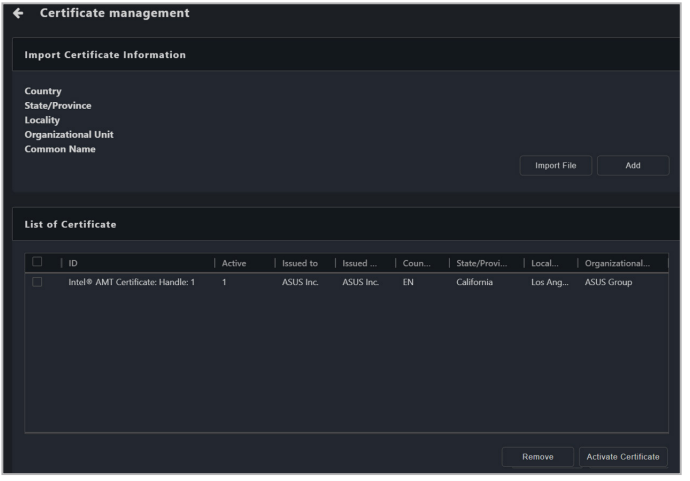


Start / Stop	Start or stop recording the audit log.
Refresh	Refresh the audit log to the latest updated state.
Clear	Clear the audit log records.
Export	Export the audit log records.

5.9.9 Certificate

This item allows you to import certificates for encryption and identification. This will ensure the connection between main server and client vPro device is safe and secure.

Please refer to the Certificate supplier information on the Intel website for details on obtaining certificates. Ensure to check the types supported by the certificate.



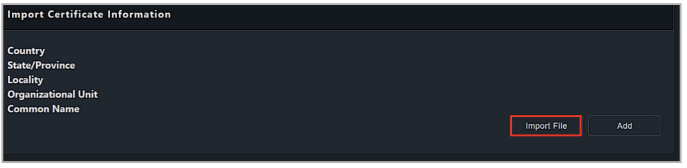
Import File	Import a certificate file.
Add	Add the imported certificate to the Certificates list.
Country	Import the certificate's country code.
State/Province	Import the certificate's state/province.
Locality	Import the certificate's locality.
Organization Unit	Import the certificate's organization unit.
Common Name	Import the certificate's common name.
Active	1 represents the certificate is active, and 0 represents the certificate is inactive in the **Active** column.
Remove	Removes selected certificate(s).
Activate Certificate	Activates selected certificate(s).

Adding and activating a certificate on single device

1. Click **Certificate** on the **Management Control Information** page of a device to add and activate a certificate on a single device.

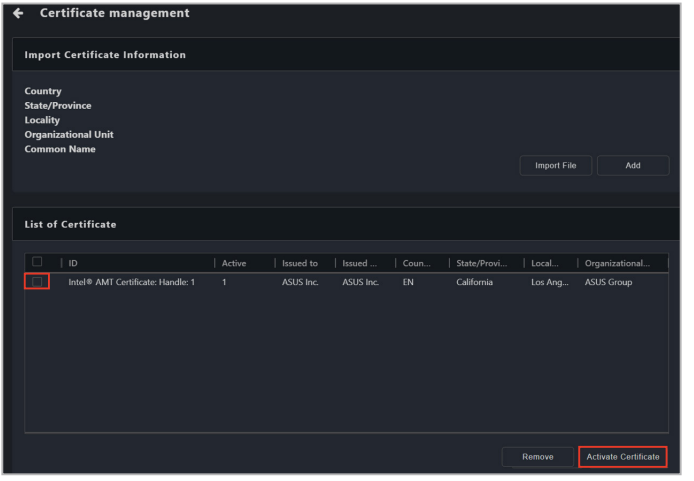
- Each client vPro device can only have 1 certificate active at a time, ensure to activate the certificate after importing the certificate.
- The **Remove** and **Activate Certificate** functions are only supported if you accessed the **Certificate** function through the **Management Control Information** page of a single device.

2. Click on **Import File** and select the certificate to import.



3. Check if the imported certificate information is correct in the **Import Certificate Information** block, then click **Add**.

4. The newly added certificate will show up in the **List of Certificate**. Select the certificate you wish to activate from the List of Certificate block, then click **Activate Certificate**.



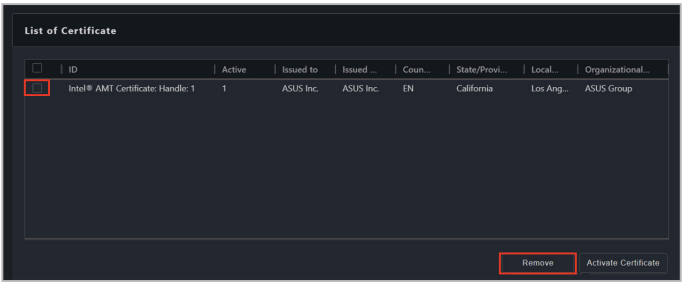
Removing a certificate on a single device

1. Click **Certificate** on the **Management Control Information** page of a device to add and activate a certificate on a single device.

The **Remove** and **Activate Certificate** functions are only supported if you accessed the **Certificate** function through the **Management Control Information** page of a single device.

2. Select the certificate(s) you wish to remove from the **List of Certificate** and click **Remove**.

You cannot delete an active certificate. Please select and activate a different inactive certificate first if you wish to delete a currently active certificate.

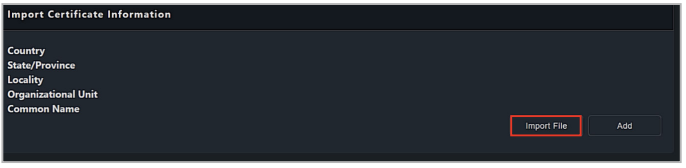


Adding and activating a certificate on multiple device

1. Select multiple devices on the main menu page, then select **OOB-Control** > **Certificate Management** from the **Select Function** drop down menu.

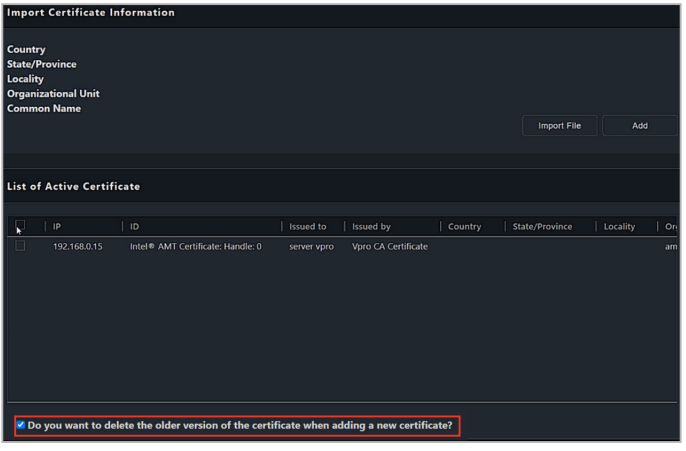
- Each client vPro device can only have 1 certificate active at a time, ensure to activate the certificate after importing the certificate.
- The **Remove** and **Activate Certificate** functions are only supported if you accessed the **Certificate** function through the **Management Control Information** page of a single device.

2. Click on **Import File** and select the certificate to import.



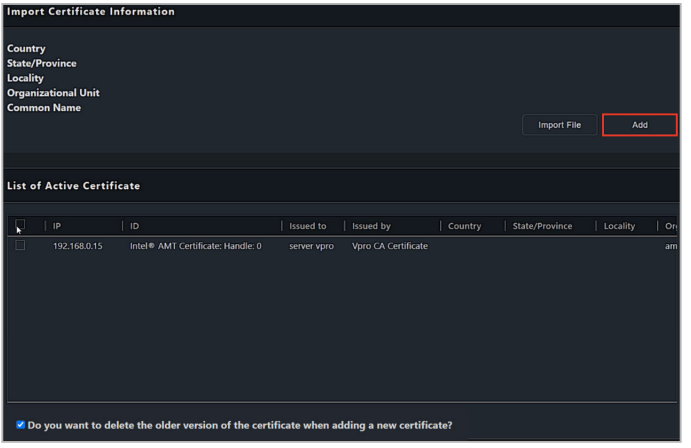
3. Check if the imported certificate information is correct in the **Import Certificate Information** block.
4. If required, check the **Do you want to delete the older version of the certificate when adding a new certificate?** option.

The **Do you want to delete the older version of the certificate when adding a new certificate?** option is only available if you accessed the **Certificate** function through the **OOB-Control** > **Certificate Management**.



5. Click on **Add** the newly added certificate will be displayed in the **List of Active Certificate** block.

- If you checked the **Do you want to delete the older version of the certificate when adding a new certificate?** option in step 4, the newly added certificate will replace the older version of the certificate.
- If you did not check the **Do you want to delete the older version of the certificate when adding a new certificate?** option, the previously active older version of the certificate will become inactive and not be displayed in the List of Active Certificate block. To delete the older inactive certificate, you will need to access the Certificate page by clicking **Certificate** on the **Management Control Information** page of a single device.

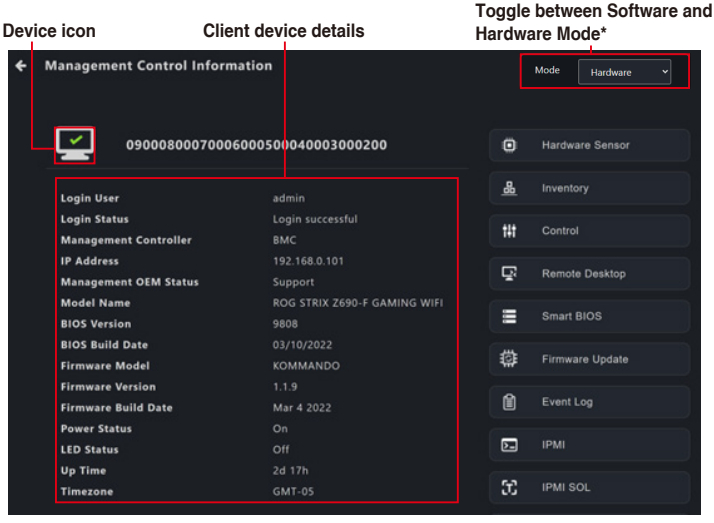


5.10 BMC Management Control Information

The **BMC Management Control Information** allows you to monitor hardware and asset information or manage functions such as KVM remote control, remote power control, Serial-over-LAN (SOL), media redirection, or IPMITool commands.

- The functions in this section are hardware controlled and values may differ with the software version. Please refer to Chapter 4 for more information on Software mode.
- Click the icon to expand or hide additional information.

- Before using BMC management control, please enable BMC functions in the BIOS of the client device, set the BMC username and password on the client device, and ensure that the connection to the BMC device and web console is stable.
- Certain functions such as hardware and asset information are available even when the client device is offline. For other functions, please wait for ASUS Control Center Express to finish connecting to the BMC remote management controller before selecting any functions to avoid unexpected behavior.
- Please ensure that the client device supports the BMC remote management controller and that all sensors are connected and working properly.

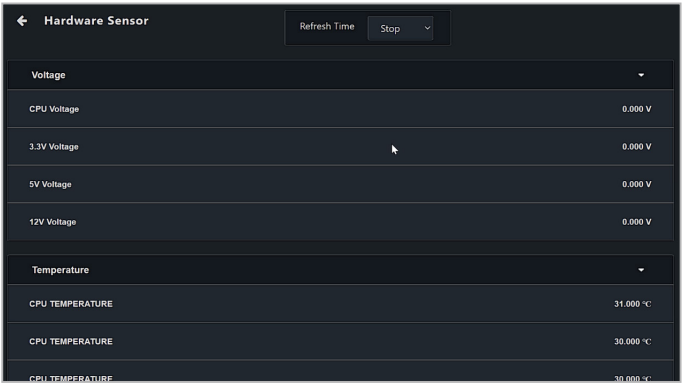


* **This item will not be available if you accessed the Management Control Information page through Management Control.**

Device icon	Displays the connection status of the client device's BMC remote management controller. The client device's web console can be opened by clicking on the device icon. To return to ASUS Control Center Express, click **Sign Out** on the left sidebar of the web console.
Login user	Displays the user account currently logged into the client device's BMC remote management controller. The login user can be switched.
Login status	Displays the current login status to the client device's BMC remote management controller.
Management controller	Displays the type of remote management controller of the client device.
IP address	Displays the IP address of the client device.
Management OEM status	Displays whether the client device supports OEM management functionality.
Model name	Displays the model name of the client device.
BIOS version	Displays the BIOS version of the client device.
BIOS build date	Displays the BIOS build date of the client device.
Firmware model	Displays the firmware model of the client device.
Firmware version	Displays the firmware version of the client device.
Firmware build date	Displays the firmware build date of the client device.
Power status	Displays the current power status of the client device.
LED status	Displays the status of the client device's LED indicators.
Uptime	Displays the uptime of the client device.
Timezone	Displays the timezone set for the BMC remote management controller.

5.10.1 Hardware Sensor

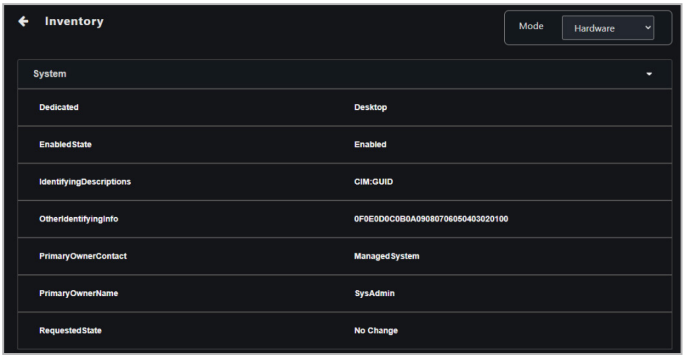
This item allows you to view the voltage, temperature, fan speed, and sensor information of the client BMC device.



Refresh Time	Set the refresh time interval for the Hardware Sensor.
Voltage	Displays the voltage of the device hardware.
Current	Displays the current of the device hardware.
Temperature	Displays the temperature of the device hardware.
Fan	Displays the fan rotation speed of the device hardware.
VERSION_ERR sensor	Displays the status of the VERSION_ERR sensor.
Watchdog2 sensor	Displays the status of the Watchdog2 sensor.

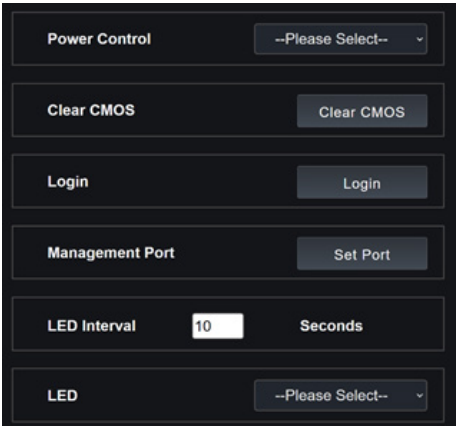
5.10.2 Inventory

This item allows you to view system, processor, memory, PCIE devices, PCIE functions, storage controller, and other hardware information.



5.10.3 Control

This item allows you to configure login credentials, ports, and LED indicators, clear CMOS, or remotely execute power control functions on a client device.



Power Control

Allows you to remotely execute power control functions on the client device through the BMC remote management controller, such as a system restart.

Power On (G0/S0)	Power on the client device through the BMC remote management controller.
Power Off - Soft (G2/S5)	Power off the client device through the BMC remote management controller.
Power Off - Hard (G3)	Force the client device to power off through the BMC remote management controller when the OS is unresponsive.
Power Cycle - Soft off (G2/S5)	Restart the client device after shutting down from the OS through the BMC remote management controller.
Power Cycle - Hard Off (G3)	Power off and restart the client device through the BMC remote management controller.

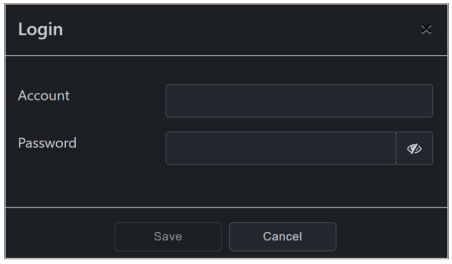
Clear CMOS

Allows you to clear the CMOS of the client device's BIOS, restoring it to factory settings. The progress of the operation can be checked in the mission center.

- The client device must be powered off before the CMOS can be cleared.
- Availability of this function may depend on BIOS and BMC firmware support.

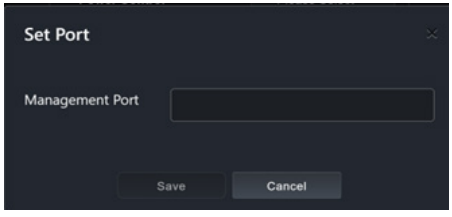
Login

Allows you to enter the account and password that ASUS Control Center Express will use to log into the client device's BMC remote management controller. After successfully logging in, the BMC remote management controller will automatically switch to the newly logged in account.



Sync OEM Port

Allows you to synchronize the management port used for the BMC web console.



- The management port must match the port used by the BMC web console or BMC functions will not be available.
- To set the default management port for all devices, click on **Settings** in the menu bar of the main control panel, then click **Options** > **General Configuration**, and scroll down to **BMC Account** > **Management Port**.

LED Interval

Allows you to set the state and blink interval of the client device's LED indicator.

LED On	The client device's LED indicator will turn on.
LED Off	The client device's LED indicator will blink on and off.
LED Interval	The client device's LED indicator will turn on for the specified interval, then return to the "off" state and blink on and off.

5.10.4 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. 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.

Video	**Pause Video**	Pauses Console Redirection
	Resume Video	Resumes Console Redirection when the session is paused.
	Refresh Video	Updates the display shown in the Console Redirection window.
	Display On	Turns on the display of the client device
	Display Off	Turns off the display of the client device
	Capture Screen	Captures a screenshot of the Console Redirection screen.
Mouse	**Show Client Cursor**	Shows or hides the local mouse cursor on the client device
	Mouse Mode	Switches between Absolute, Relative, and Other mouse modes
Options	**Zoom**	Adjusts the zoom of the Console Redirection screen
	Block Privilege Request	Sets partial or no permissions for privilege requests
	Bandwidth	Adjusts the bandwidth used for Console Redirection
	Compression Mode	Sets the compression mode
	DCT Quantization	Adjusts the image quality for Console Redirection between 0 (best quality) to 7 (best performance)
Keyboard		Switches between U.S., German, and Japanese keyboard layouts
Send keys	**Hold Down**	Holds down the selected key on the client device
	Press and Release	Presses and releases the selected key on the client device
Hot Keys	**Add Hot Keys**	Creates a new hotkey. Click on **Add Hot Keys** > **Add** and place the cursor in the text box, then press then release the key combination to define a macro.
Video Record	**Record Video**	Starts recording the Console Redirection screen.
	Stop Recording	Stops recording the Console Redirection screen
	Record Settings	Configures the video recording settings

(continued on the next page)

Power	Remotely executes power control functions
Active Users	Shows the currently active users on the server.
Help	Displays additional information on H5Viewer
Browse File	Click this button to add or modify CD media such as a physical DVD/CD-ROM drive and CD image types such as *.iso*, then click **Start Media** to start or stop the redirection.
Start Media	Starts or stops redirection of the media file.

5.10.5 Smart BIOS

This item allows you to update the BIOS of a device by uploading a BIOS file manually or from the BIOS Cache if the device cannot be powered on to perform a BIOS update or repair. You can also back up or restore the BIOS user profile and configuration settings.

- Availability of this function may depend on BIOS and BMC firmware support.
- The client device will begin updating the BIOS after shutting down. The update process may take a while, please wait for the update to be finished. Once the BIOS flash is finished the client device will restart.

DO NOT disconnect the power supply during the BIOS flash.

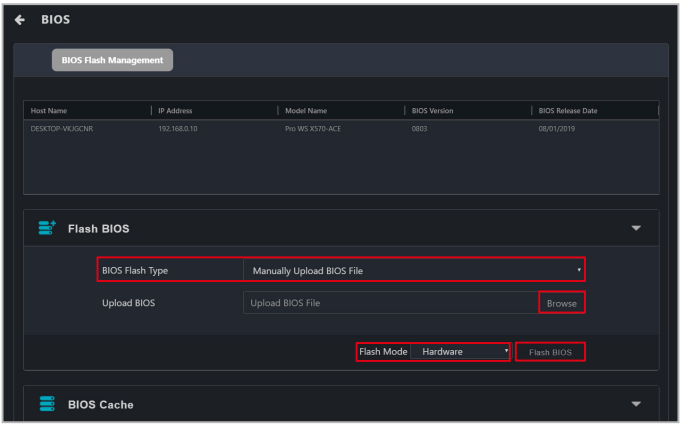
Flashing BIOS by manually uploading a BIOS file

Manually upload a BIOS file to flash the BIOS of the client device.

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**

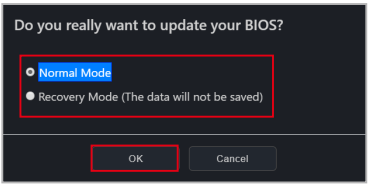
3. Click on **Flash BIOS**.

Flash Mode will default 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. Some configuration data will be deleted. Please contact an ASUS service center for assistance after the **Recovery Mode** BIOS flash is completed.

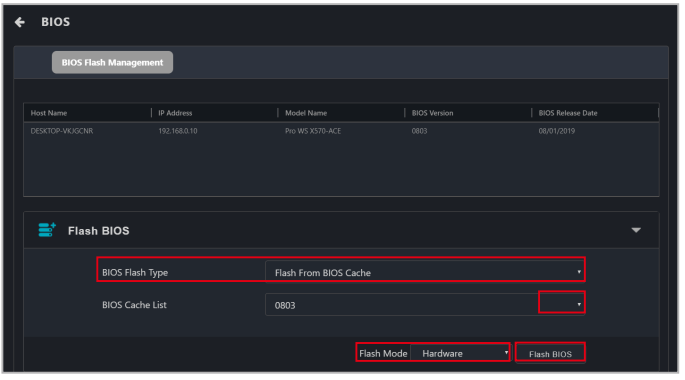


Flashing BIOS from the BIOS cache

You can select a BIOS file from the BIOS cache.

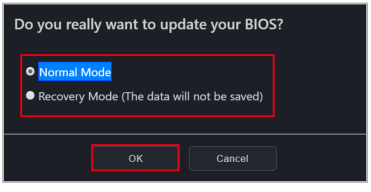
1. Select **Flash from BIOS Cache** in the **BIOS Flash Type** field.
2. Select a BIOS file from the **BIOS Cache List** drop down menu.
3. Click on **Flash BIOS**.

Flash Mode will default to **Hardware Mode**.

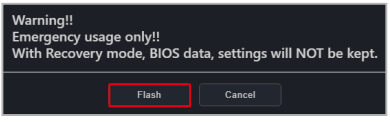


4. Select if you wish to perform a **Normal Mode** BIOS flash or if you wish to do a **Recovery Mode** BIOS flash, then click **OK**.

Performing a **Recovery Mode** BIOS Flash will reset all BIOS configurations. BIOS data and configuration settings will also be deleted. Please contact an ASUS service center for assistance after the **Recovery Mode** BIOS flash is completed.

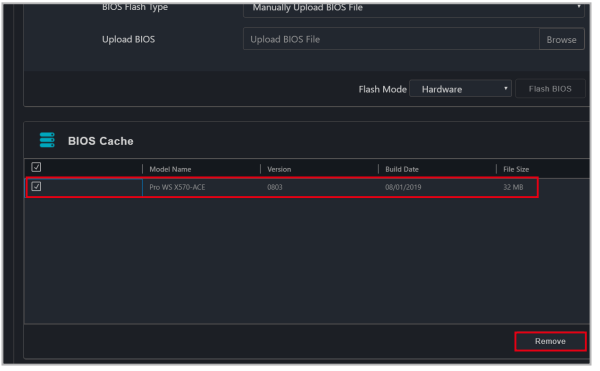


5. (Optional) If you selected **Recovery Mode**, you will be prompted with a warning message, as **Recovery Mode** will remove all previous BIOS data and configurations. Click **Flash** to continue with using **Recovery Mode**.



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**.



Downloading BIOS user profile data

- Availability of this function may depend on BIOS, IPMI, and BMC firmware support.
- Ensure that the client device has finished booting into the operating system before downloading BIOS user profile data.
- If a firmware update was recently completed, restart the client device before downloading BIOS user profile data.
- User profile data saved using BMC is not compatible with user profile configuration files created locally by the BIOS on client devices.

1. Select a client device from the device list.
2. Fill in the **Download path** and **Download file name** fields.
3. Click **Download** to download the BIOS user profile data (.CMO).

Uploading BIOS user profile data

- After BIOS user profile data is uploaded, the client device(s) will automatically update BIOS settings upon the next startup. DO NOT disconnect the power supply or turn off the client device(s) during the BIOS settings update.
- To cancel a BIOS user profile data update, do not restart the client device and click **Cancel**.
- The BIOS version of the saved BIOS user profile data must match the BIOS version of the client device.
- It is not recommended to start BIOS OOB update and BIOS user profile update tasks simultaneously.
- Ensure that the current BIOS user profile data is backed up before uploading any BIOS user profile data.

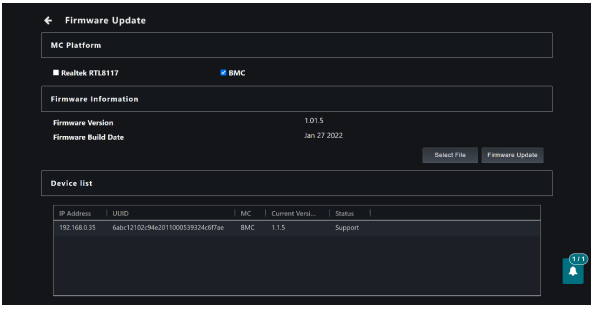
1. Fill in the **Upload file path** and **User profile password** (optional) fields.
2. Click **Upload** to upload to a single client device, or **Upload all devices** to upload to multiple client devices.
3. Once the upload is completed, restart the client device(s).

5.10.6 Firmware Update

This item allows you to update the firmware of the BMC remote management controller, and also displays the results of the firmware update.

Uploading and updating firmware

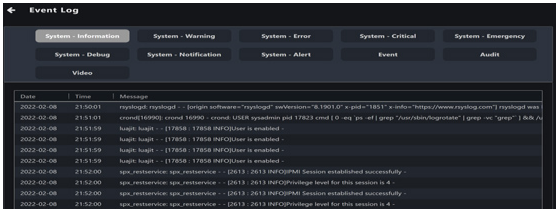
1. Tick the checkbox for **BMC** under **MC Platform**
2. Click on **Select File**, then select your firmware file (.img) and click **Open**.
2. Click on **Firmware Update**, then wait for the update to be completed.
3. You can check the results of the firmware update in the Mission Center.
4. If the client device's firmware was updated while it was powered on, please reboot the client device after the firmware has been successfully updated.



5.10.7 Event Log

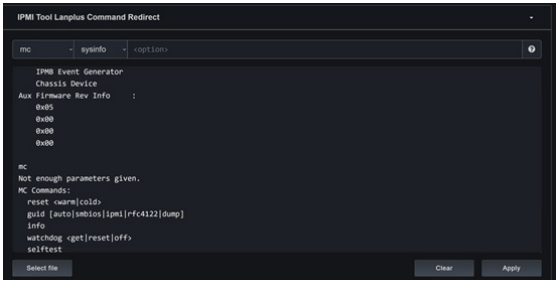
This item allows you to view the event log of the last time the client device was powered on, giving you more information to analyze the cause of the problem or issue.

Please use the Notification Rule Management menu to manage which client devices, utilization status messages, hardware sensor events, or management controller alarms are shown in the Event Log. To set up notification rules, please click on located at the top right menu bar of the Dashboard, then select **Options** > **Rule Management**. For more information, please refer to **8.1.2 Rule Management**.



5.10.8 IPMI

IPMI Tool Lanplus Command Redirect allows remote execution of commands to configure settings or view information on the client device.



To execute commands on multiple client devices, please return to the main control panel and select the devices you wish to send commands to, then click **Select Function** > **OOB - Control** > **IPMI** > **IPMI Tool Lanplus Command Redirect**

In order to write FRU data, please unlock the FRU by executing the following command:

`raw 0x30 0x17 0x01`

Once the FRU is unlocked, execute the following command to write FRU data:

`fru write <fru id> <file>`

1. Select the desired command from the drop down menu.
2. Input any required and/or optional command parameters into the input box.

- The command parameters will be displayed in the input box.
- Click on **?** to view additional information about the selected command.

3. (Optional) Click **Select File** to upload a .bin file.
4. Click **Apply** to execute the command. The progress of the command can be viewed in the mission center. Results of completed commands will be shown in the IPMI Tool window.

If the command was executed on multiple devices, you can click on the name of a device in the Device List to view the result of the completed command.

5. (Optional) Click **Clear** to clear the IPMI Tool window.

5.10.9 IPMI Serial-over-LAN (SOL)

This item allows you to access the serial console over Serial-over-LAN (SOL).

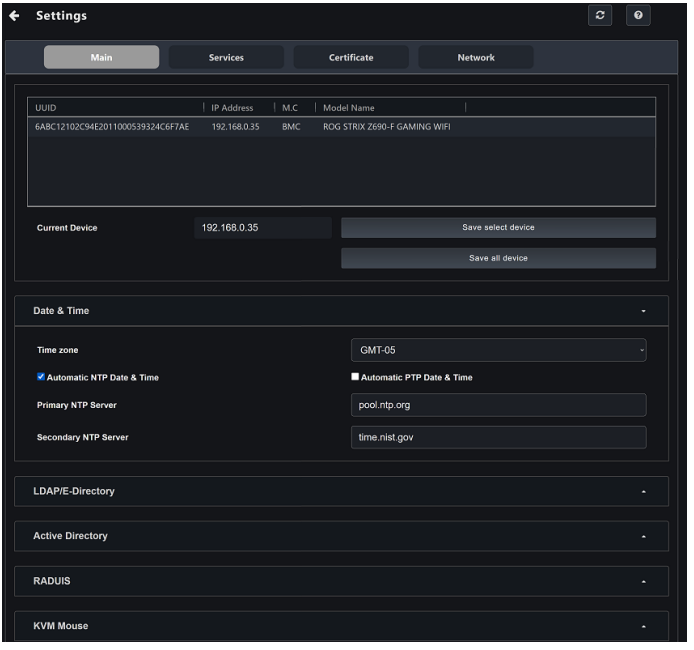
1. Click **Start** to start Serial-over-LAN via BMC on the client device.
2. Click **Stop** to end Serial-over-LAN via BMC on the client device.

5.10.10 Settings

This item allows you to configure BMC related settings.

1. After settings are changed, click on **Save select device** to update the selected client device with the new settings or click on **Save all devices** to update all BMC devices with the new settings.
2. Click on the icon to confirm that the changes have been committed. The status of the operation can also be viewed in the Mission Center.

To show additional information about the settings, click the icon.



Date & Time

This page allows you to set the date and time on the BMC.

Select Time Zone	Select the time zone from the **Select Time Zone** drop down menu.
Automatic NTP Date & Time	Enable or disable automatic time and date synchronization with the NTP server.
Primary NTP Server*	Allocate the primary NTP server to automatically update the date and time.
Secondary NTP Server*	Allocate the secondary NTP server to automatically update the date and time.
Automatic PTP Date & Time	Enable or disable the PTP server to automatically update the date and time.
PTP Interface*	Set the PTP server interface.
PTP Preset*	Set the PTP preset type to SlaveOnly or MasterSlave modes (default: SlaveOnly).
PTP Transport*	Set the PTP transport type to IPv4 or Ethernet modes (default: IPv4).
PTP Ipmode*	Set the PTP Ipmode to Unicast or Multicast modes.
PTP Unicast IP*	Set the Master IP address when PTP is in Unicast mode.
PTP Delay Mechanism*	Set the PTP delay mechanism to E2E or P2P (default: E2E).
PTP Inbound Latency*	Set the PTP inbound latency in nanoseconds (default: 0ns).
PTP Outbound Latency*	Set the PTP outbound latency in nanoseconds (default: 0ns).
PTP Priority1*	Set the priority of the PTP clock between 0 and 128 for the Master and 255 for the Slave.
PTP Max Master Capacity*	Set the max master capacity of the PTP clock (default: 5).
PTP Log Request Delay*	Set the PTP log request delay (default: 1).
Panic Mode*	Set PTP clock to not reset if jump is more than 1 second (default: unchecked).

Settings marked with an asterisk (*) are only available when the checkbox for **Automatic NTP Date & Time** or **Automatic PTP Date & Time** is selected.

LDAP/E-Directory

This item allows you to set the LDAP/E-directory Settings.

Enable LDAP/E-Directory Authentication	Enable or disable LDAP/E-Directory Authentication.
Encryption Type	Set the LDAP/E-Directory encryption type to No Encyption, SSL, or StartTLS.
Common Name Type	Set the Common Name Type to IP Address or FQDN.
Server Address	Set the LDAP/E-Directory server address.
Port	Enter LDAP/E-Directory port.
Bind DN	Set the Bind DN used to authenticate the client in bind operations.
Password	Set the password used to authenticate the client during bind operations.
Search Base	Set which part of the external directory tree is searched by the LDAP/E-directory server.
Attribute of User Login	Set the attribute used to identify the client.
CA Certificate File*	Select the trusted CA certificate file.
Certificate File*	Select the client certificate file.
Private Key*	Select the private key file.

Settings marked with an asterisk (*) are only available when the checkbox for **SSL** or **StartTLS** is selected.

Active Directory Settings

This item allows you to set the Active directory Settings.

Enable Active Directory Authentication	Enable or disable Active Directory Authentication.
SSL	Enable or disable SSL encryption.
Secret Username	Set the Active Directory server administrator username.
Secret Password	Set the Active Directory server administrator password.
User Domain Name	Set a domain name for the user.
Domain Controller Server Address 1-3	Enter the IP address of at least one Active Directory server.

RADIUS Settings

This item allows you to enable or disable RADIUS authentication and enter the required information to access the RADIUS server.

Enable RADIUS Authentication	Enable or disable RADIUS Authentication.
Server Address	Set the RADIUS server address
Port	Set the RADIUS server port.
Secret	Set the RADIUS server password.
Administrator*	Set the RADIUS administrator attribute.
Operator*	Set the RADIUS operator attribute.
User*	Set the RADIUS user attribute.
OEM Proprietary*	Set the RADIUS OEM proprietary attribute.
No Access*	Set the RADIUM no access attribute.

Advanced settings marked with an asterisk (*) should be set according to the vendor specific attributes for the RADIUS users on the server.

KVM Mouse Setting

This item allows you to set the mouse mode.

Relative Positioning (Linux)	Calculated relative mouse position displacement is sent to the server.
Absolute Positioning (Windows)	Absolute position of the local mouse is sent to the server. This option is recommended for Windows or later versions on Linux.
Other Mode (SLES-11 OS Installation)	Calculated displacement from the local mouse in the center position is sent to the server.

Log Settings

This item allows you to set the log policy for the event log.

Linear Storage Policy	Set the SEL Log Setting Policy to Linear Storage.
Circular Storage Policy	Set the SEL Log Setting Policy to Circular Storage.

Advanced Log Settings

This item allows you to set advanced log settings for the event log.

System Log	Enable **System Log** to view all system events. Entries can be filtered based on their classification levels.
Local Log	Check this item to save the logs locally on the BMC device.
Remote Log	Check this item to save the logs in a remote machine.
Port Type	Set the port type to TCP or UDP.
File Size	Set the size of the local log file in bytes between 3 and 65535.
Rotate Count	When logged information exceeds the specified file size, old log information will automatically be rotated to backup based on the rotate count value. • Rotate count value must be 0 or 1. • If the rotate count is 0, the old log information will be permanently cleared each time.
Remote Log Server	Set the remote server address for the system log.
Remote Server Port	Set the port number for the system log.
Enable Audit Log	Enable this item to view all audit events for the client device.

Media Redirection Settings

This item allows you to set the media redirection settings.

- Availability of this function may depend on BMC support.
- Settings marked with an asterisk (*) are only available when the checkbox for **CIFS** is selected.

Remote Media Support		Enable or disable remote media support. When enabled, CD/DVD and Hard disk remote media types will appear. Users can configure different settings for the different remote media types. Configuration options will be displayed for each media type, or the same options can be applied to both.
Mount CD/ DVD	**Server Address for CD/DVD Images**	Enter the address of the server where the remote videos are stored.
	Path In Server	Enter the path of the media on the remote server.
	Share Type for CD/ DVD	Set the share type to NFS or Samba (CIFS).
	Domain Name*	Enter the domain name of the remote server.
	Username*	Enter the username for the remote server.
	Password*	Enter the password for the remote server.
	Same Settings for Harddisk Images	Apply the server information entered for **Mount CD/ DVD** to **Mount Harddisk**.
Mount Harddisk	**Server Address for CD/DVD Images**	Enter the address of the server where the remote videos are stored.
	Path In Server	Enter the path of the remote media on the server.
	Share Type for CD/ DVD	Set the share type to NFS or Samba (CIFS).
	Domain Name*	(Optional) Enter the domain name of the remote media.
	Username*	Enter the username
	Password*	Enter the password

VMedia Instance Settings

This item allows you to configure settings for the redirection of virtual media to supported CD/DVD and/or hard disk devices.

Availability of certain functions depends on client device BMC support.

CD/DVD device instances	Select the number of CD/DVD devices to be supported for Virtual Media redirection.
Hard disk instances	Select the number of Hard disk devices to be supported for Virtual Media redirection.
Remote KVM CD/DVD device instances	Select the number of Remote KVM CD/DVD devices to be supported for Virtual Media redirection.
Remote KVM hard disk instances	Select the number of Remote KVM hard disk devices to be supported for Virtual Media redirection.
Emulate SD Media as USB disk on the host	Enable emulation of SD Media as an USB disk on the host.

Media Remote Session Settings

This item allows you to configure settings for the remote session.

KVM Single Port Application	Allows Single Port Application support in BMC.
Keyboard Language	Select the keyboard language.
Virtual Media Attach Mode	Select the Virtual Media Attach Mode.
Retry Count	Set the number of times to retry when a KVM failure occurs between 1 to 20.
Retry Time Interval (Seconds)	Set the number of seconds to wait for subsequent retries between 5 to 30 seconds.
Server Monitor OFF Features Status	Enable or disable the Server Monitor OFF feature.
Automatically OFF Server Monitor when KVM Launches	Enable to automatically turn off the monitor of the client device when KVM launches

PAM Order Settings

This item allows you to configure the PAM order for user authentication into the BMC. The list of PAM modules supported by the BMC is displayed. Drag and drop the PAM modules to reorganize their positions in the sequence.

SMTP Settings

This item allows you to configure the SMTP mail server.

LAN Interface	Select the LAN interface to be configured.
Sender Email ID	Enter a valid **Sender Email ID** on the SMTP Server. Maximum allowed size for Email ID is 64 bytes, which includes username and domain name.
Primary/Secondary SMTP Support*	Enable or disable SMTP support for the BMC.
Primary/Secondary Server Name*	Enter the name of the SMTP server for reference purposes.
Primary/Secondary Server IP*	Enter the server address for the SMTP server.
Primary/Secondary SMTP Port*	Enter the SMTP port.
Primary/Secondary Secure SMTP Port*	Enter the SMTP secure port.
Primary/Secondary SMTP Authentication*	Enable or disable SMTP authentication.
Primary/Secondary Username*	Enter the username for the SMTP user account.
Primary/Secondary Password*	Enter the password for the SMTP user account.
Primary/Secondary SMTP SSLTLS Enable*	Enable or disable the SMTP SSLTLS protocol.
Primary/Secondary SMTP STARTTLS Enable*	Enable or disable the SMTP STARTTLS protocol.

Settings marked with an asterisk (*) are only available when the checkbox for **Primary SMTP Support** or **Secondary SMTP Support** is selected.

Firewall IP Address Rules

This item allows you to configure the firewall IP address rules.

IP Single (or) Range Start	Enter a single IP address or the start of an IP address range.
IP Range End	(Optional) Enter the end of an IP address range.
Enable Timeout	Enable or disable timeout.
Start Date*	Set the date when the firewall rule comes into effect.
Start Time*	Set the time when the firewall rule comes into effect.
End Date*	Set the date when the firewall rule expires.
End Time*	Set the time when the firewall rule expires.
Rule	Allow or block the specified IP address or range.

Settings marked with an asterisk (*) are only available when the checkbox for **Enable Timeout** is selected.

Firewall IP Address Exist Rules

This item shows existing firewall rules. To remove an existing rule, click the **X** in the corresponding row.

Video Trigger Settings

This item allows you to configure the events that will trigger the auto video recording function of the KVM server.

Critical Events (Temperature/Voltage)	Enable or disable a trigger for the auto video recording function.
Non-critical Events (Temperature/Voltage)	
Non-recoverable Events (Temperature/Voltage)	
Fan State Changed Events	
Watchdog Timer Events	
Chassis Power On Events	
Chassis Power Off Events	
Chassis Reset Events	
LPC Reset Events	
Date and Time Events	
Pre-Event Video Recordings	Enable Pre-Event Video Recordings and set recording to Pre-Crash or Pre-Reset.

Video Remote Storage Settings

This item allows you to configure video remote storage settings.

Record Video to Remote Server	Enable or disable Remote Video support.
Maximum Dumps	Set the maximum dump limit between 1 and 100.
Maximum Duration	Set the maximum duration between 1 and 3600 seconds.
Maximum Size	Set the maximum size of dumps between 1 and 500 MB.
Server Address	Set the IP address of the remote server where the remote videos will be stored.
Path in Server	Set the path of the media on the remote server.
Share Type	Set the share type to NFS or Samba (CIFS).
Domain Name*	Enter the domain name of the remote server.
Username*	Enter the username for the remote server.
Password*	Enter the password for the remote server.

Settings marked with an asterisk (*) are only available when the checkbox for **CIFS** is selected.

Pre-Event Video Recording Settings

This item allows you to configure Pre-Event video recording settings.

To enable Pre-Event Video Recording, please go to the **Video Trigger Settings** section.

Video Quality	Select the video quality.
Compression Mode	Select the compression mode.
Frames Per Second	Select the frames per second (FPS).
Video Duration	Select the duration of the video recording in seconds.

SOL Trigger Settings

This item allows you to configure the events that will trigger Serial-over-LAN (SOL) video recording.

Critical Events (Temperature/Voltage)	Enable or disable a trigger for the auto video recording function.
Non-critical Events (Temperature/Voltage)	
Non-recoverable Events (Temperature/Voltage)	
Fan State Changed Events	
Watchdog Timer Events	
Chassis Power On Events	
Chassis Power Off Events	
Chassis Reset Events	
LPC Reset Events	
Date and Time Events	

SOL Remote Video Settings

This item allows you to configure Serial-over-LAN (SOL) video recording settings.

Log Size	Set the preferred size of the log file in KB up to 128KB.
Log File Count	Set the number of log files between 0 and 1.
Record Video to Remote Server	Enable or disable storing recorded videos on a remote server instead of on the BMC.
Server Address*	Set the IP address of the remote server where the remote videos will be stored.
Path in Server*	Set the path of the media on the remote server.
Share Type*	Set the share type to NFS or Samba (CIFS).
Domain Name*	Enter the domain name of the remote server.
Username*	Enter the username for the remote server.
Password*	Enter the password for the remote server.

Settings marked with an asterisk (*) are only available when the checkbox for **Record Video to Remote Server** and/or **CIFS** is selected.

SOL Recorded Video

This item shows existing Serial-over-LAN (SOL) recorded videos. Click on a video to download and save it. To delete a video, click the **X** in the corresponding row.

SOL Configuration

This item allows you to edit SOL configuration options.

Availability of this function depends on client device BMC support.

Volatile Bit Rate	Set the volatile bit rate.
Non-volatile Bit Rate	Set the non-volatile bit rate.

Fan Mode

This item allows you to view the current fan mode and switch between different fan modes.

Availability of certain fan modes depends on client device BMC support.

Generic Mode	Set the fan of the client device to generic mode.
Full Speed Mode	Set the fan of the client device to full speed mode.
Silent Mode	Set the fan of the client device to silent mode.
Turbo Mode	Set the fan of the client device to turbo mode.

Fan Customized

This item allows you to specify a custom fan curve.

Availability of this function depends on client device BMC support.

Fan Temperature Source

This item allows you to select a temperature sensor to control fan speed.

- If temperature information is unavailable, the CPU temperature will be used. If the CPU temperature is also unavailable, the fan speed will default to 60%.
- To use CHA_FAN sensor and control functions, please ensure that the fans are connected to the corresponding fan headers and that the 6-pin PSU connector is connected to a power supply.
- Fan speed control support depends on BMC, motherboard, BIOS, and firmware support.

PSU Redundancy

This item allows you to configure PSU redundancy settings, allowing you to focus system power consumption on one PSU device for improved power efficiency.

PSU Redundancy	Enable or disable PSU Redundancy

To use PSU Redundancy, the PSU PM_BUS header and SMART_PSU switch jumper must be activated.

Service Web Configuration

This item allows you to configure the Web service.

Active	Enable or disable the Web service.
Interface Name	Select the interface used for the Web service.
Secure Port	Enter the secure port used for the Web service. (default: 443)
Timeout	Configure the session timeout value in multiples of 60 seconds between 300 to 1800 seconds
Maximum Sessions	Shows the maximum number of allowed sessions.

Service KVM Configuration

This item allows you to configure the KVM service.

Active	Enable or disable the KVM service.
Interface Name	Select the interface used for the KVM service.
Secure Port	Enter the secure port used for the KVM service. (default: 443)
Timeout	Configure the session timeout value in multiples of 60 seconds between 300 to 1800 seconds
Maximum Sessions	Shows the maximum number of allowed sessions.

Service CD-Media Configuration

This item allows you to configure the CD-Media service.

Active	Enable or disable the CD-Media service.
Interface Name	Select the interface used for the CD-Media service.
Secure Port	Enter the secure port used for the CD-Media service. (default: 443)
Maximum Sessions	Shows the maximum number of allowed sessions.

Service HD-Media Configuration

This item allows you to configure the HD-Media service.

Active	Enable or disable the HD-Media service.
Interface Name	Select the interface used for the HD-Media service.
Secure Port	Enter the secure port used for the HD-Media service. (default: 443)
Maximum Sessions	Shows the maximum number of allowed sessions.

Service SSH Configuration

This item allows you to configure the SSH service.

Active	Enable or disable the SSH service.
Interface Name	Select the interface used for the SSH service.
Secure Port	Enter the secure port used for the SSH service. (default: 22)
Timeout	Configure the session timeout value in multiples of 60 seconds between 60 to 1800 seconds
Maximum Sessions	Shows the maximum number of allowed sessions.

SSL Generate Certificate

This item will allow you to generate an SSL certificate. Click the **Generate** checkbox to show the SSL Generate Certificate section.

Common Name (CN)	Set the common name of the generated certificate.
Organization (O)	Set the organization of the generated certificate.
Organization Unit (OI)	Set the organization unit of the generated certificate.
City or Locality (L)	Set the city or locality of the organization.
State or Province (ST)	Set the state or province of the organization.
Country (C)	Set the country of the organization.
Email Address	Set the email address of the organization.
Valid For	Set the requested validity period of the generated certificate between 1 and 3650 days.
Key Length	Set the key length in bits of the generated certificate.

SSL Upload Certificate

This item will allow you to upload an SSL certificate. Click the **Upload** checkbox to show the SSL Upload Certificate section.

Current Certificate	Shows the date and time of the current certificate.
New Certificate	Select a new certificate file to upload.
Current Private Key	Shows the date and time of the current private key.
New Private Key	Select a new private key file to upload.

Current Certificate Information

This item will allow you to view information about the current certificate.

Network IP Configuration

This item will allow you to manage LAN support for the interface.

Enable LAN	Enable or disable LAN support for the selected interface.
LAN Interface	Select the interface to be configured.
MAC Address	Shows the MAC address of the selected interface.
Enable IPv4	Enable or disable IPv4 for the selected interface.
Enable IPv4 DHCP	Enable or disable dynamic configuration of IPv4 addresses using Dynamic Host Configuration Protocol (DHCP)
IPv4 Address*	Set the static IPv4 address.

(continued on the next page)

IPv4 Subnet*	Set the static subnet mask.
IPv4 Gateway*	Set the static default gateway.
Enable IPv6	Enable or disable IPv6 for the selected interface.
Enable IPv6 DHCP	Enable or disable dynamic configuration of IPv6 addresses using Dynamic Host Configuration Protocol (DHCP)
IPv6 Index*	Set the IPv6 Index.
IPv6 Address*	Set the static IPv6 Address.
Subnet Prefix Length*	Set the IPv6 Subnet Prefix length
IPv6 Gateway*	Set the IPv6 Gateway
Enable VLAN	Enable or disable VLAN support for the selected interface.
VLAN ID	Set the VLAN ID.
VLAN Priority	Set the VLAN priority.

Settings marked with an asterisk (*) are only available when **IPv4/IPv6** is enabled and **DHCP** is disabled.

Network DNS Configuration

This item will allow you manage DNS settings.

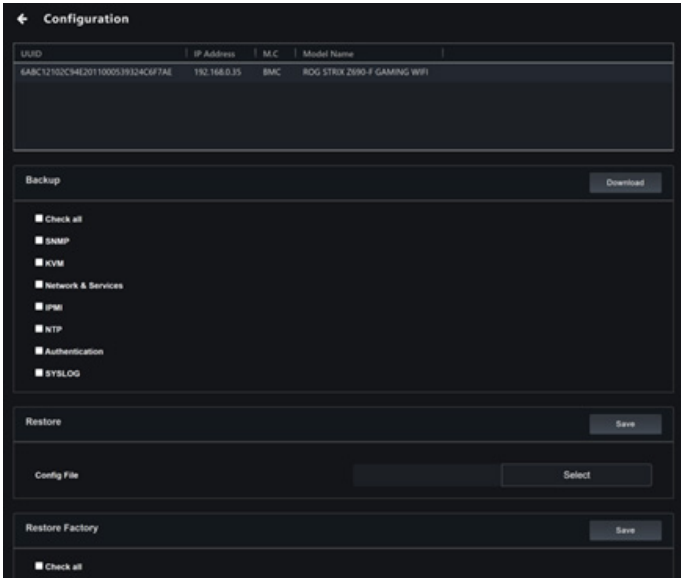
DNS Enabled	Enable or disable the DNS service.
mDNS Enabled	Enable or disable Multicast DNS.
Host Name Setting	Set Host Name configuration to Auto or Manual.
Host Name	Set the Host Name if it is not configured automatically.
BMC Interface	Shows the BMC Interface name.
Register BMC	Enable or disable BMC registration.
Registration Method	Select from the following registration methods: - **Nsupdate**: Register with the DNS server using the nsupdate application. - **DHCP Client FQDN**: Register with the DNS server using DHCP option 81. - **Hostname**: Register with the DNS server using DHCP option 12.
TSIG Authentication Enabled	Enable or disable TSIG authentication
Current TSIG Private File Info	Shows the date and time of the current TSIG Private File if TSIG Authentication is enabled.
New TSIG Private File	Select a new TSIG Private File to upload if TSIG Authentication is enabled.

(continued on the next page)

Domain Setting	Set Domain configuration to Auto or Manual.
Domain Interface	Set the domain interface if the domain is configured automatically.
Domain Name	Set the domain name if the domain is configured manually.
Domain Name Server Setting	Set Domain Name Server configuration to Auto or Manual.
IP Priority	Set the IP priority if the Domain Name Server is configured automatically.
DNS Server 1-3	Set the DNS servers if the Domain Name Server is configured manually.

5.10.11 Configuration

This item allows you to backup, restore, or factory reset configuration settings.



Backup

1. To backup configuration settings, select the items you wish to backup by ticking the corresponding checkbox or select **Check All** to select all items at once.
2. Click **Download** to save the backup of the configuration settings to your backup location.

Restore

1. To restore the configuration settings from backup, click **Select** and choose a previously made backup file.
2. Click **Save** to restore the configuration settings from the backup file to the client device.

Restore Factory

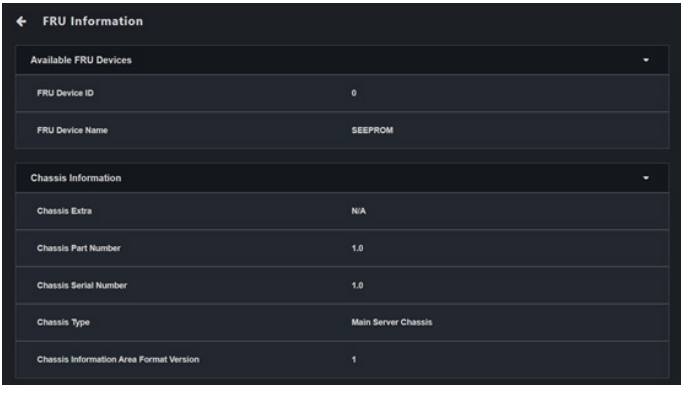
1. To restore configuration settings to factory defaults, select the items you wish to reset by ticking the corresponding checkbox(es) or select **Check All** to select all items at once.
2. Click **Download** to save the backup of the configuration settings to your backup location.

Restoring settings to factory defaults cannot be undone. It is recommended that you create a backup of the current settings before restoring to factory defaults.

5.10.12 FRU Information

This item shows information about the BMC's FRU (field replaceable unit) device, including basic information, chassis information, board information, and production information.

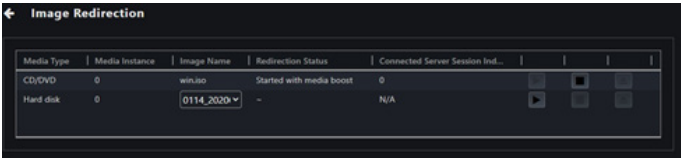
In order to write FRU data, please refer to **5.10.8 IPMI**.



5.10.13 Image Redirection

This item allows you to select images to host as virtual media through BMC. You can start view, clear, and start redirection of available images.

- Availability of this function may depend on BMC support.
- Administrator privileges are required for image redirection.
- To configure the image, you need to enable **Remote Media Support** in **Settings** > **Media Redirection** > **General Settings**.
- Supported CD/DVD formats: ISO9660, UDF(v1.02~v2.60)
- Supported CD/DVD media file types: (*.iso), (*.nrg)
- Supported HDD media file types: (*.img), (*.ima)
- Maximum media file size: 5GB



Redirecting local media

Start redirection	Click the Play button to redirect the selected image
Stop redirection	Click the Stop button to stop the remote image redirection.
Upload image	Click the Upload button to upload an image to the client device. • BMC functions will be unavailable until the upload is completed. Upload time will depend on network conditions and file size. • If an ongoing upload is cancelled, BMC functions will be temporarily unavailable while the system rolls back changes. If this fails to complete in a timely matter, try restarting the client device.
Clear	Click the Clear button to clear the selected image from the BMC.

Redirecting remote media

Start redirection	Click the Play button to redirect the selected image
Stop redirection	Click the Stop button to stop the remote image redirection.
Clear	Click the Clear button to clear the selected image from the BMC.

5.10.14 Platform Event Filters

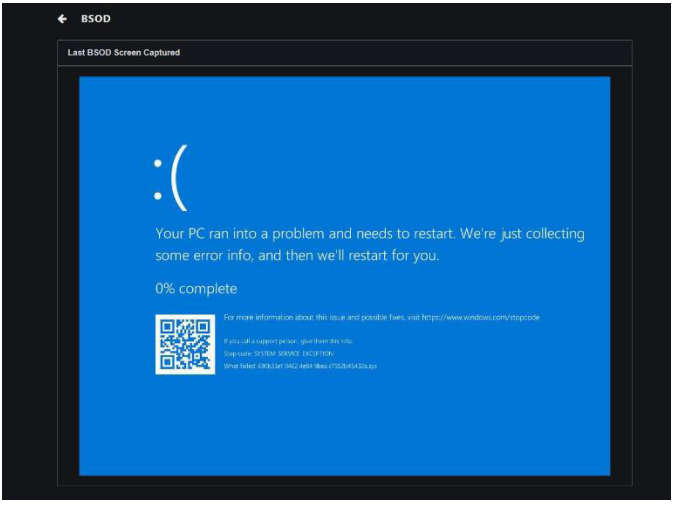
This item allows you to connect to the BMC web console of the client device to manage platform event filter settings, alert policies, and LAN destinations.

To return to ASUS Control Center Express, click **Sign Out** on the left sidebar of the web console.

5.10.15 BSOD Capture

This item shows the last BSOD (Blue Screen of Death) captured by the BMC device to aid in investigating and diagnosing system abnormalities.

To enable BSOD Capture, the KVM service must be enabled through **Settings > Services > KVM**.



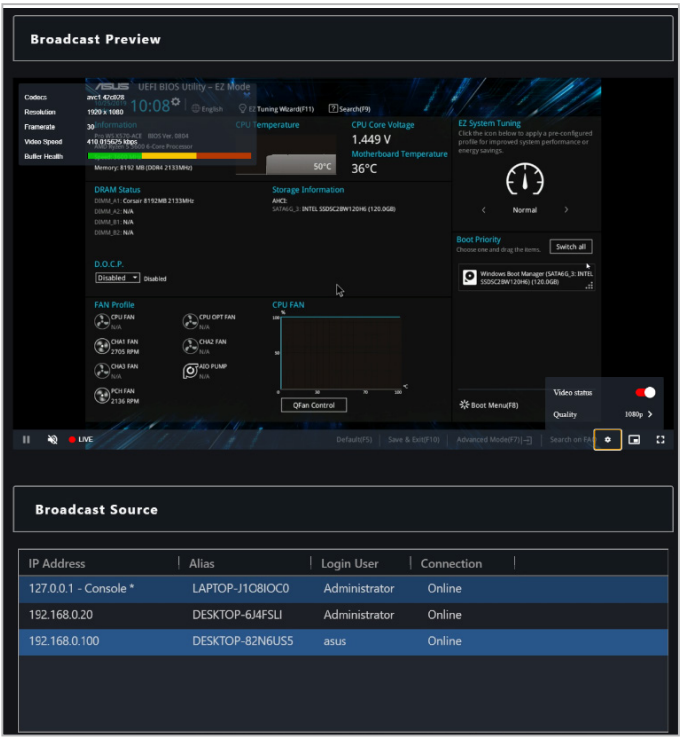
5.10.16 Error Codes

0x83100002	Client device does not support BMC.
0x83100003	Command invalid.
0x83100025	Client device must be powered off to clear CMOS.
0x83100026	Check if the SPI connector is connected to the IPMI TPM connector on the motherboard.
0x83100033	Could not connect to the BMC web interface.
0x83100034	BMC login credentials incorrect.
0x83100006	Could not synchronize BMC functions. Check network connectivity and try again. If this issue persists, shut down the client device, disconnect the power, then restart the client device.
0x831F4077	Could not log into BMC on the client device. Check if BMC is working correctly on the client device or reenter BMC login credentials and try again. If this issue persists, shut down the client device, disconnect the power, then restart the client device.
0x831F4038	No response received from BMC on the client device. If this issue persists, shut down the client device, disconnect the power, then restart the client device.

5.11 Screen Broadcast

Screen broadcast allows either one-to-one or one-to-many access to the client device's screen, video camera devices, and broadcast a selected clip, and also allow you to select the resolution, video quality, and audio quality of the broadcasted video or clip.

To use the Screen Broadcast function, select the device(s) you would like to create a broadcast room with on the main menu page and select **Screen Broadcast** > **Create a broadcast room** from the **Select Function** drop down menu. If a broadcast room has already been created, select **Screen Broadcast** > the created broadcast room, from the **Select Function** drop down menu.



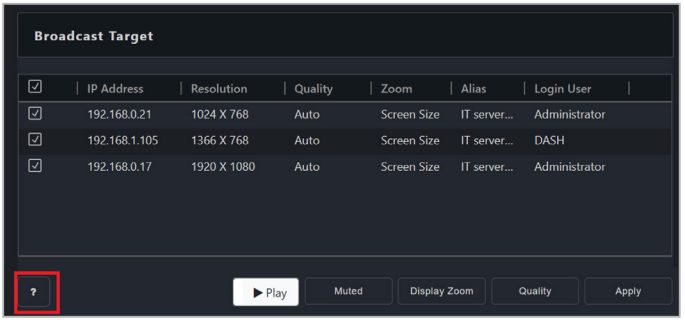
Broadcast Room Overview

Room Name	Enter the name of the broadcast room
Broadcast Source	Select the device to be the broadcast source
Input Type	Select if you would like to broadcast the broadcast source's display device, camera device, or a video file on the selected device.
Broadcast Target	Select the targets you would like to broadcast to.
Play/Stop	Play or stop the broadcast.
Muted	Mute or unmute the broadcast sound for broadcast target(s) when broadcasting.
Display Zoom	Select the screen size of the broadcast.
Quality	Select the resolution of the broadcast.
Create	Create the broadcast using the settings set. If you are editing an existing broadcast room, this option will not be available.
Apply	Apply the changes made to the settings of the broadcast room. If you are creating a new broadcast room, this option will not be available.

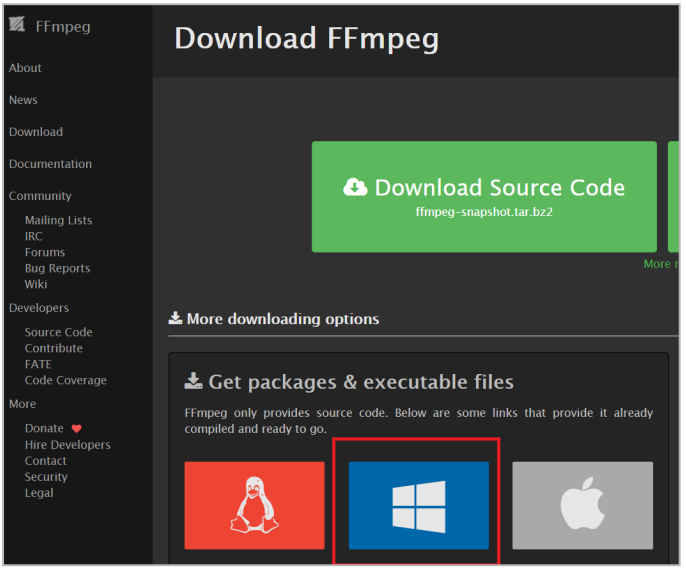
- The main server will be marked in the **Broadcast Source**. **Video files** can only be broadcast when the main server is selected as the broadcast source. You can broadcast **Display Device** and **Camera Device** from any broadcast source.
- The resolution may differ according to the **Input Type** selected and the resolutions it supports.

5.11.1 Setting up the broadcast environment

Before using the Screen Broadcast function, please set up the main server's playback environment for the broadcast function. Please refer to the following steps or click on ? at the bottom left of the Broadcast Room for information on setting up the Broadcast function playback environment settings.



1. Visit https://ffmpeg.org/, then navigate to the download section, and select the Windows version in the **Get packages & executable files** block.

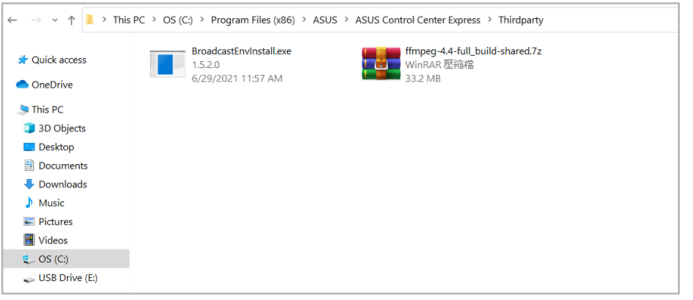


2. Select **Windows builds from gyan.dev**.

3. Select and download the **ffmpeg-release-full-shared.7z** file.

It is recommended to download ffmpeg versions 4.4, 5.0.1, or 5.1.2.

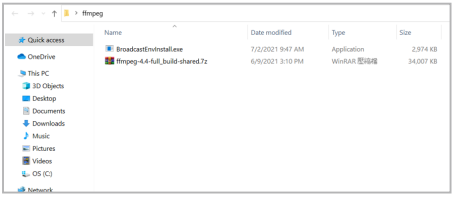
4. After the download is completed, move the downloaded ffmpeg installation zip file into the same folder as the ffmpeg environment variables file (**BroadcastEnvInstall.exe**) located in the *ASUS Control Center Express\Thirdparty* installation folder.



- The default installation path for ASUS Control Center Express is *ASUS Control Center Express\Thirdparty*, if you selected a different path when installing ASUS Control Center Express, ensure to change the installation folder path accordingly.
- You may change the folder path for the downloaded ffmpeg installation zip file and ffmpeg environment variables file (BroadcastEnvInstall.exe) if required, however, both files need to be located in the same folder.

5. Launch **BroadcastEnvInstall.exe** to set the ffmpeg environmental variable settings, then press any key to exit once the settings have been set.

Ensure both downloaded ffmpeg installation zip file and ffmpeg environment variables file (BroadcastEnvInstall.exe) are located in the same folder before setting the ffmpeg environment variables.

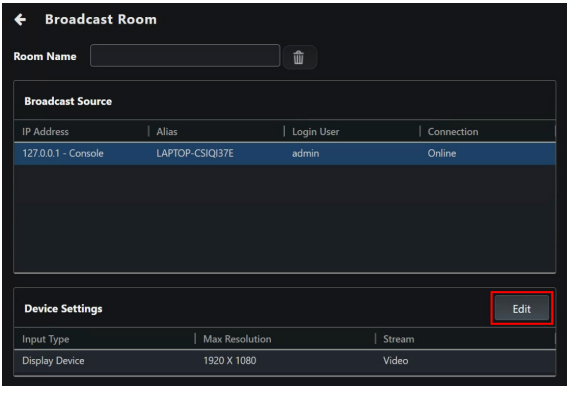



```
Run start install
start unzip
finish unzip
installation succeeded
Press any key to continue . . .
```

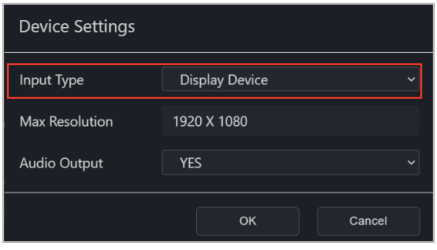
5.11.2 Adding a new Broadcast Room

To use the broadcast function, you will need to create a broadcast room. On the Broadcast Room page, you can configure different settings for the broadcast, such as the selecting the webcam or a video as the broadcast source, or selecting the broadcast target.

1. Select the device(s) you would like to create a broadcast room with on the main menu page and select **Screen Broadcast** > **Create a broadcast room** from the **Select Function** drop down menu.
2. Enter the broadcast room name into the **Room Name** field.
3. Select the broadcast source from the broadcast source list.
4. Click on **Edit** next to **Input Type** to configure the Device settings.



5. Select the **Input Type** in the Device Settings window. Depending on the input type selected, the configuration options for Device Settings may differ.



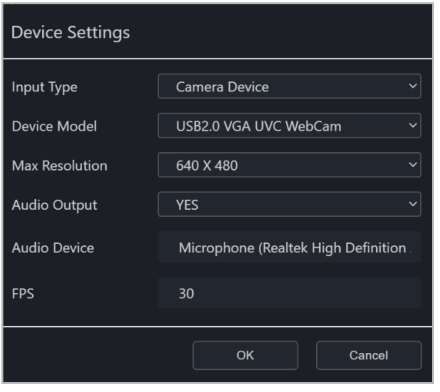
- **Display Device**

Set the display device of the broadcast source device for the broadcast.

Max Resolution	The maximum resolution of the display device.
Audio Output	Select whether to enable or disable audio output for the broadcast.

- **Camera Device**

Set the camera device of the broadcast source device for the broadcast.

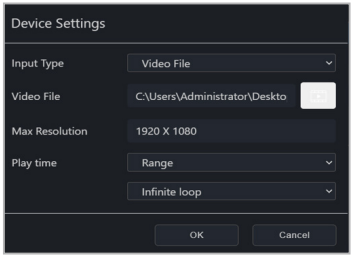


Device Model	Select the camera to be used for the broadcast.
Max Resolution	The maximum resolution of the camera.
Audio Output	Select whether to enable or disable audio output for the broadcast.
Audio Device	Select the audio device for the broadcast.
FPS	Select the camera's frames per second (FPS).

The **Max Resolution** options may differ depending on the resolutions the camera supports. The FPS will be adjusted according to the resolution selected.

- **Video File**

  Select a video file on the broadcast source device for the broadcast.

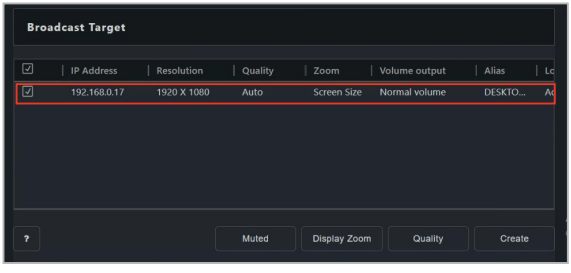


Video File	Select the video file to be used for the broadcast. Supported video codec formats: MPEG-2, MPEG-4, .AVI, and .WMV.
Max Resolution	The maximum resolution of the video broadcast.
Play time	Select the number of times the video file is looped from either a set range, or a custom number.
	Select the number of times to loop, or enter the number manually.

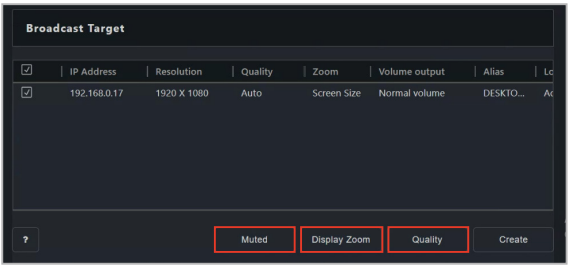
- The main server will be marked in the **Broadcast Source**. **Video files** can only be broadcast when the main server is selected as the broadcast source.
- To select multiple video files and create a playlist, click **Edit** next to **Device Settings** again and select the next video file.

6. To change any configuration options, click **Edit** next to **Device Settings** again.

7. Check the client devices you would like to broadcast to.



8. Configure the **Display Zoom**, **Quality**, and whether the audio should be muted for the broadcast

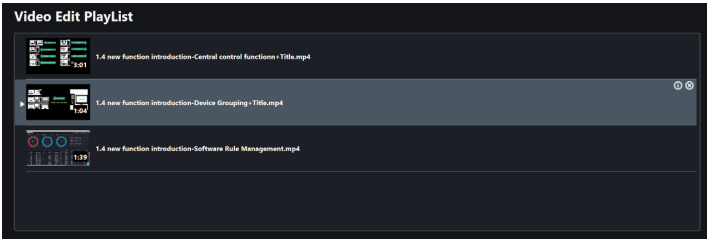


9. Click **Create** to create the broadcast room.

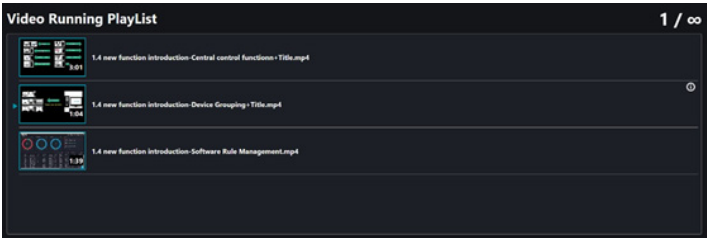
5.11.3 Managing video playlists

When a video file is added, the playlist editor will automatically appear and can be used to view or change the order in which video files are played.

- To change the position of a video file in the playlist, click and drag the title of the video file to change its position in the playlist.
- To select which video file is played first in the broadcast, click the title of the video file. It will be highlighted and played first when the broadcast is started.
- Once a video file is added, click the icon to view information about a video file in the playlist, or click on the icon to delete a video from the playlist.



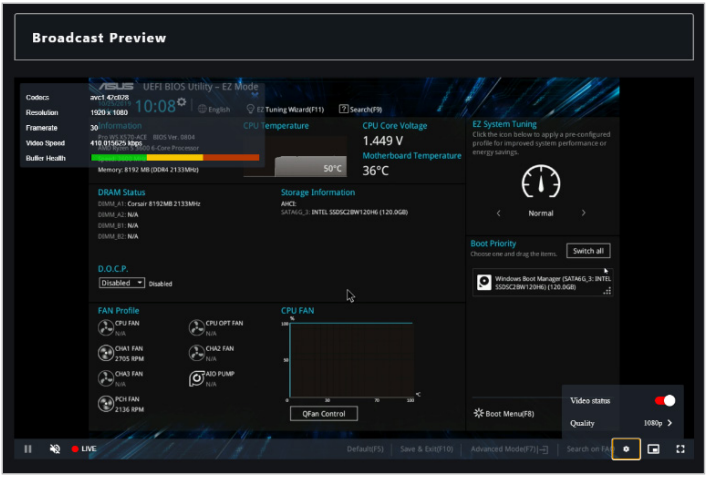
If the broadcast is currently active, the playlist viewer will appear instead. The currently playing video will be highlighted with a blue frame and arrow icon. To make changes to the playlist, please stop the broadcast first.



5.11.4 Starting or stopping a broadcast

You can start or stop the broadcast of an existing broadcast room by following the below steps:

1. Navigate to the **Broadcast Room** of an existing broadcast room.
2. Scroll to the bottom of the page, then click on **Play**.
3. You can view the data transmission rate and health status of the broadcast in the **Broadcast Source** block.
4. You can configure or view the settings of the broadcast from the items located at the bottom of the Broadcast Preview.



Play / Stop	Play or stop the broadcast.
Volume	Adjust the volume of the preview broadcast of the main server. This option only affects the volume of the broadcast source, and will not adjust the volume for client devices.
Video Status	Displays the current status of the broadcast.
Settings	Allows you to toggle the **Video status** on/off, and also select the quality of the broadcast.
Picture-in-Picture	Select if you would like to view the preview broadcast in Picture-in-Picture (PiP).
Full Screen	Select if you would like to view the preview broadcast in full screen.

5. Press **Stop** to end the ongoing broadcast.

- You can configure the settings for the Broadcast Room when a broadcast is playing. Please refer to **5.10.4 Editing an existing Broadcast Room** for more information.
- Clicking on next to the Broadcast Room Name will delete the Broadcast Room if you no longer need the Broadcast Room.
- You cannot broadcast to client devices which are offline, if a selected device is offline whilst the broadcast is playing, the broadcast will automatically play when the device changes to online status.
- Client device(s) cannot update agents during a broadcast. Stop and close the broadcast first if you wish to update the agents for the device(s).
- A device selected as broadcast target can be set as the broadcast source if the **Input Type** selected is **Display Device** or **Camera Device**.

5.11.5 Editing an existing Broadcast Room

1. (optional) If you wish to add new device(s) to the existing broadcast room, select the new client device(s) you would like to add to the broadcast room before continuing with step 2.
2. From the **Select Function** drop down menu, select **Screen Broadcast**, then select the Broadcast Room you would like to edit.
3. Follow steps 2-8 of section **5.10.2 Adding a new Broadcast Room** to edit the Broadcast Room.

If you added new device(s) to the broadcast room, ensure to select the newly added device(s) in the **Broadcast Target** block.

4. Click **Apply** once you are finished to apply the changes made, or click **Play** to play the broadcast using the new changes.

Clicking on next to the Broadcast Room Name will delete the Broadcast Room if you no longer need the Broadcast Room.

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.

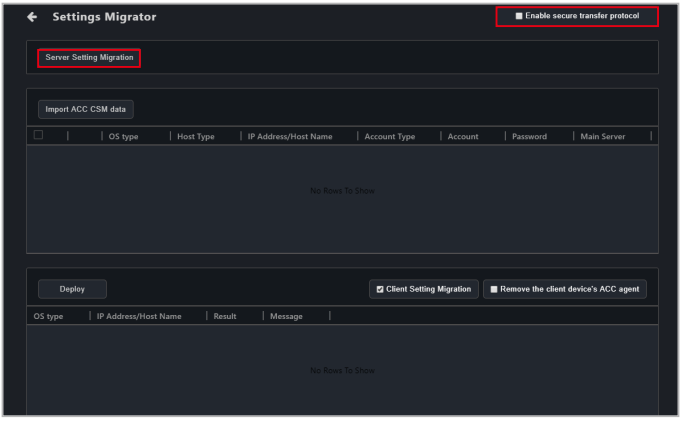
To access **Settings Migrator**, click on located at the top right menu bar, then select **Settings Migrator**.

The screenshots in this section are for reference only.

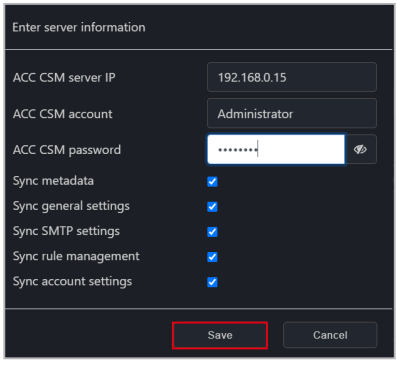
6.1.1 Migrating configurations of ACC CSM server

You can migrate the ACC CSM server configurations to ASUS Control Center Express by following the steps below:

1. (optional) Check the **Enable secure transfer protocol** option to ensure the data to be migrated is protected with a safety protocol.
2. Click on **Server Setting Migration**.



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



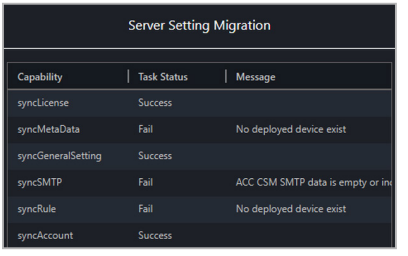
ACC CSM server IP	IP address of the ACC CSM server you wish to import
ACC CSM account	The administrator account of the ACC CSM server you wish to import
ACC CSM password	The password for the administrator account of the ACC CSM server you wish to import
Sync metadata	Check to import metadata fields of ACC CSM
Sync general setting	Check to import specific general settings of ACC CSM. These settings include: MainServer Settings - Web page refresh timer - Check for updates timer Agent Configuration - Hardware sensor interval - Utilization time interval - Agent response timer
Sync SMTP setting	Check to import the SMTP settings of ACC CSM
Sync rule management	Check to import notification rules of ACC CSM • Imported notification rules will only be applied to ACC CSM client devices managed by ASUS Control Center Express. • If new deployed CSM devices are added after you have already migrated server configurations, please use the **Setting Migrator** again after the deployment to sync the configurations.

(continued on the next page)

Sync account setting	Check to import the accounts and roles of ACC CSM The default account for ACC CSM cannot be imported. 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.

Migrated CSM product license keys will be migrated to the **CSM License Information** list under the **License** tab in ASUS Control Center Express. Please refer to **8.2 License information** for more information.

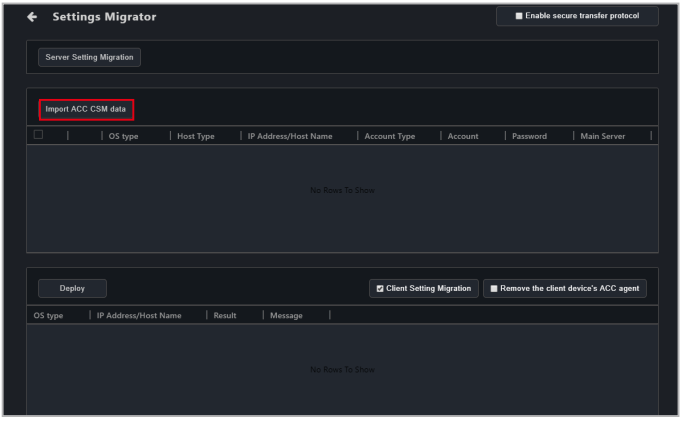
4. The results of the configuration and data migration may differ according to the ACC CSM's configurations. You can view the migration results for each option in the mission center.



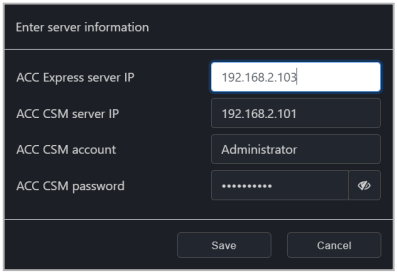
6.1.2 Importing ACC CSM data

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

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



2. Enter the required information into the fields.



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

3. Click on **Save** when you are finished to begin importing the data of the client devices.

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

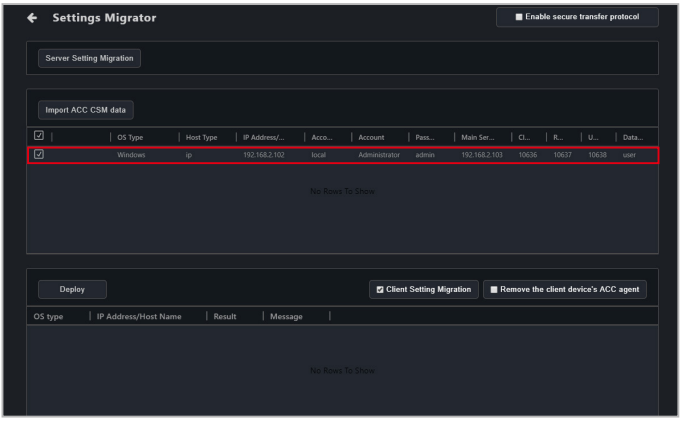
If an imported client device has already been deployed with an ASUS Control Center Express agent, **This device has already been deployed to** will be displayed. If you wish to redeploy to this device, please remove the agent first, you may refer to section **3.3 Removing agents** for more information.

6.1.3 Deploying ACCE agents to ACC CSM 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 **8.1.4 License**.

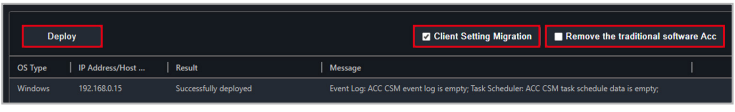
2. Double click on the imported client devices you wish to deploy agents to and change the password to the administrator password of the client device, then click on **Save**. You can also edit the default Agent device's administrator account and password, under **Settings** > **Options** > **General Configurations** > **Agent device's administrator account**. Please refer to **8.1.4 Agent account password** for more information.
3. Check the devices you wish to deploy an agent to in the imported devices list.



4. (optional) Check **Client setting migration** to import the ACC CSM client settings and data for the selected devices when you deploy, this option is checked by default. Please refer to the table below for more information on the client settings and data **Client setting migration** will import.

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

5. (optional) Check **Remove the client device's ACC agent** to remove any previous versions of ASUS Control Center agents installed on the selected client devices when deploying new agents.
6. Click on **Deploy** and wait for the agent deployment to be completed. The results of the deployment may differ according to the ACC CSM's configurations. You can view the deployment and data migration results for each device in the result block.



Ensure a Windows operating system Administrator account of the client is enabled and has a password set.

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.

Chapter 7

This chapter describes how to generate various reports on client devices.

Report Generator

7.1 Report Generator

You can generate reports on the connection status, software installation history, and hardware information of the client device.

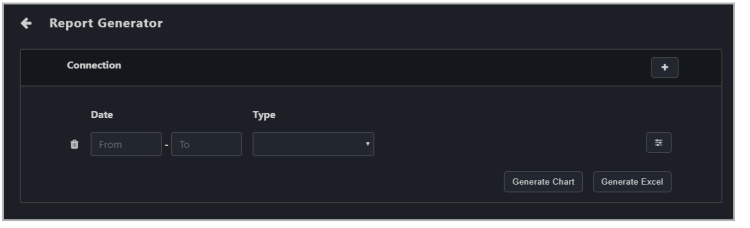
The information entered in this section is for reference only.

7.1.1 Connection Report

The Connection report will generate a report on the connection status of a single or multiple selected device(s).

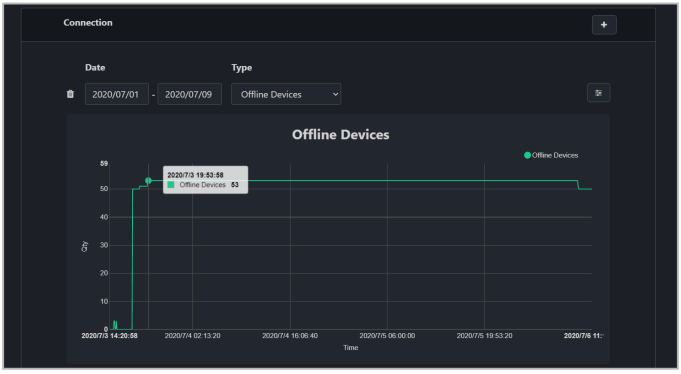
You can enable or disable connection history recording for reports in **Settings** > **Options** > **General Configuration** under the **Report Generator** block.

To create a connection report on all devices click on located at the top right menu bar, then select **Connection**. To create a connection report on multiple devices, select the devices you wish to create a connection report on from the Device Overview, then click on **Select Function** > **Report Generator** > **Connection**.

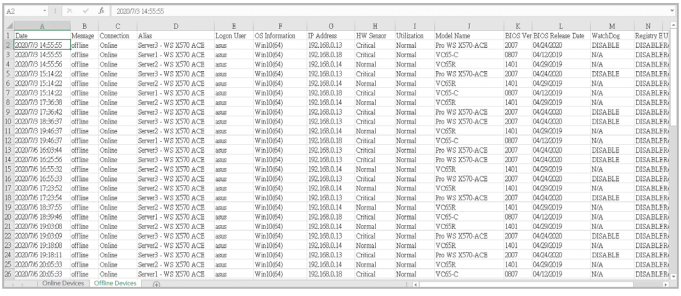


Date	Set a date range to generate the report. If this field is left blank, a report will be generated on all the dates recorded on the main server.
Type	Select if you want to generate a report on Online Devices or Offline Devices.
Customize ( )	Select the metadata fields you would like to display on the report.
Add (+)	Add additional reports.
Delete ( )	Delete the selected generated chart and report information fields.
Generate Chart	Generate a line chart on the information entered or selected.
Generate Excel	Generate a excel file on the information entered or selected. The generated Excel file will not include a line chart.

Generated Connection Report chart



Generated Connection Report Excel file

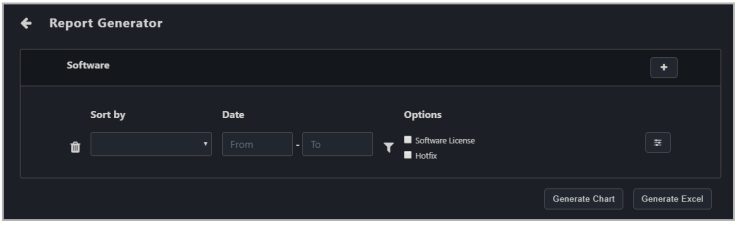


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Date	Message	Connection	Alias	Logon User	OS Information	IP Address	HW Sensor	Utilization	Model Name	BIOS Ver	BIOS Release Date	WatchDog	Registry EU
2	2020/7/3 14:55:55	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
3	2020/7/3 14:55:55	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC65-C	0807	04/12/2019	N/A	DISABLE/R/
4	2020/7/3 14:55:56	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
5	2020/7/3 15:14:22	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
6	2020/7/3 15:14:22	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
7	2020/7/3 15:14:22	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC65-C	0807	04/12/2019	N/A	DISABLE/R/
8	2020/7/3 17:36:38	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
9	2020/7/3 17:36:42	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
10	2020/7/3 18:36:37	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
11	2020/7/3 19:46:37	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
12	2020/7/3 19:46:37	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC65-C	0807	04/12/2019	N/A	DISABLE/R/
13	2020/7/6 16:02:44	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
14	2020/7/6 16:25:56	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
15	2020/7/6 16:55:32	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
16	2020/7/6 16:55:33	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
17	2020/7/6 17:23:52	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
18	2020/7/6 17:23:54	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
19	2020/7/6 18:37:55	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
20	2020/7/6 18:39:46	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC65-C	0807	04/12/2019	N/A	DISABLE/R/
21	2020/7/6 19:03:08	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
22	2020/7/6 19:03:09	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
23	2020/7/6 19:18:08	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
24	2020/7/6 19:18:11	offline	Online	Server3 - WS X570 ACE	asus	Win10(64)	192.168.0.13	Critical	Normal	Pro WS X570-ACE	2007	04/24/2020	DISABLE	DISABLE/R/
25	2020/7/6 20:05:33	offline	Online	Server2 - WS X570 ACE	asus	Win10(64)	192.168.0.14	Normal	Normal	VC65R	1401	04/29/2019	N/A	DISABLE/R/
26	2020/7/6 20:05:33	offline	Online	Server1 - WS X570 ACE	asus	Win10(64)	192.168.0.18	Critical	Normal	VC65-C	0807	04/12/2019	N/A	DISABLE/R/

7.1.2 Software Report

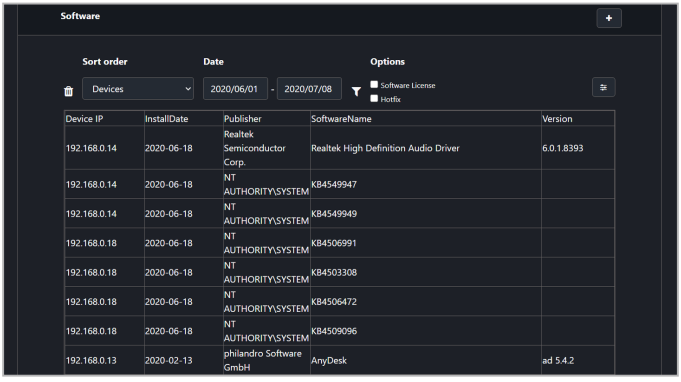
The Software report will generate a report on the software installation history of a single or multiple selected device(s).

To create a software report on all devices click on located at the top right menu bar, then select **Software**. To create a software report on multiple devices, select the devices you wish to create a software report on from the Device Overview, then click on **Select Function** > **Report Generator** > **Software**.



Sort by	Select if you want to sort the generated report by **Devices** or by **Software**. • **Devices:** Generate report based on the devices and shows the software installed on it. • **Software:** Generate report based on the software and which devices have this software installed on it.
Date	Set a date range to generate the report. If this field is left blank, a report will be generated on all the dates recorded on the main server.
Options	Check **Software License** to generate a report only on Software License updates. Check **Hotfix** to generate a report only on hotfix updates. If this field is left blank, a report will be generated on all options.
Filter ( )	Use the filter function to select which software you would like to generate a report on. If this field is left blank, a report will be generated on all software recorded on the main server.
Customize ( )	Select the metadata fields you would like to display on the report.
Add ( )	Add additional reports.
Delete ( )	Delete the selected generated chart and report information fields.
Group	Filter the generated report by an existing group or add a new group to filter by. For more information on adding groups, please refer to **2.2.5 Creating client device groups**.
Generate Chart	Generate a table on the information entered or selected.
Generate Excel	Generate a excel file on the information entered or selected.

Generated Software Report chart



Software

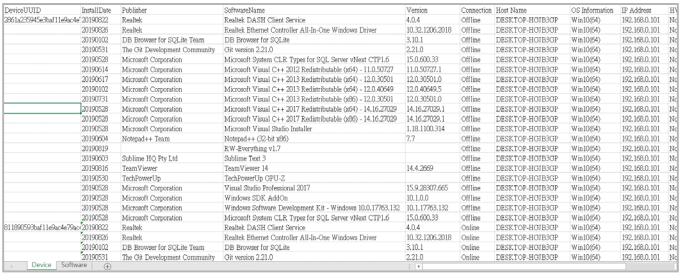
Sort order: Devices

Date: 2020/06/01 - 2020/07/08

Options: Software License, Hotfix

Device IP	InstallDate	Publisher	SoftwareName	Version
192.168.0.14	2020-06-18	Realtek Semiconductor Corp.	Realtek High Definition Audio Driver	6.0.1.8393
192.168.0.14	2020-06-18	NT AUTHORITY\SYSTEM	KB4549947	
192.168.0.14	2020-06-18	NT AUTHORITY\SYSTEM	KB4549949	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4506991	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4503308	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4506472	
192.168.0.18	2020-06-18	NT AUTHORITY\SYSTEM	KB4509096	
192.168.0.13	2020-02-13	philandro Software GmbH	AnyDesk	ad 5.4.2

Generated Software Report Excel file



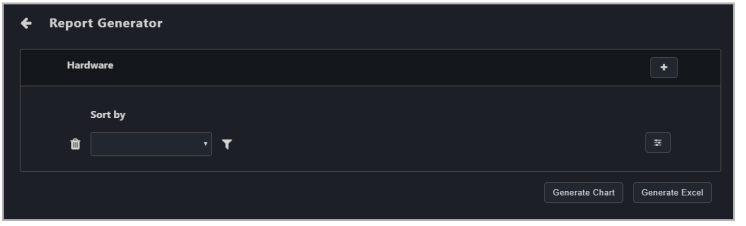
DeviceUUID	InstallDate	Publisher	SoftwareName	Version	Connection	Host Name	OS Information	IP Address	HV
2861a25f945e8caf11e9ac4e	20190822	Realtek	Realtek DASH Client Service	4.0.4	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190626	Realtek	Realtek Ethernet Controller All-In-One Windows Driver	10.32.1206.2018	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190102	DB Browser for SQLite Team	DB Browser for SQLite	3.10.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190531	The Git Development Community	Git version 2.21.0	2.21.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190520	Microsoft Corporation	Microsoft System CLR Types for SQL Server vNext CTP1.6	15.0.600.33	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190614	Microsoft Corporation	Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.50727	11.0.50727.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190617	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501	12.0.30501.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190102	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40649	12.0.40649.5	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190731	Microsoft Corporation	Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501	12.0.30501.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Microsoft Visual C++ 2017 Redistributable (x64) - 14.16.27029	14.16.27029.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Microsoft Visual C++ 2017 Redistributable (x86) - 14.16.27029	14.16.27029.1	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Microsoft Visual Studio Installer	1.18.1100.314	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190604	Notepad++ Team	Notepad++ (32-bit x86)	7.7	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190819		RW-Everything v1.7		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190603	Sublime HQ Pty Ltd	Sublime Text 3		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190816	TeamViewer	TeamViewer 14	14.4.2669	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190530	TechPowerUp	TechPowerUp GPU-Z		Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Visual Studio Professional 2017	15.9.28307.665	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Windows SDK AddOn	10.1.0.0	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Windows Software Development Kit - Windows 10.0.17763.132	10.1.17763.132	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190528	Microsoft Corporation	Microsoft System CLR Types for SQL Server vNext CTP1.6	15.0.600.33	Offline	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
811890593baf11e9ac4e79ac	20190822	Realtek	Realtek DASH Client Service	4.0.4	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190626	Realtek	Realtek Ethernet Controller All-In-One Windows Driver	10.32.1206.2018	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190102	DB Browser for SQLite Team	DB Browser for SQLite	3.10.1	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No
	20190531	The Git Development Community	Git version 2.21.0	2.21.0	Online	DESKTOP-HOTB3OP	Win10(64)	192.168.0.101	No

Device | Software

7.1.3 Hardware Report

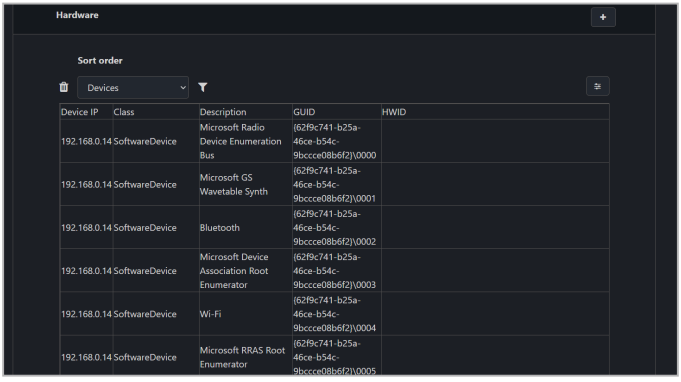
The Hardware report will generate a report on the hardware of a single or multiple selected device(s).

To create a hardware report on all devices click on located at the top right menu bar, then select **Hardware**. To create a hardware report on multiple devices, select the devices you wish to create a hardware report on from the Device Overview, then click on **Select Function** > **Report Generator** > **Hardware**.



Sort by	Select if you want to sort the generated report by **Devices** or by **Hardware**. • **Devices:** Generate report based on the devices and shows the hardware installed on it. • **Hardware:** Generate report based on the hardware and which devices have this hardware installed on it.
Filter ( )	Use the filter function to select which hardware component you would like to generate a report on. If this field is left blank, a report will be generated on all hardware components recorded on the main server.
Customize ( )	Select the metadata fields you would like to display on the report.
Add ( )	Add additional reports.
Delete ( )	Delete the selected generated chart and report information fields.
Group	Filter the generated report by an existing group or add a new group to filter by. For more information on adding groups, please refer to **2.2.5 Creating client device groups**.
Generate Chart	Generate a table on the information entered or selected.
Generate Excel	Generate a excel file on the information entered or selected.

Generated Hardware Report chart



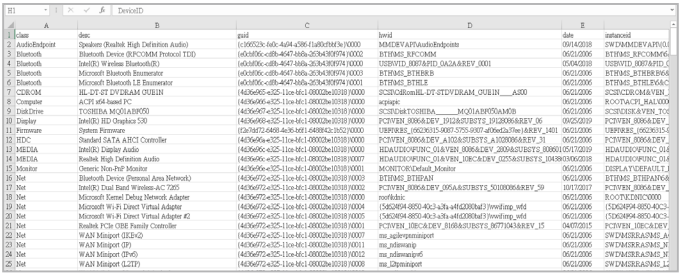
Hardware

Sort order

Devices

Device IP	Class	Description	GUID	HWID
192.168.0.14	SoftwareDevice	Microsoft Radio Device Enumeration Bus	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0000	
192.168.0.14	SoftwareDevice	Microsoft GS Wavetable Synth	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0001	
192.168.0.14	SoftwareDevice	Bluetooth	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0002	
192.168.0.14	SoftwareDevice	Microsoft Device Association Root Enumerator	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0003	
192.168.0.14	SoftwareDevice	Wi-Fi	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0004	
192.168.0.14	SoftwareDevice	Microsoft RRAS Root Enumerator	{62f9c741-b25a-46ce-b54c-9bccce08b6f2}\0005	

Generated Hardware Report Excel file



H1 DeviceID

	A	B	C	D	E	
1	class	desc	guid	hwid	date	instanceid
2	AudioEndpoint	Speakers (Realtek High Definition Audio)	{c166523c-fe0c-4a94-a586-f1a80cf8d3e}\0000	MMDEVAPI\AudioEndpoints	09/14/2018	SWD\MMDEVAPI\{0.0
3	Bluetooth	Bluetooth Device (RFCOMM Protocol TDI)	{e0cbf06c-cdb8-4647-bb8a-263b43f0f974}\0002	BTHMS_RFCOMM	06/21/2006	BTHMS_RFCOMM\6&...
4	Bluetooth	Intel(R) Wireless Bluetooth(R)	{e0cbf06c-cdb8-4647-bb8a-263b43f0f974}\0000	USB\VID_8087&PID_0A2A&REV_0001	05/04/2018	USB\VID_8087&PID_0
5	Bluetooth	Microsoft Bluetooth Enumerator	{e0cbf06c-cdb8-4647-bb8a-263b43f0f974}\0003	BTHMS_BTHBRB	06/21/2006	BTHMS_BTHBRB\6&
6	Bluetooth	Microsoft Bluetooth LE Enumerator	{e0cbf06c-cdb8-4647-bb8a-263b43f0f974}\0001	BTHMS_BTHLE	06/21/2006	BTHMS_BTHLE\6&C
7	CDROM	HL-DT-ST DVDRAM GUB1N	{4d36e965-e325-11ce-bfc1-08002be10318}\0000	SCSI\CdRomHL-DT-STDVDRAM_GUB1N____A800	06/21/2006	SCSI\CDROM&VEN_
8	Computer	ACPI x64-based PC	{4d36e966-e325-11ce-bfc1-08002be10318}\0000	acpiapic	06/21/2006	ROOT\ACPI_HAL\000
9	DiskDrive	TOSHIBA MQ01ABF050	{4d36e967-e325-11ce-bfc1-08002be10318}\0000	SCSI\DiskTOSHIBA_____MQ01ABF050\4A0B	06/21/2006	SCSI\DISK&VEN_TO
10	Display	Intel(R) HD Graphics 530	{4d36e968-e325-11ce-bfc1-08002be10318}\0000	PCI\VEN_8086&DEV_1912&SUBSYS_19128086&REV_06	09/25/2019	PCI\VEN_8086&DEV_
11	Firmware	System Firmware	{f2e7dd72-6468-4e36-b6f1-6488f42c1b52}\0000	UEFI\RES_{992636f5-5097-5755-9307-af09ed2a79ee}&REV_1401	06/21/2006	UEFI\RES_{992636f5-5
12	HDC	Standard SATA AHCI Controller	{4d36e96a-e325-11ce-bfc1-08002be10318}\0000	PCI\VEN_8086&DEV_A102&SUBSYS_A1028086&REV_31	06/21/2006	PCI\VEN_8086&DEV_
13	MEDIA	Intel(R) Display Audio	{4d36e96c-e325-11ce-bfc1-08002be10318}\0000	HDAUDIO\FUNC_01&VEN_8086&DEV_2809&SUBSYS_80860105\7&2019	06/21/2006	HDAUDIO\FUNC_01&
14	MEDIA	Realtek High Definition Audio	{4d36e96c-e325-11ce-bfc1-08002be10318}\0007	HDAUDIO\FUNC_01&VEN_10EC&DEV_0255&SUBSYS_104380D0\6&28	06/21/2006	HDAUDIO\FUNC_01&
15	Monitor	Generic Non-PnP Monitor	{4d36e96e-e325-11ce-bfc1-08002be10318}\0001	MONITOR\Default_Monitor	06/21/2006	DISPLAY\DEFAULT_
16	Net	Bluetooth Device (Personal Area Network)	{4d36e972-e325-11ce-bfc1-08002be10318}\0003	BTHMS_BTHPAN	06/21/2006	BTHMS_BTHPAN\6&
17	Net	Intel(R) Dual Band Wireless-AC 7265	{4d36e972-e325-11ce-bfc1-08002be10318}\0002	PCI\VEN_8086&DEV_095A&SUBSYS_50108086&REV_59	10/17/2017	PCI\VEN_8086&DEV_
18	Net	Microsoft Kernel Debug Network Adapter	{4d36e972-e325-11ce-bfc1-08002be10318}\0000	root\kdnic	06/21/2006	ROOT\KDNIC\0000
19	Net	Microsoft Wi-Fi Direct Virtual Adapter	{4d36e972-e325-11ce-bfc1-08002be10318}\0004	{5d624f94-8850-40c3-a3fa-a4fd2080baf3}\wwfmp_wfd	06/21/2006	{5D624F94-8850-40C3-
20	Net	Microsoft Wi-Fi Direct Virtual Adapter #2	{4d36e972-e325-11ce-bfc1-08002be10318}\0005	{5d624f94-8850-40c3-a3fa-a4fd2080baf3}\wwfmp_wfd	06/21/2006	{5D624F94-8850-40C3-
21	Net	Realtek PCIe GBE Family Controller	{4d36e972-e325-11ce-bfc1-08002be10318}\0001	PCI\VEN_10EC&DEV_8168&SUBSYS_86771043&REV_15	04/07/2015	PCI\VEN_10EC&DEV_
22	Net	WAN Miniport (IEEE-O	{4d36e972-e325-11ce-bfc1-08002be10318}\0007	ms_agilevpnminiport	06/21/2006	SWD\MSRRAS\MS_A
23	Net	WAN Miniport (IP)	{4d36e972-e325-11ce-bfc1-08002be10318}\0011	ms_ndiswanip	06/21/2006	SWD\MSRRAS\MS_N
24	Net	WAN Miniport (IPv6)	{4d36e972-e325-11ce-bfc1-08002be10318}\0012	ms_ndiswanipv6	06/21/2006	SWD\MSRRAS\MS_N
25	Net	WAN Miniport (L2TP)	{4d36e972-e325-11ce-bfc1-08002be10318}\0009	ms_l2tpminiport	06/21/2006	SWD\MSRRAS\MS_L

Chapter 8

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

Account & General Settings

8.1 Options menu

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

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

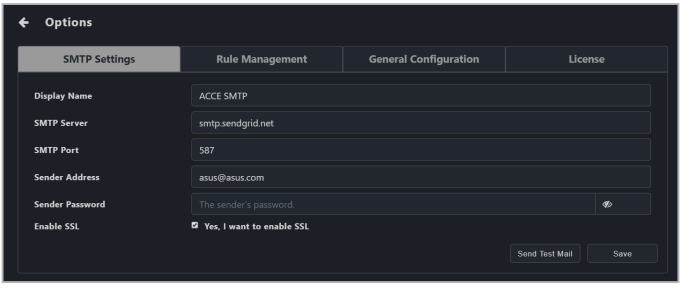
The information entered in this section is for reference only.

8.1.1 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.

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.



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

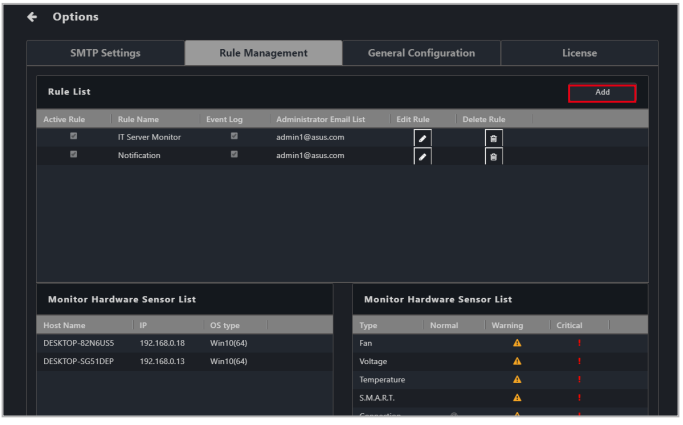
2. (optional) Click on **Send Test Mail**, then enter an email and click **Send** to receive the test mail allowing you to check the status of the SMTP. If the SMTP is functioning properly, you should receive an email.
3. Click **Save** to save the changes made.

8.1.2 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.

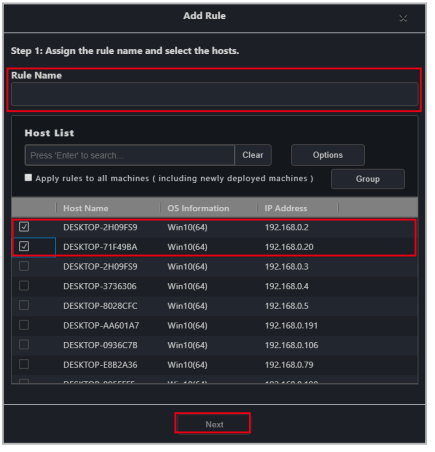
Adding a new rule

1. Click on **Add**.



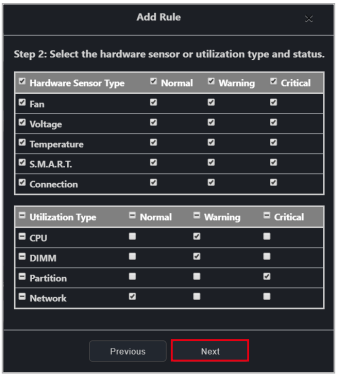
2. Enter a rule name, then select the devices to apply the rule to. Click **Next**.

- 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.
- Selecting a group in the **Group** option will check the devices in that group on the **Host List**.
- 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**.
- Check **Apply rules to all machines (including newly deployed machines** to apply the new rule to all devices in the **Host List**.



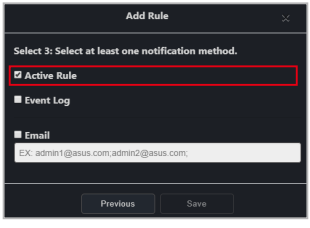
3. Select conditions (type and status of hardware or utilization sensors) to send notifications, then click **Next**.

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**.



4. You can select to enable or disable the newly added rule by checking **Active Rule**.

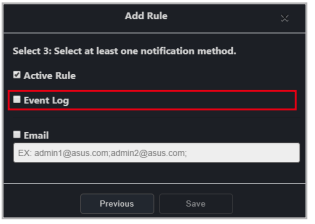
Active Rule is checked by default.



5. 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.

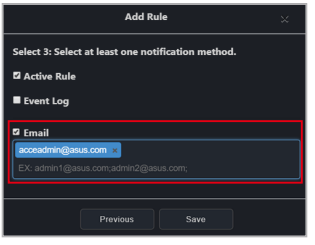


- Email

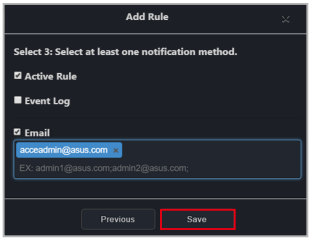
  The notification is sent to the entered email addresses.

Ensure to set up the SMTP server settings before using the email function. For more information please refer to **8.1.1 SMTP Settings**.

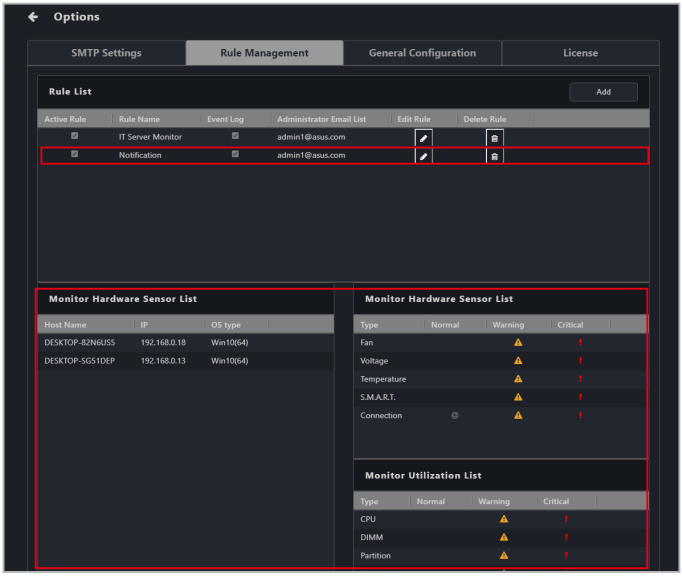
When entering multiple emails, press <Enter> after each email to separate the emails.



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



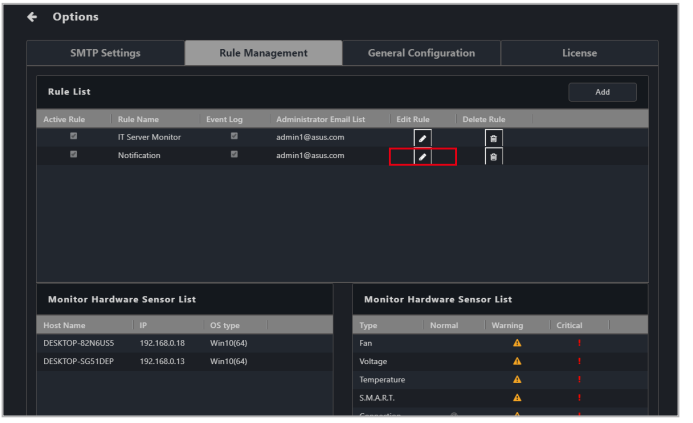
Your newly added rule should appear under **Rule List**, this displays the rule name and details of your selected notification method. Clicking on the newly added rule will display the devices associated with the rule in the **Monitor Hardware Sensor List**, and the list of hardware and utilizations 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.

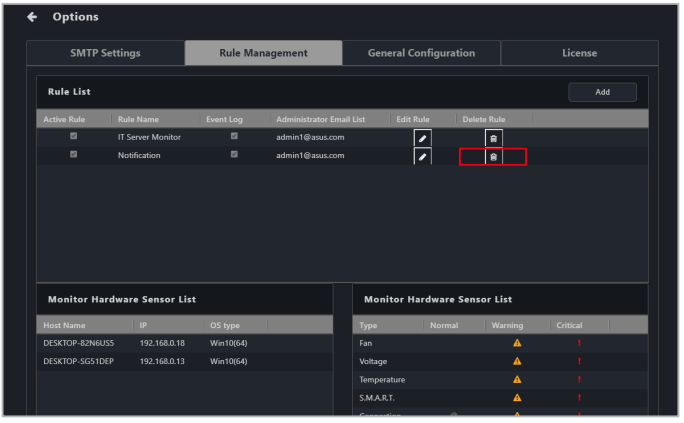
1. Select a rule in the **Rule List** you wish to edit, then click on in the **Edit Rule** column.



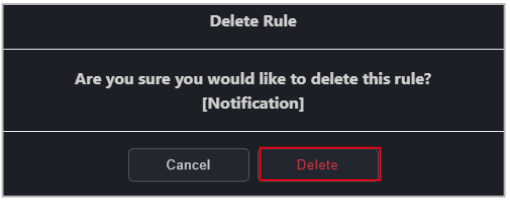
2. Follow steps 2 to 5 edit your Rule, then click **Save** to save the changes made.

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.

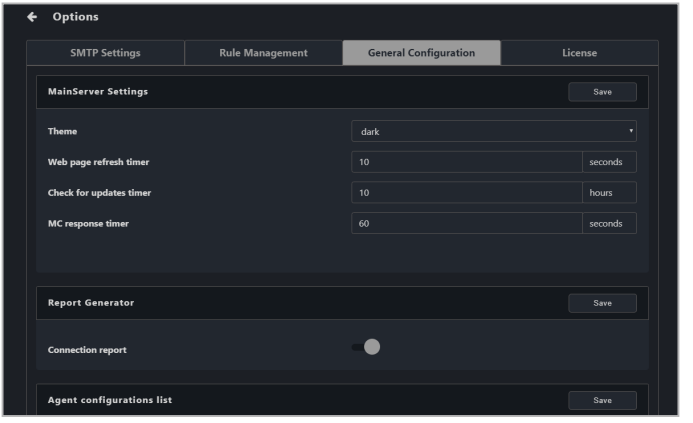


2. Click **Delete** to delete the rule.



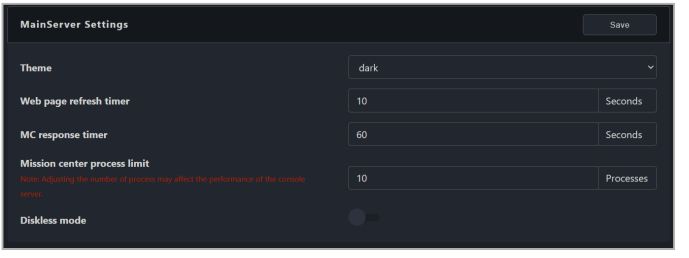
8.1.3 General Configuration

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.



Theme	Select a color theme (**acc_csm**, **acc**, **dark**, **metal**) for your main server.
Web page refresh timer	Set the time interval in seconds between each refresh of all webpages of the main server.
Mission center process limit	Set the maximum number of mission center processes.
Diskless mode	Enable to allow diskless mode, which allows you to deploy agents to remote machines without storage devices.

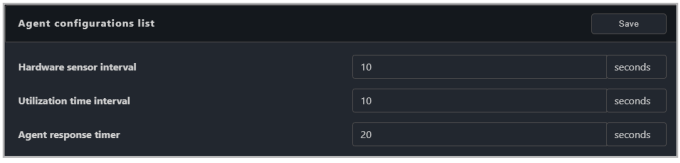
Report Generator:

Allows you to enable or disable recording for Connection reports. Click on **Save** to save the changes made.

Connection report	Enable or disable recording for connection reports.

Agent configuration list:

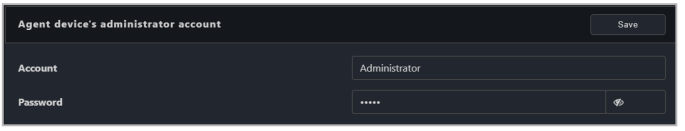
Configure the agent sensor intervals and response times. Click on **Save** to save the changes made.



Hardware sensor interval	Set the time interval in seconds for the hardware sensor to return sensor values .
Utilization time interval	Set the time interval in seconds for the utilization sensor to return sensor values .
Agent response timer	Set the time interval in seconds for the agent to query tasks from the main server.

Agent device's administrator 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.

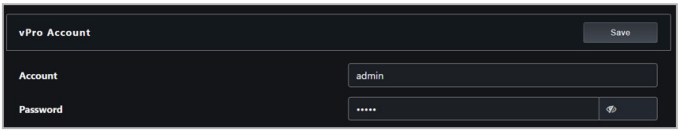


Account	Set the default administrator account.
Password	Set the default administrator password.

- If the account type is a domain account, you may enter the account in the format *Domain\Account*, which will set the default account used when deploying to a domain account.
- When using the default account when deploying, make sure of the language of the client device. The system account with administrator privileges may differ according to the system language, and may affect agent deployment to that device.

vPro Account:

Set the default login account used to log into the client vPro remote management controller. Click on **Save** to save the changes made.

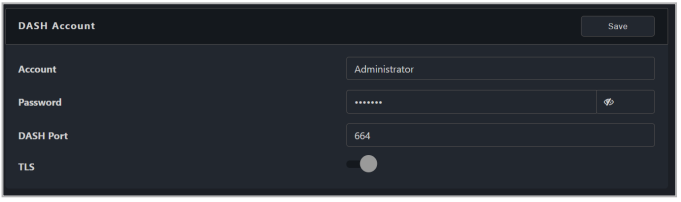


Account	Set the default account to log into the client device's vPro remote management controller.
Password	Set the default password to log into the client device's vPro remote management controller.

The account and password entered should match the account and password for the client device's vPro remote management controller.

DASH Account:

Set the default login account used to log into the client DASH remote management controller. Click on **Save** to save the changes made.

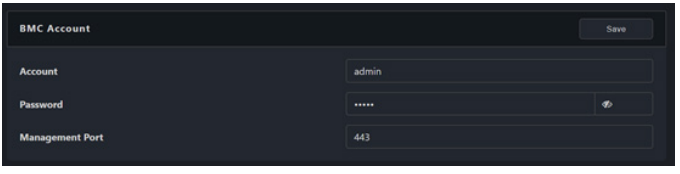


Account	Set the default account to log into the client device's DASH remote management controller.
Password	Set the default password to log into the client device's DASH remote management controller.
DASH port	Set the port for DASH (default: 664).
TLS	Enable or disable TLS (Transport Layer Security).

The account and password entered should match the account and password for the client device's DASH remote management controller.

BMC Account:

Set the default login account used to log into the client BMC remote management controller. Click on **Save** to save the changes made.



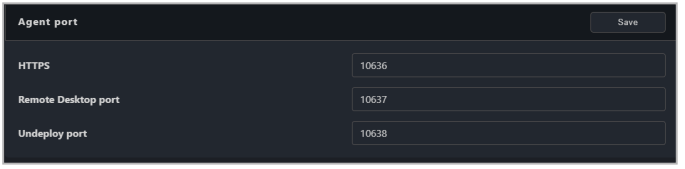
Account	Set the default account to log into the client device's BMC remote management controller.
Password	Set the default password to log into the client device's BMC remote management controller.
Management Port	Set the port for BMC (default: 443).

The account and password entered should match the account and password for the client device's BMC remote management controller.

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.

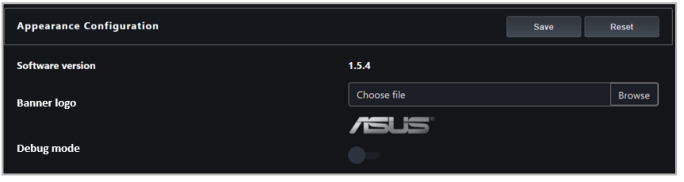
We recommend using the default values as this will require no further adjustments to the client device's firewall settings.



HTTPS	Set the port for webpage access. Default is 10636.
Remote Desktop port	Set the port for remote desktop. Default is 10637.
Undeploy port	Set the port for removing the agent from clients. Default is 10638.

Appearance Configuration:

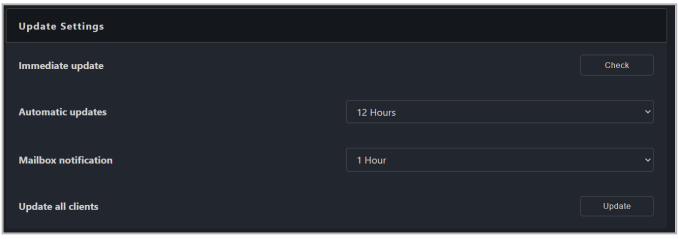
View the version of the main server, as well as customize the banner logo. Click on **Save** to save the changes made, or click on **Reset** to return to the default banner logo.



Software version	Displays the version of the main ASUS Control Center Express server.
Banner Logo	Click **Browse** to select and upload a new banner logo. The banner logo can be viewed in the top left corner of the main dashboard overview.
Debug mode	Enable or disable debug mode.

Update Settings:

Configure the update settings for the main server and clients.

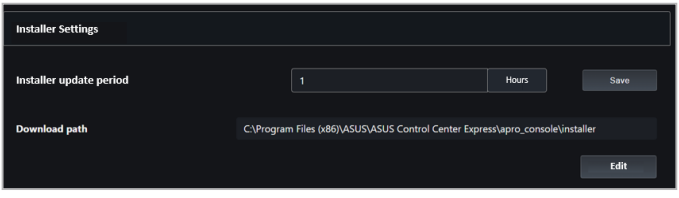


Immediate update	Click **Check** to check for and download new updates for the ASUS Control Center Express main software.
Automatic updates	Enable this option to automatically check for ASUS Control Center Express updates and send update notifications.
Mailbox notification	Set the notification and update time for ASUS Control Center Express mailbox.
Update All Clients	Click **Update** to begin updating all client agents

- **Automatic updates** is set to **Disable** by default.
- **Mailbox notification** is enabled by default.

Installer Settings:

Configure the Installer settings. Click on **Save** to save the changes made.

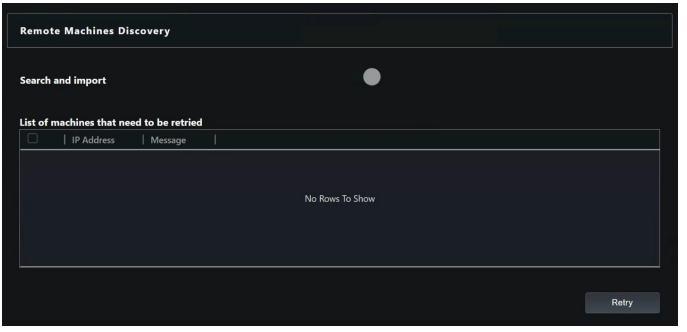


Installer Update Period	Set how often the installer will check for new updates.
Download path	View the current download path.
Edit	Select a new download path.

Remote Machines Discovery:

Enable **Search and import** to search for deployed devices that have not yet been added to the Device List. If there are devices that were not successfully added, check if sufficient licenses are available and click **Retry** to try again.

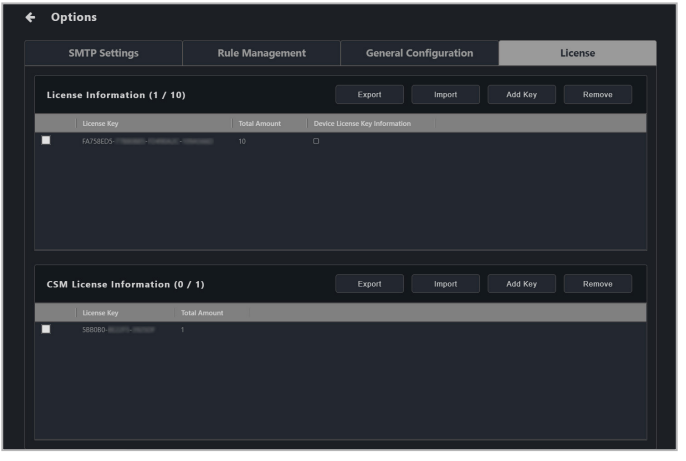
Disable **Search and Import** after you finish, as it may interfere with agent management.



8.1.4 License

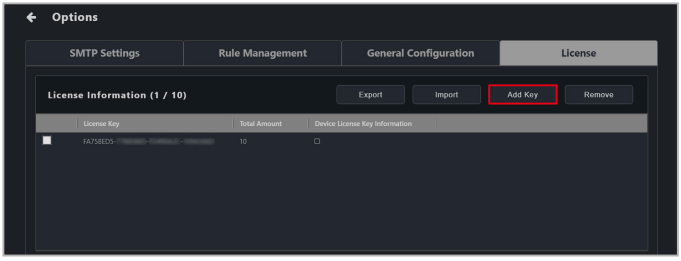
You may add or remove license keys in this menu. You may also import license information from previous versions of ACC.

Every client device you wish to deploy an agent to requires a corresponding license key.

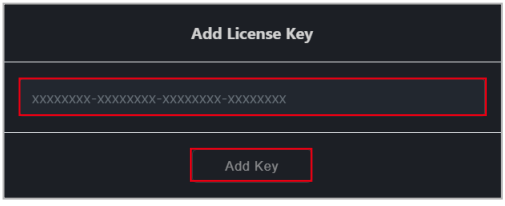


To add a single license key

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

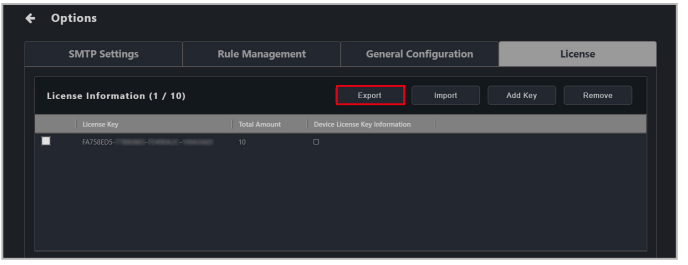


3. Key in the license key and then click on **Add Key** to register a license for a single device on ASUS Control Center Express.

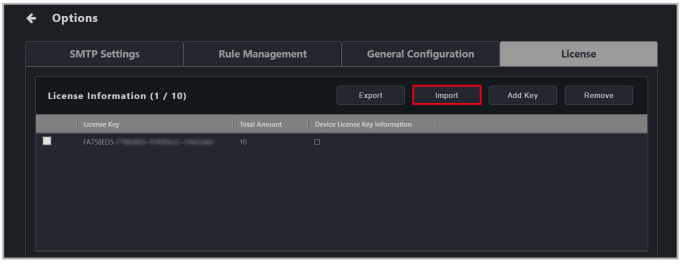


To import multiple license keys

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.



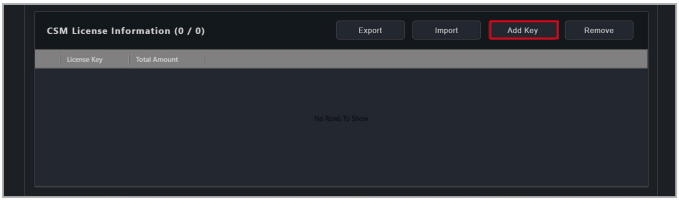
To add an ACC CSM license key

If you wish to deploy to a CSM client device, please enter the 18 character CSM license key in the CSM License Information block to activate the CSM client device. You can also use the **Setting Migrator** to migrate the CSM license keys from ACC CSM to ASUS Control Center Express. For more information on the Settings Migrator, please refer to **Chapter 6 Settings Migrator**.

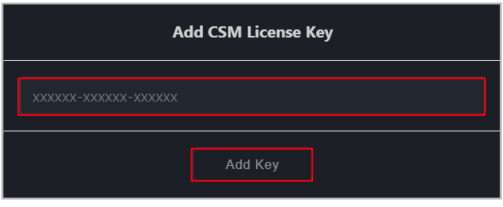
Every CSM client device you wish to deploy an agent to requires a corresponding CSM license key.

Migrated CSM product license keys will be migrated to the **CSM License Information** list.

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

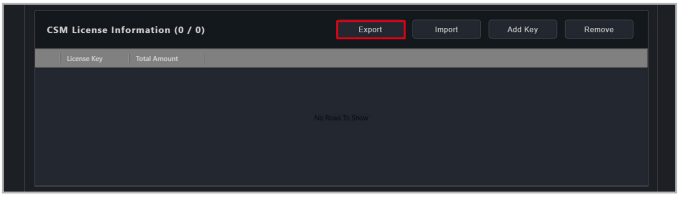


3. Key in the license key and then click on **Add Key** to register a license for a single device on ASUS Control Center Express.

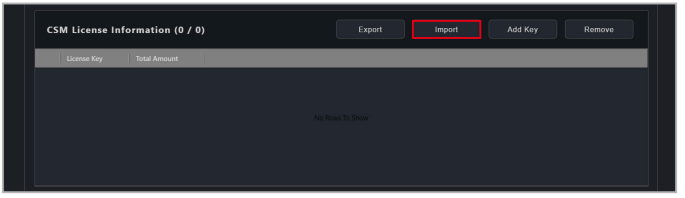


To import multiple ACC CSM license keys

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

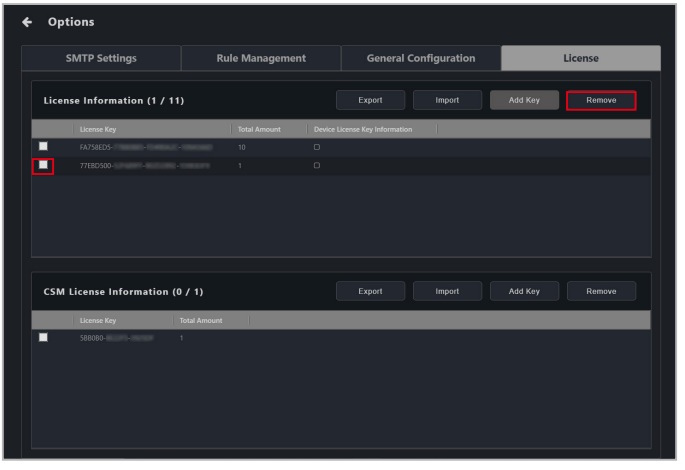


2. Click on **Import** to import your edited .csv file.



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**.



8.2 Account menu

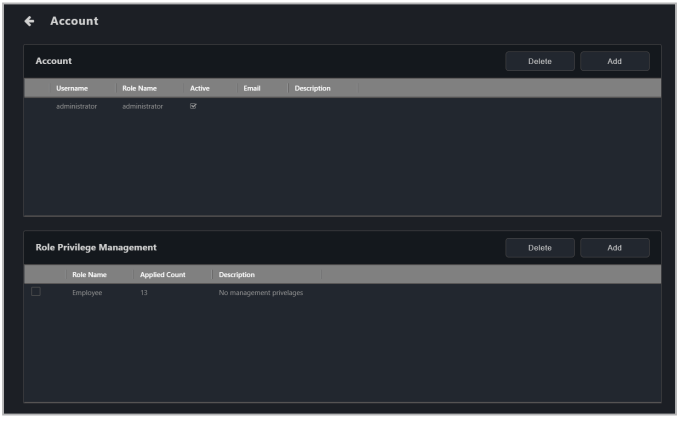
The Account menu allows you to manage accounts for ASUS Control Center Express. You can also scan a QR code for easy access to the web version of ASUS Control Center Express or provide feedback to the developers.

The information entered in this section is for reference only.

8.2.1 Account Settings

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

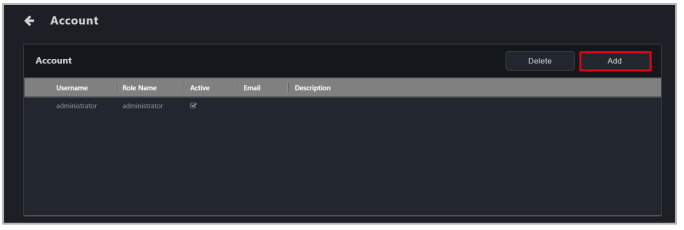
To access **Account Settings**, click on located at the top right menu bar, then select **Settings**.



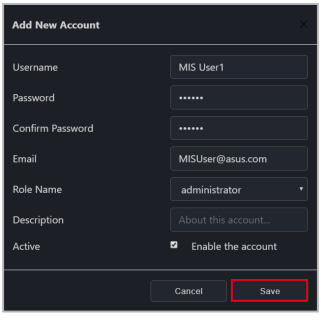
- The default account and password for ASUS Control Center Express is **administrator** and **admin** respectively.
- Change the default account and password of ASUS Control Center Express to ensure better security.

To add an account

1. Click on **Add**.



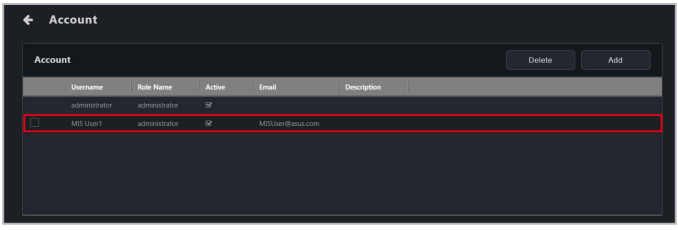
2. Enter the required information into the fields, and check **Enable the account** in the **Active** field to enable this account, then click on **Save** to add this new account.



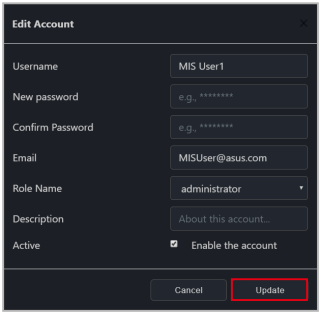
Username	Username of the account.
Password	Password for the account.
Confirm Password	Confirm the password for the account.
Email	Email associated with the account.
Role Name	The role assigned to the account will determine what privileges it has. You can select to use the preset **administrator** or **viewer** roles or add new roles. To add or modify roles, please refer to **8.2.2 Role Privilege Management**.
Description	Enter a brief description on the account.
Active	Check to enable the account.

To edit an account

1. Click on the account you wish to modify.



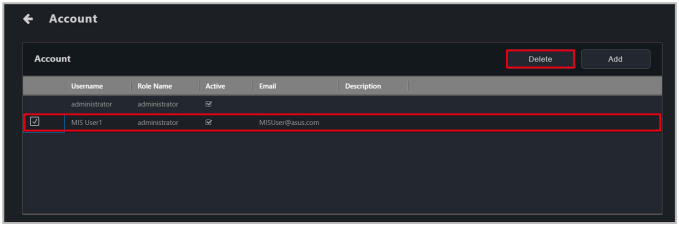
2. You may edit the account details, click on **Update** once you are finished.



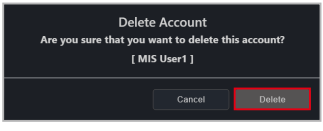
To delete an account

1. Select 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**.



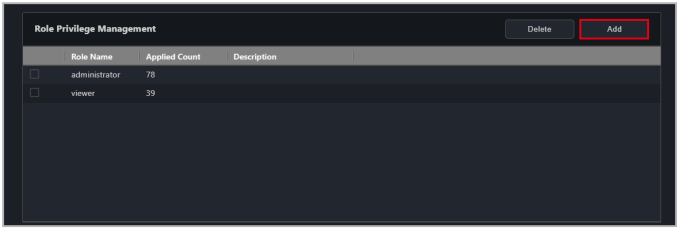
8.2.2 Role Privilege Management

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**.

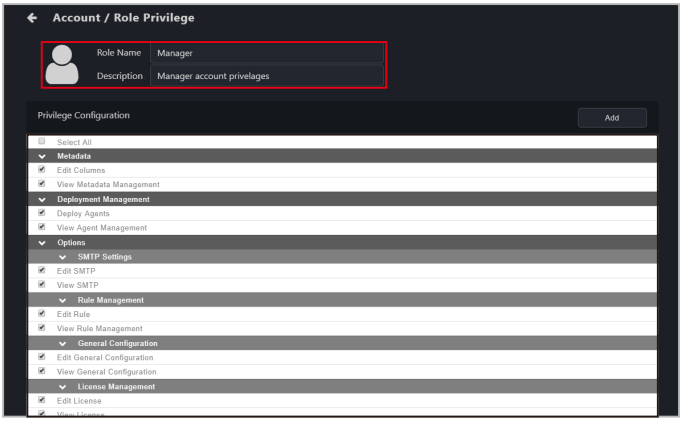
To add a new role

1. Click on **Add**.

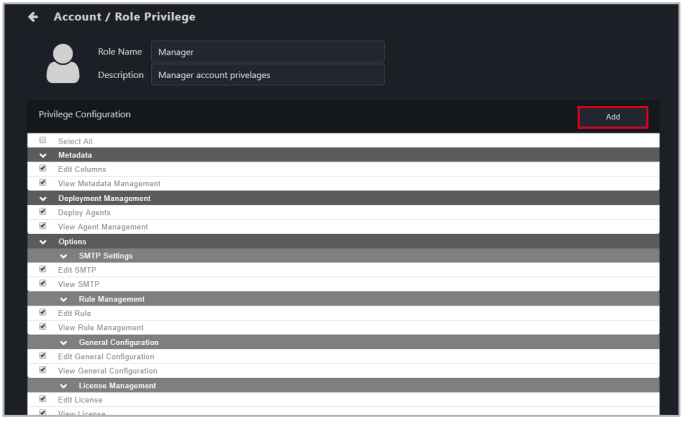


2. Enter the **Role Name** and **Description** for the role, then check the privileges you want to assign to this role in the Privilege Configuration block.

Check the **Select All** option to select all privileges; clicking on this option again will deselect all privileges.

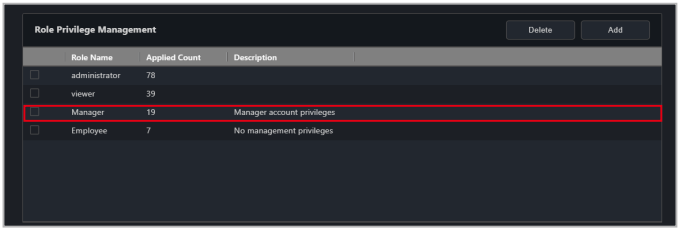


3. Click **Add** to add the new role.

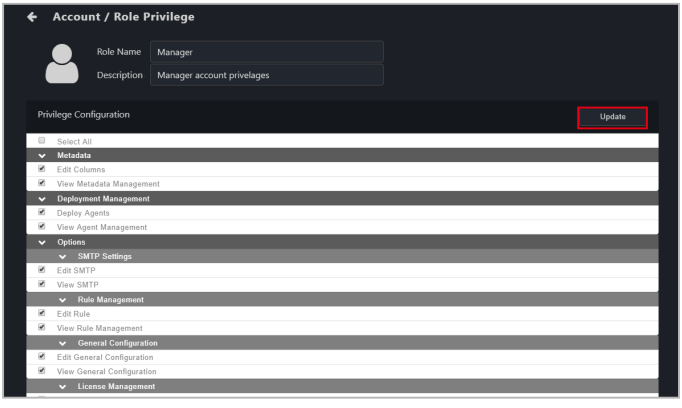


To edit a role

1. Click on the role you wish to edit.

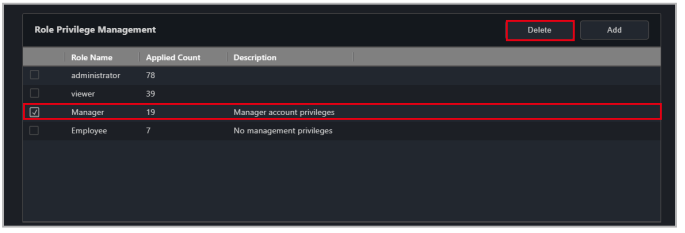


2. You may edit the **Role Name** and **Description**, or modify the **Privilege Configuration**. Click on **Update** once you are finished.



To delete a role

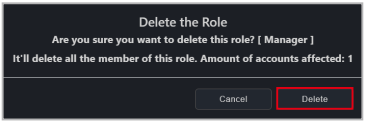
1. Select the role(s) you wish to delete, then click **Delete**.



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

The preset roles cannot be deleted.

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.



8.3 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**.

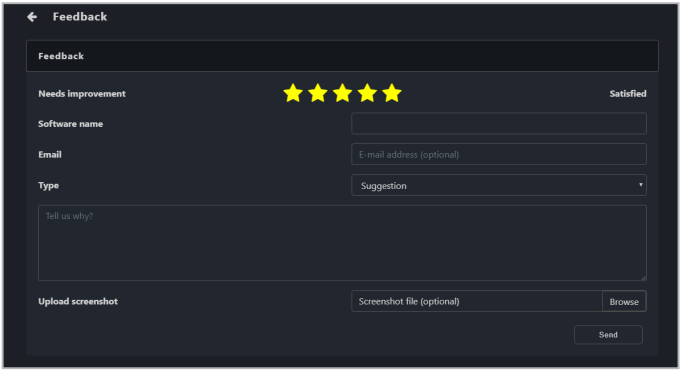
The illustration in this section is for reference only.

- The mobile device you used to scan the QR code needs to be connected to the main server's IP address.
- If the main server's network environment is a domain or a personal network, you will need to ensure your mobile device can connect to the main server (through a WiFi router or VPN) before scanning the QR code.
- If the main server's network environment includes a public network, please switch to the public network's QR code by clicking on the drop down menu before scanning the QR code.

8.4 Submit Feedback

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

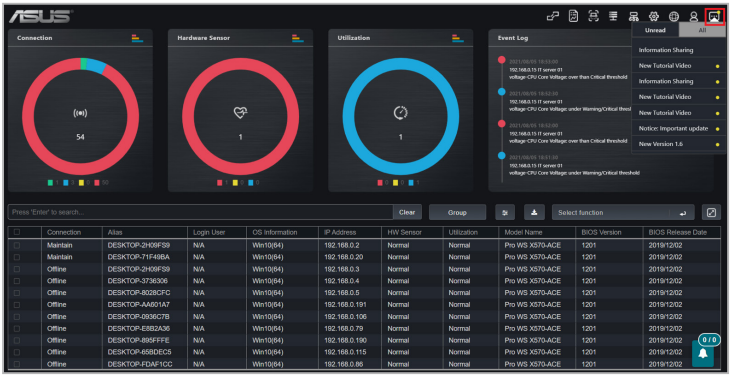
To submit feedback, click on located at the top right menu bar, then select **Feedback**.

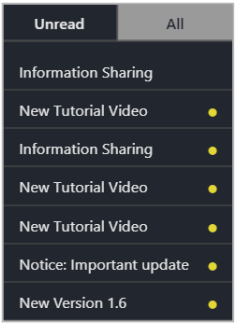


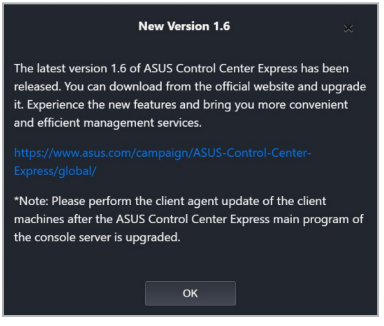
8.5 Mailbox

You can read important information and the latest updates on ASUS Control Center Express, such as the latest update released, update notifications, operation precautions, or introductions for new functions from the Mailbox.

To view the items in **Mailbox**, click on located at the top right menu bar.





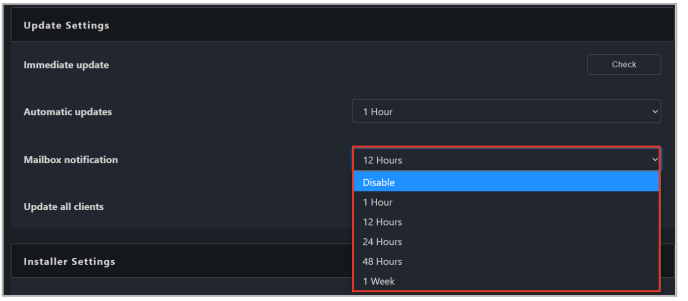


Unread	Click to view all unread messages. Clicking on a message will allow you to view the message in detail.
All	Click to view all messages. Clicking on a message will allow you to view the message in detail.

Unread messages will be marked with a yellow dot, once the message is read, the yellow dot will disappear, and the message will be removed from the **Unread** tab the next time you access the **Mailbox**.

8.5.1 Setting the Mailbox notification

1. Click on located at the top right menu bar, then select **Options** > **General Configuration**, then scroll to **Update Settings**.
2. Select how often to check for new notifications or messages and prompt mail notifications from the **Mailbox notification** drop down menu.



8.6 Backup and Restore

You can backup or restore the data and settings of your ASUS Control Center Express main server. Please follow the instructions for the type of database (MySQL or SQLite) selected during installation of ASUS Control Center Express.

- Ensure that your data and settings are backed up on a regular basis.
- It is strongly recommended to backup your data and settings before updating ASUS Control Center Express.
- For data security reasons, the backup data can only be restored on the original main server and operating system. The backup data cannot be restored if the main server is replaced or if the operating system is reinstalled.

8.6.1 Managing data and settings in MySQL databases

If you have selected MySQL during installation of ASUS Control Center Express, you can use the ACCE DBtool or manually backup and restore your data and settings.

Using the ACCE DBTool to backup, restore, or repair data and settings (recommended):

1. On the main server, go to **Start** > **ASUS Control Center Express**, right click on **ACCE DBTool**, and click on **Run as Administrator**.

- All data will be deleted during restore, repair, or reinstallation of the MySQL database. It is recommended to create a new backup before initiating these actions.
- Please wait for all actions to be completed before continuing to use ASUS Control Center Express.

2. Navigate to the install directory for ASUS Control Center Express in the **Open File** prompt and select the database file.

The ASUS Control Center Express folder path will vary depending on the path you selected during installation.

3. Set the MySQL communication port if it differs from the default setting.
4. The ACCE DBTool allows you to backup, restore, reinstall, or repair your data. Please refer to the list below for more information:
   - Backup your data: Backs up the current database.
   - Restore from backup: Restores your data from a selected backup file.
   - Reinstall database: Reinstalls the MySQL database.
   - Repair database: Checks the selected backup file for errors and attempts repairs. Data may not be recovered if it is corrupted beyond repair.

Manually backing up data and settings:

1. On the main server, please close and exit ASUS Control Center Express, then go to **Start** > **ASUS Control Center Express** and click on **Stop ACCE Service**.
2. In a command prompt with full Administrator privileges, input the following command to stop the MySQL server:

   `sc stop DataStorage`

```
C:\WINDOWS\system32>sc stop DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x5265c00
```

3. Input the following command to confirm if the MySQL server has stopped completely:

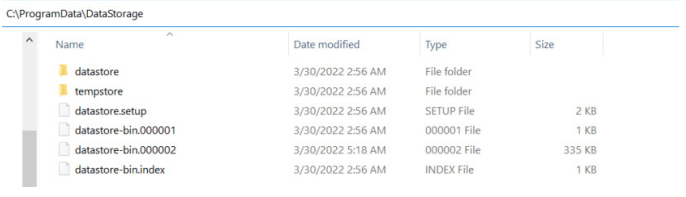
   `sc query DataStorage`

```
C:\WINDOWS\system32>sc query DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

The status of STATE should be *1 STOPPED.*

4. Backup the contents of the MySQL data storage directory to your backup location.



The default data storage directory is set to *C:\ProgramData\DataStorage.*

5. Once the files are backed up, input the following command in the command prompt to restart the MySQL server.

sc start DataStorage

```
C:\WINDOWS\system32>sc start DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x3a98
        PID                : 18652
        FLAGS              :
```

6. Go to **Start** > **ASUS Control Center Express** and click on **Start ACCE Service**.

Manually restoring data and settings:

1. On the main server, please close and exit ASUS Control Center Express, then go to **Start** > **ASUS Control Center Express** and click on **Stop ACCE Service**.
2. In a command prompt with full Administrator privileges, input the following command to stop the MySQL server:

sc stop DataStorage

```
C:\WINDOWS\system32>sc stop DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                               (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x1
        WAIT_HINT          : 0x5265c00
```

3. Input the following command to confirm if the MySQL server has stopped completely:

sc query DataStorage

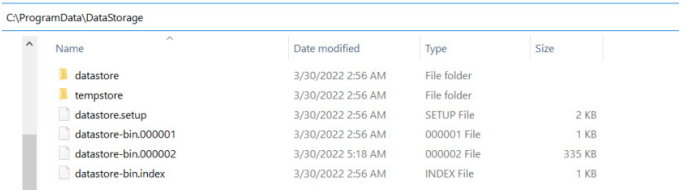
```
C:\WINDOWS\system32>sc query DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

The status of STATE should be *1 STOPPED*.

4. Copy the backup from your backup location to the MySQL data storage directory and click **Replace All**.

- The default data storage directory is set to *C:\ProgramData\DataStorage.*



5. Once the files are restored, input the following command in the command prompt to restart the MySQL server:

```
sc start DataStorage
```

```
C:\WINDOWS\system32>sc start DataStorage

SERVICE_NAME: DataStorage
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0x3a98
        PID                : 18652
        FLAGS              :
```

6. Go to **Start** > **ASUS Control Center Express** and click on **Start ACCE Service**.

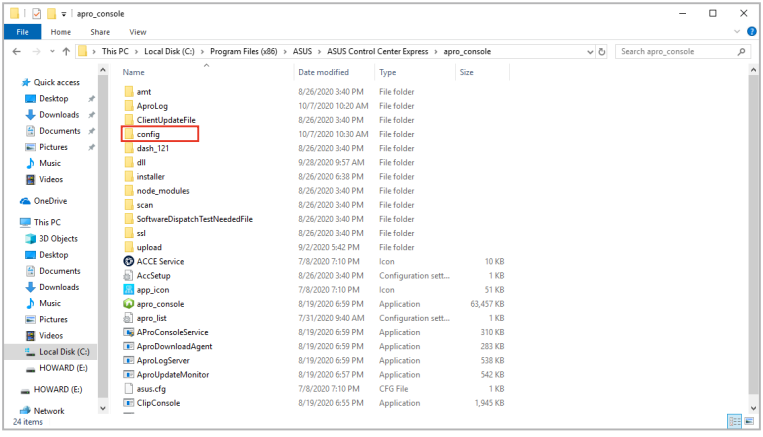
8.6.2 Backing up data and settings in SQLite databases

If you have selected SQLite during installation of ASUS Control Center Express, please follow the below instructions to back up your data:

1. Locate the folder your ASUS Control Center Express is installed to on your main server.

- The default folder is set to *C:\Program Files (x86)\ASUS\ASUS Control Center Express*.
- The ASUS Control Center Express folder path will vary depending on the path you selected during installation.

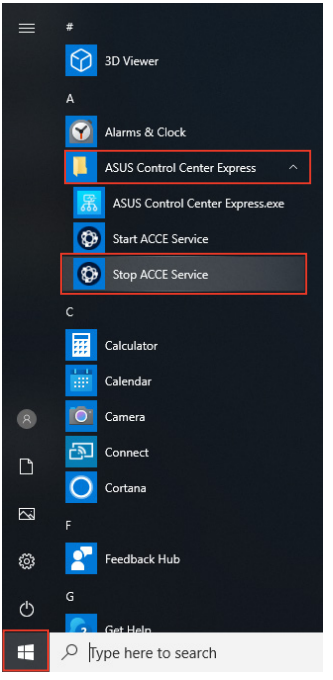
2. Navigate to the **apro_console** folder.
3. Backup the **config** folder, including all files in the **config** folder to your backup location.



8.6.3 Restoring data and settings in SQLite databases

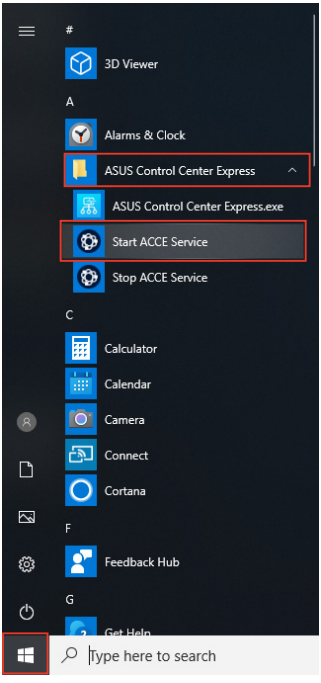
If you have selected SQLite during installation of ASUS Control Center Express, please follow the below instructions to restore your data. We recommend backing up your current ASUS Control Center Express data and settings before restoring the settings and data of a previous backup. For more details about backing up your ASUS Control Center Express data and settings, please refer to **8.6.1 Backing up data and settings in SQLite databases**.

1. If your ASUS Control Center Express is currently in operation or in use, please close and exit ASUS Control Center Express.
2. On the main server, go to **Start** > **ASUS Control Center Express**, and click on **Stop ACCE Service**.



3. Locate the backup file (**config**) you would like to restore and copy it and all the files in the backup folder.

4. Navigate to the folder your ASUS Control Center Express is installed to on your main server, then open the **apro_console** folder.

- The default folder is set to *C:\Program Files (x86)\ASUS\ASUS Control Center Express*.
- The ASUS Control Center Express folder path will vary depending on the path you selected during installation.

5. Replace the **config** folder and all the files in it by pasting the copied **config** folder and all the files in it from step 3 into the **apro_console** folder.
6. Once the folder and files have been successfully replaced, go to **Start** > **ASUS Control Center Express**, and click on **Start ACCE Service**.