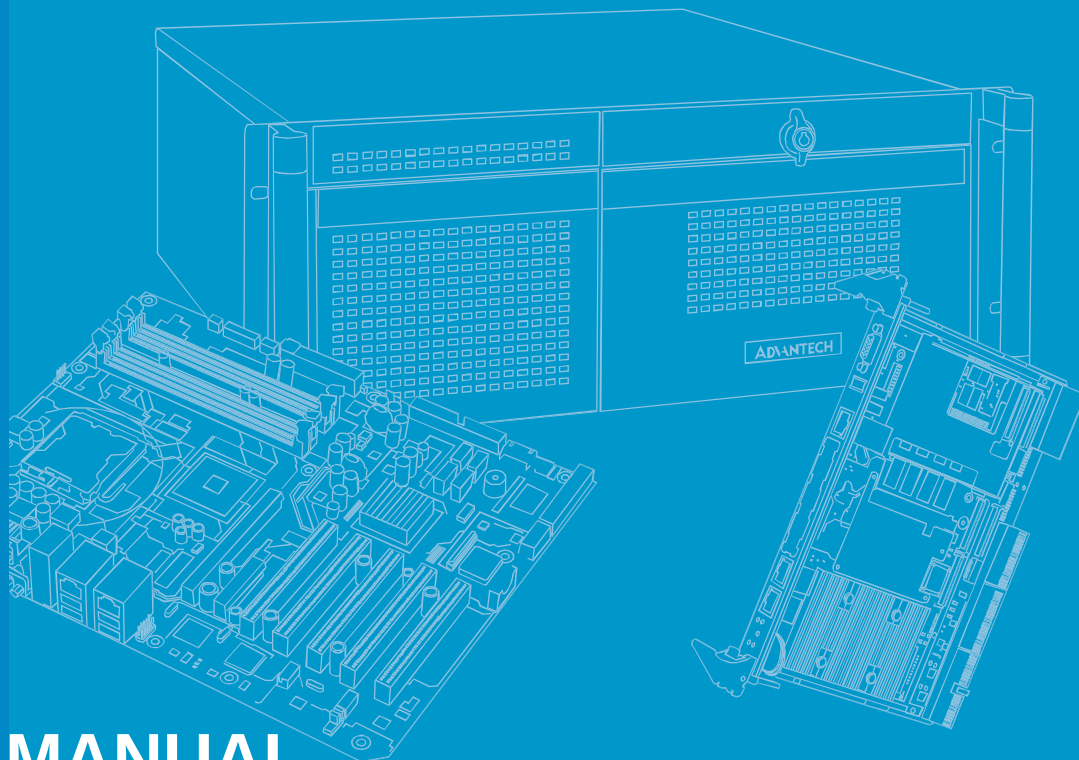




USER MANUAL

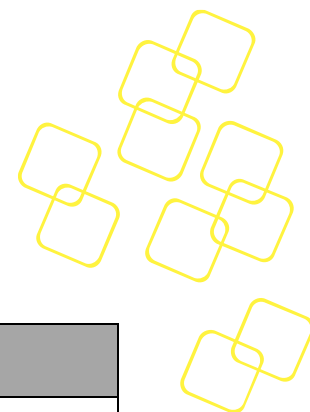
ADVANTECH Node Explorer

Edition 8

Apr. 2023

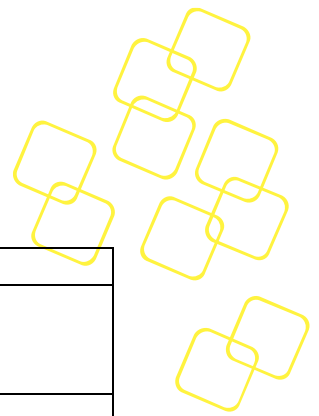
ADVANTECH

Enabling an Intelligent Planet



Revision History

Document Release Date	Document Revision	Software Revision and Modifications
4/5/2023	Edition 8.0	Base on nodeexp-1.25.2 remove "booting" status in power status - 3.5.1 System Power Control
02/17/2023	Edition 7.0	Base on nodeexp-1.25.1 1. Add Force First-Time Login Password Change mechanism in chapter 2 Accessing Node Explorer (Nodeexp-1.24.0) 2. 3.1 Tool Bar - toolbar image update 3. 3.3.2 Sensor Status : support sensor refresh automatically every 10 seconds 4. 3.3.3 Event Log: Web SEL Alert history add more detail clarification. 5. 3.4.3.9 The Session Timeout Tab: add the notes for the range restriction of session timeout. 6. 3.4.5.2 Channel Policy tab 7. Add new 3.4.6 RAID Management Add more description on the 8. Front Panel. Update the description of System LED (Chassis Alarm Status LED) 9. Panel page. Add description for Chassis Alarm Status tab 10. iKVM functionality : iKVM frame rate 11. 3.5.4 Remote Serial Console : close current serial console session dialog
05/07/2021	Edition 6.0	Official release Base on nodeexp-1.22.2
04/21/2021	Edition 5.5	Base on nodeexp-1.22.2 1. LDAP Configurations - extra configurations - LDAP 2. RADIUS Configurations - extra configurations - RADIUS 3. VNC Service Configurations - extra configurations – VNC Service 4. Remote syslog configurations - extra configurations - remote syslog 5. Added Load / Save BIOS configurations in maintenance - configurations 6. Supports output BMC debug log to Syslog configurations - maintenance - BMC debug log 7. Host Screenshot configurations - maintenance - host screenshot 8. BIOS setup



		remote control - BIOS setup
04/14/2020	Edition 5.3	Based on noteexp-1.20.5 1. Include BMC debug log in maintenance page. 2. Refine the statements in remote storage.
03/30/2020	Edition 5.0	Based on noteexp-1.20.5 1. BIOS post code tool bar, remote control - system power control 2. IPv6 default gateway configurations - network 3. User permission (PAM module) configurations - extra configurations - user management - edit user 4. CA certificate chain (customized feature) configurations - extra configurations - SSL certificate - upload SSL certificate 5. Firewall (port, IPv4, IPv6) (customized feature) configurations - extra configurations - firewall 6. BMC debug download (customized feature) configuration - maintenance - BMC debug log 7. SSH key management (customized feature) configuration - extra configurations - SSH key management 8. Session timeout configurations - extra configurations – session timeout 9. Open remote serial console in new tab directly 10.Supports display of instant sensor reading
02/28/2019	Edition 4.0	Based on noteexp-1.18.8 PEF destination dialog: makes it easier to select and copy text from replace word list System power control • Show BIOS POST code in tool bar • BIOS Boot Option : Add BIOS support information Remote storage • One-click connect/disconnect
11/23/2018	Edition 3.0	Based on noteexp-1.18.1 1. Added some useful notes 2. User experience improvement 3. New functionalities - Supports simplified/traditional Chinese - Information for multi-node system - Maintenance page • Loads default/download/upload configuration with encryption • Firmware upgrade check Remote Control will be released in noteexp-1.19.0 • More BIOS boot options in system power control • Front panel • Remote serial console



09/30/2018	Edition 2.0	New features in noteexp-1.17.4 - System health : advanced inventory, web alert - Configuration : advanced setting of alerts, VLAN Setting in network, NTP setting, user management, network – Ipv6 - Extra configuration: Time sync, firmware upgrade, SNMP - Remote storage Modify remote control – iKVM, login session timeout and limitation Adjust Advantech web layout, information in sensor status Login timeout is 1 week
09/29/2017	Edition 1.0	1 st official release based on noteexp-1.15.0

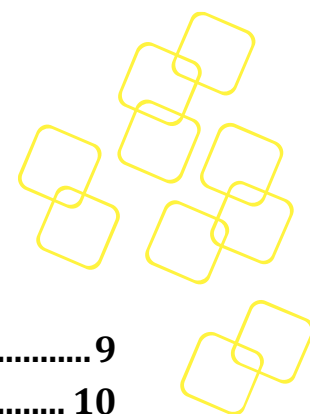
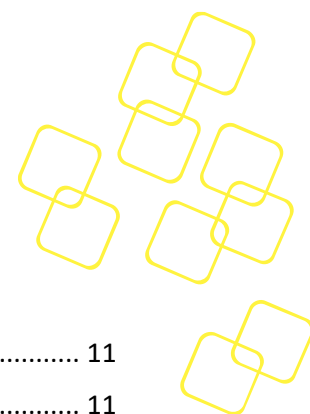


TABLE OF CONTENTS

1. NODE EXPLORER	9
2. ACCESSING NODE EXPLORER	10
3. WEB PAGE INDEX	13
3.1 TOOL BAR.....	13
3.2 OVERVIEW.....	14
3.3 SYSTEM HEALTH.....	15
3.3.1 Advanced Inventory.....	15
3.3.2 Sensor Status.....	15
3.3.3 Event Log	18
3.3.4 Web Alert.....	20
3.3.5 Session	21
3.4 CONFIGURATION	22
3.4.1 Alerts.....	22
3.4.2 Network.....	27
3.4.3 Extra Configurations.....	29
3.4.4 Maintenance	44
3.4.5 BMC Interface control	58
3.4.6 RAID Management.....	59
3.5 REMOTE CONTROL SESSION	64
3.5.1 System Power Control.....	64
3.5.2 Front Panel.....	68
3.5.3 iKVM Redirection	70
3.5.4 Remote Serial Console	82
3.5.5 BIOS Setup	87
4. TIPS AND TROUBLESHOOTING.....	89
4.1 WEB PAGE TIMEOUT.....	89
4.2 SESSION LIMITATIONS.....	89
4.3 SECURITY WARNING MESSAGE	89
4.4 LOG OUT	90



LIST OF FIGURES

Figure 1: Login Page.....	11
Figure 2: Change password for First Time Login	11
Figure 3: Main Page after a Successful Login	12
Figure 4: Overview Page	14
Figure 5: Advanced Inventory page.....	15
Figure 6: Sensor Status Page	16
Figure 7: Sensor Status Indicating Alarm Levels and Crossed Thresholds	16
Figure 8: Plotted-Out History Curve for Downloading	17
Figure 9: Event Log Page.....	18
Figure 10: Save Details as a .Json File.....	19
Figure 11: Web Alert Page.....	20
Figure 12: Details in Event Log	20
Figure 13: Session List Page.....	21
Figure 14: Session details	21
Figure 15: Alerts Page.....	22
Figure 16: Alert Setting Modification (Event Filter Table).....	23
Figure 17: Alert Setting Modification (Alert Policy Table)	24
Figure 18: Destinations Settings (PET Trap)	25
Figure 19: Destinations Settings (SMTP Email).....	25
Figure 20: Destinations Settings (SMTP Email).....	26
Figure 21: Network Page	27
Figure 22: IPv6 information per LAN Interface.....	28
Figure 23: User Management Tab	29
Figure 24: LDAP Tab (Authentication via Remote LDAP Server)	30
Figure 25 RADIUS Tab (Authentication via Remote RADIUS Server).....	31
Figure 26: Time Tab (System Time and NTP Settings)	32
Figure 27: Time Zone Successfully Set.....	32
Figure 28: Offsetting the System Time	33
Figure 29: NTP Settings.....	34
Figure 30: SSL Certificate Tab	35
Figure 31: Upload SSL	36
Figure 32: SSH Key Management Tab.....	37

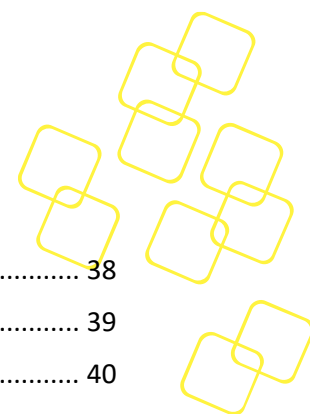


Figure 33: SMTP Tab.....	38
Figure 34: SNMP Tab	39
Figure 35: Session Timeout Tab.....	40
Figure 36: Session Timeout Success	40
Figure 37: Add Port Firewall	41
Figure 38: Add IPv4/IPv6 Address Firewall.....	41
Figure 39: VNC Service Tab.....	42
Figure 40: TightVNC Viewer.....	42
Figure 41: Remote Syslog Tab	43
Figure 42: Maintenance page.....	44
Figure 43: The Version Tab	44
Figure 44: More Version Information on Other FW/SW	45
Figure 45: The Configuration Tab	45
Figure 46: Enter Your Password for Confirmation	46
Figure 47: Re-confirm Loading the Default Settings	46
Figure 48: Default Settings Successfully Loaded	47
Figure 49: Encryption Key Popup	48
Figure 50: Check the Always Allow Button to Download Multiple File.....	48
Figure 51: Enter Login Password for Confirmation	49
Figure 52: Select File then Press Next to Upload Configuration File.....	49
Figure 53: Uploading the Configuration File	50
Figure 54: Enter the Encryption Key.....	51
Figure 55: Confirmation Failed	51
Figure 56: Confirmation of the Applied Update.....	51
Figure 57: Applying the Configuration	52
Figure 58: Configuration Successfully Applied	52
Figure 59: Firmware Upgrade Tab.....	53
Figure 60: Firmware Image Uploading to the BMC.....	53
Figure 61: Confirmation of Upgrade.....	54
Figure 62: Error Message during Upgrade	54
Figure 63: Firmware Upgrade in Progress	55
Figure 64: Firmware Upgrade Successful	55
Figure 65: BMC Debug Log	56
Figure 66: Check debug.archive	56

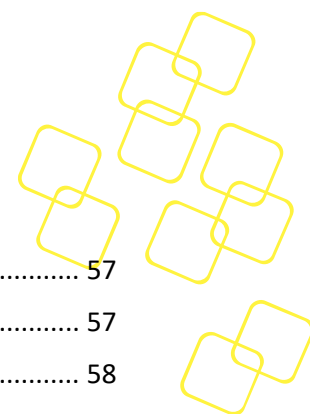


Figure 67: The Host Screenshot Tab.....	57
Figure 68: Reviewed Screenshot by One Click	57
Figure 69: BMC Interface Control.....	58
Figure 70: BMC Channel Policy.....	58
Figure 71: Configuration - RAID Management –RAID INFO Page.....	59
Figure 72: Configuration - RAID Management –RAID CONFIG Page	60
Figure 73: RAID Management - RAID CONFIG – Create RAID	61
Figure 74: RAID CONFIG – Delete RAID	61
Figure 75: RAID CONFIG – Delete RAID – Select Virtual Drive	62
Figure 76: : RAID CONFIG – Clear Configuration	62
Figure 77: RAID CONFIG – Hot Spare Control.....	63
Figure 78: RAID CONFIG – Locate Drive.....	63
Figure 79: Server Power Control Page.....	64
Figure 80: BIOS POST Code History dialog.....	64
Figure 81: BIOS Boot Options are Saved	65
Figure 82: Server Power Action Countdown	66
Figure 83: Front Panel Page.....	68
Figure 84: Chassis Identification tab	68
Figure 85: Chassis Alarm Status.....	69
Figure 86: Redirecting.....	70
Figure 87: Pop-ups Were Blocked On This Page.	70
Figure 88: iKVM Screenshot Example: Graphic UI.....	70
Figure 89: iKVM Redirection Settings Buttons	72
Figure 90: iKVM is Disconnected Because of Timeout or Shutdown	72
Figure 91: Remote Storage functionality.....	73
Figure 92: Remote Storage Connected via SMB.....	74
Figure 93: Remote Storage (SMB) Successfully Mounted	75
Figure 94: Remote Storage (SMB) Mount Failed.....	75
Figure 95: Remote Storage (SMB) Disconnected	76
Figure 96: The Remote Image (SMB) is Connected	76
Figure 97: Remote Storage (Web)	77
Figure 98: Selecting an Image File for Remote Storage (Web)	77
Figure 99: Virtual Drive Successfully Mounted via Remote Storage (Web)	78
Figure 100: The Remote Image (Web) is provided by another Client.....	78

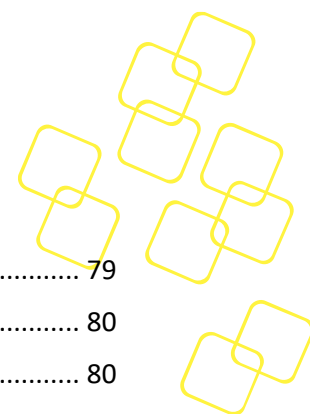
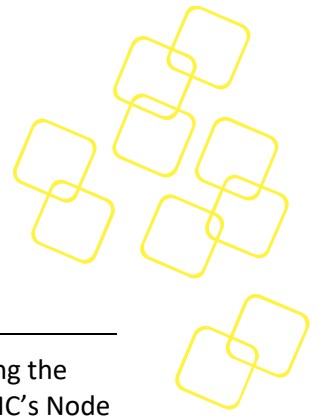


Figure 101: Virtual Drive Disconnected	79
Figure 102: Restarting x86 Payload and Entering BIOS Setup Menu	80
Figure 103: Restarting x86 Payload from Tool Bar and Entering BIOS Setup Menu	80
Figure 104: Select Remote Storage in BIOS Setup Menu	81
Figure 105: Serial Console in BIOS Setup Menu	82
Figure 106: Enable Serial Console in BIOS Setup Menu	83
Figure 107: Save Serial Console Configuration in the BIOS Setup Menu	83
Figure 108: Open Serial Console in Remote Serial Console Page.....	84
Figure 109: Redirecting.....	84
Figure 110: Remote Serial Console Page	85
Figure 111: Disable UART Redirection.....	85
Figure 112: Close Current Sessions	86
Figure 113: Open BIOS Setup Page.....	87
Figure 114: Asked for Username and Password in BIOS Setup Page	87
Figure 115: BIOS Setup Page (BIOS Setup Web Utility)	88
Figure 116: Security Warning Message	89
Figure 117: Log Out	90



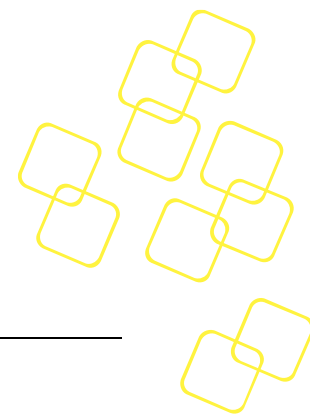
1. NODE EXPLORER

Node Explorer is a web-based interface that provides a simple approach for accessing the BMC in order to manage and monitor the system's health status. By default, the BMC's Node Explorer is enabled for Advantech's Advanced Platform Management in Advantech's server series.

This node explorer (nodeexp) version can be checked in the version tab referred to section 3.4.4.1.

If you cannot find the information you are looking for or need more detailed information on a specific topic, please refer to the list of additional documents and other sources of information below. Please contact your Advantech representative if you need help obtaining these documents or still cannot find what you are looking for.

- *Intelligent Platform Management Interface Specification*, Version 2.0, Revision 1.1, October 1, 2013-E7 April 21, 2015.
- *IPMI – Platform Management FRU Information Storage Definition*, V1.0, Document Revision 1.1, September 27, 1999.
- *IPMI - Platform Event Trap Format Specification V1.0*, Document Revision 1.0, December 7, 1998.
- Information on Intel CPUs, chipsets and NIC silicon can be found at www.intel.com
- Advantech Product User Manual and platform management User Manual



2. ACCESSING NODE EXPLORER

Perform the following steps to access Node Explorer:

- Configure the BMC's IP as desired (by default, it is set as static address 0.0.0.0). For more details, please refer to the *Advantech Advanced Platform Management User Guide* of each product.
- Configure the IP of the remote computer and ensure that the remote computer's IP and the BMC's IP are located in the same subnet. On the remote computer, start a web browser (Google Chrome is used in our example) to access the BMC secure website.
Type ***https://<BMC IP>/nodeexp*** in the address bar, press **Enter** to go to the Node Explorer login page. Node Explorer can be accessed via both IPv4 and IPv6 addresses.
- Node Explorer comes with a default SSL Certificate; the browser might show a warning about an invalid certificate, which must be accepted before Node Explorer can be accessed.

The following web browsers have been verified with Node Explorer:

- Firefox versions 45.0.1 or later
- Chrome versions 49.0.2623.87 or later
- Safari versions 9.0.5 or later

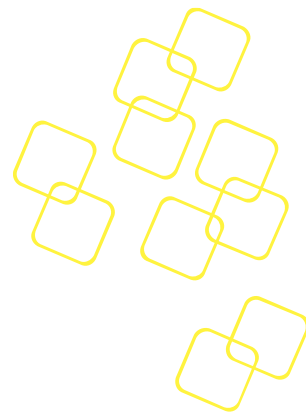


Figure 1: Login Page

- Use the default BMC LAN channel credentials (case-sensitive) for login:

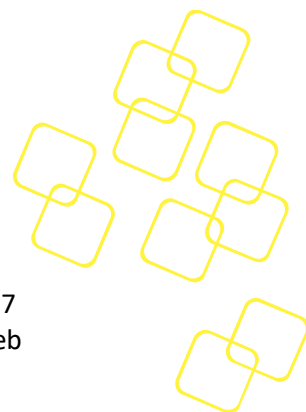
User name: administrator

Password: advantech

In products, where Force Password Change (available after nodeexp-1.25.0) is enabled, a change password dialog will pop up to ask the user to change a new password as in Figure 2 when a user logs in with default password for the **first time**.

Note: The new password **cannot** be identical to the default password.

Figure 2: Change password for First Time Login



Please note that it will require administrator privileges in order to access all the functionalities of the web interface. The login session will timeout after 3600 x 24 x 7 seconds (1 week). In addition, you will need to login again after the IP address or web browser has been changed, browser data cleared, or the BMC rebooted.

Upon successful login, the web interface overview will appear as shown in Figure 3.
Note: For security reasons, please change the user credentials after the first login.

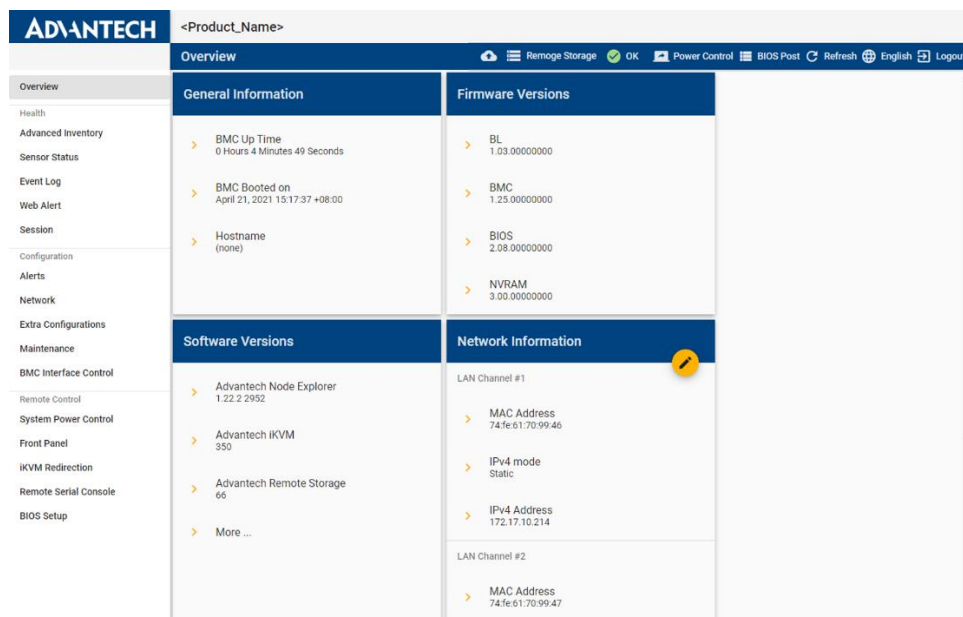
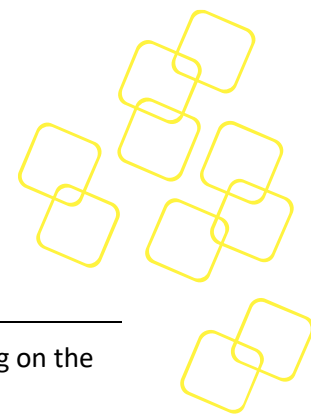


Figure 3: Main Page after a Successful Login

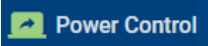
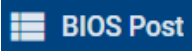
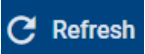
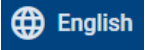
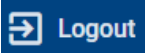


3. WEB PAGE INDEX

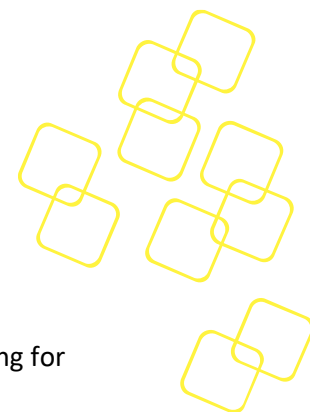
The menu structure of Node Explorer might differ between revisions and depending on the supported functionality.

3.1 Tool Bar

There are 6 icons located on the top-right corner of the web interface—same for all pages.

	Alert status (refer to Figure 7 for detailed definition). Clicking the icon will take you to the sensor status page. (Refer to 3.3.2 Sensor Status).
	Host power status. The power status will be also updated by clicking the refresh button or when navigating to a different page. Clicking the icon will let you use the Power Control option, which is the same as the System Power Control page (see 3.5.1 System Power Control for more details).
	Shortcut of BIOS POST code history. The dialog box for the BIOS POST code will be pop out as Figure 80: BIOS POST Code History dialog in chapter 3.5.1 System Power Control.
	Refreshes 3.3.2 Sensor Status , 3.3.4 Web Alert , Power Status and BIOS Post Code in 3.5.1 System Power Control page.
	Language selection supporting English, Simplified Chinese, Traditional Chinese.
	Log out.

Note: These icons will only refresh when a user clicks on the refresh button, a new page is navigated, or the system power is changed, instead of refreshing automatically all the time.



3.2 Overview

General information of the BMC uptime and BMC boot-up time, firmware version (Bootloader, BMC, BIOS, FPGA, BIOS, NVRAM), software version, and network setting for each LAN channel.

The **Network Information** box provides quick access to the network configuration page.

Edit network configuration

ADVANTECH
<Product_Name>

Overview
Remoge Storage
OK
Power Control
BIOS Post
Refresh
English
Logout

Overview
Health
Advanced Inventory
Sensor Status
Event Log
Web Alert
Session
Configuration
Alerts
Network
Extra Configurations
Maintenance
BMC Interface Control
Remote Control
System Power Control
Front Panel
iKVM Redirection
Remote Serial Console
BIOS Setup

General Information
Firmware Versions

BMC Up Time
2 Hours 2 Minutes 51 Seconds
BMC Booted on
April 21, 2021 11:29:42 +08:00
Hostname
(none)

BL
1.03.00000000
BMC
1.25.00000000
BIOS
2.08.00000000
NVRAM
3.00.00000000

Software Versions
Network Information

Advantech Node Explorer
1.22.2.2952
Advantech iKVM
350
Advantech Remote Storage
66
More ...

LAN Channel #1
MAC Address
74:fe:61:70:99:46
IPv4 mode
Static
IPv4 Address
172.17.10.214

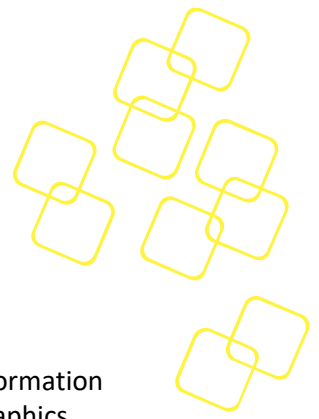
LAN Channel #2
MAC Address
74:fe:61:70:99:47
IPv4 mode
Static

Figure 4: Overview Page

On the **Overview** page, the hostname, address information and the node name at the top-right side will be only visible in multi-node systems for node identification.

Copyright 2023. All rights reserved. Advantech Co. Ltd.

Page 14



3.3 System Health

3.3.1 Advanced Inventory

The **Health - Advanced Inventory** page provides a simple way of accessing basic information on the system hardware, including processors, memory, network adapters, fans, graphics adapters, and other devices (e.g., disk drives).

Please note that the inventory of CPU, memory, storage, network, PSU, cooling, and FRU need to be supported with the appropriate BIOS.

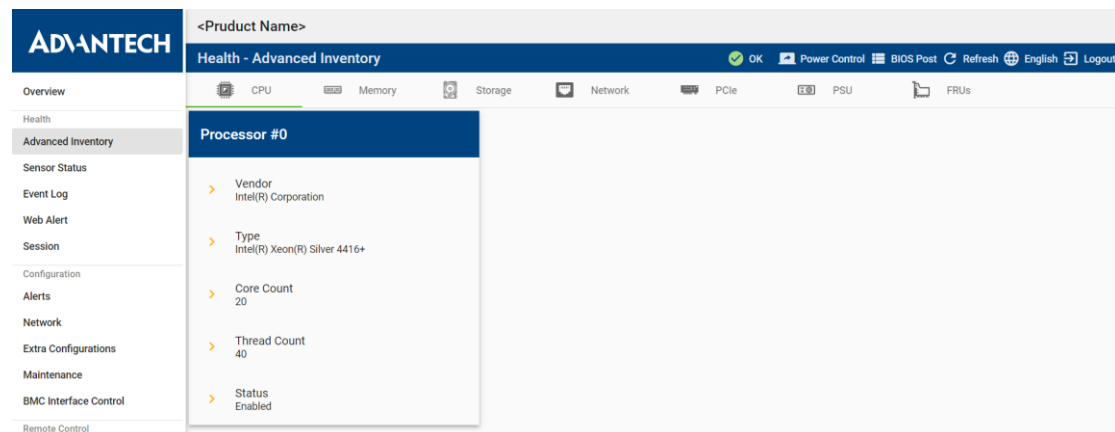


Figure 5: Advanced Inventory page

3.3.2 Sensor Status

The **Sensor Status** page provides the latest sensor readings of all system sensors.

The drop down menu located at the top of the sensor list can be used to filter preferred sensor types:

- Threshold-based All threshold-based sensors
- Temperature sensors Lists only temperature sensors
- Voltage sensors Lists only voltage sensors
- Fan sensors Lists only fan sensors
- All Lists all sensors

The instant reading for each sensor as shown in Figure 6: Sensor Status Page will be displayed beside the sensor name after nodeexp-1.20.0.

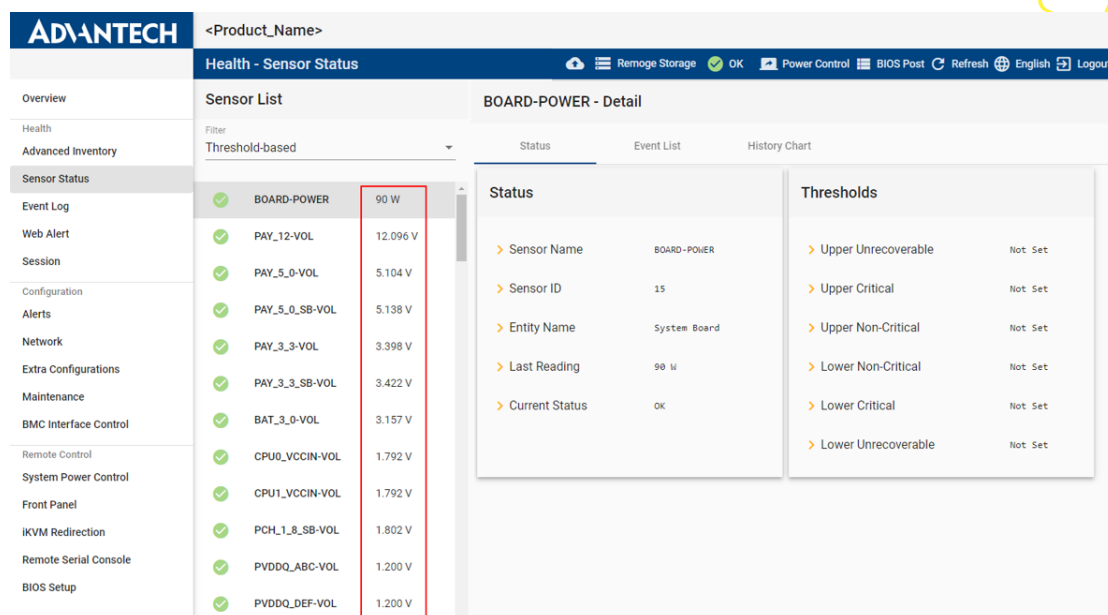


Figure 6: Sensor Status Page

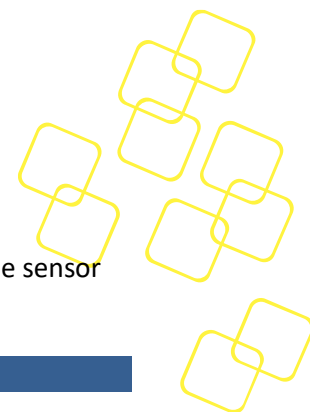
The color and icon of the sensor status indicates the alarm level and crossed thresholds, as shown in Figure 7.

- ✓ ok Sensor reading is normal
- ! warning Sensor reading has reached the upper/lower non-critical threshold
- ! major Sensor reading has reached the upper/lower critical threshold
- ! critical Sensor reading has reached the upper/lower non-recoverable threshold
- ? unknown No sensor reading

*Note: The sensor readings will be refreshed automatically every 10 seconds. Reselecting the **Sensor Status** page can also get the latest readings.*

Thresholds (3.1)	Sensor status indicator
Upper non-recoverable	! critical
Upper Critical	! major
Upper Non-Critical	! warning
Lower Non-Critical	✓ ok
Lower Critical	! warning
Lower non-recoverable	! major
	! critical

Figure 7: Sensor Status Indicating Alarm Levels and Crossed Thresholds



After a sensor has been selected from the sensor list on the left side of the page, the sensor information will be shown in three tabs.

Status

- **Status** Sensor name, ID, entity, last reading, current status
- **Thresholds** The thresholds are defined according to IPMI and BMC spec

Event List

Shows all logged events issued by the selected sensor

History chart

On the right of this page, the last 150 min (one reading per 5 min x 30) of historic sensor readings for a single threshold-based sensor are presented as a curve. There will be no historic curve for discrete sensors because they do not report a numeric reading. Clicking **Open** in New Window icon  on the top-right side of the history chart, will plot the curve, which can be downloaded as a .PNG file (see Figure 8).

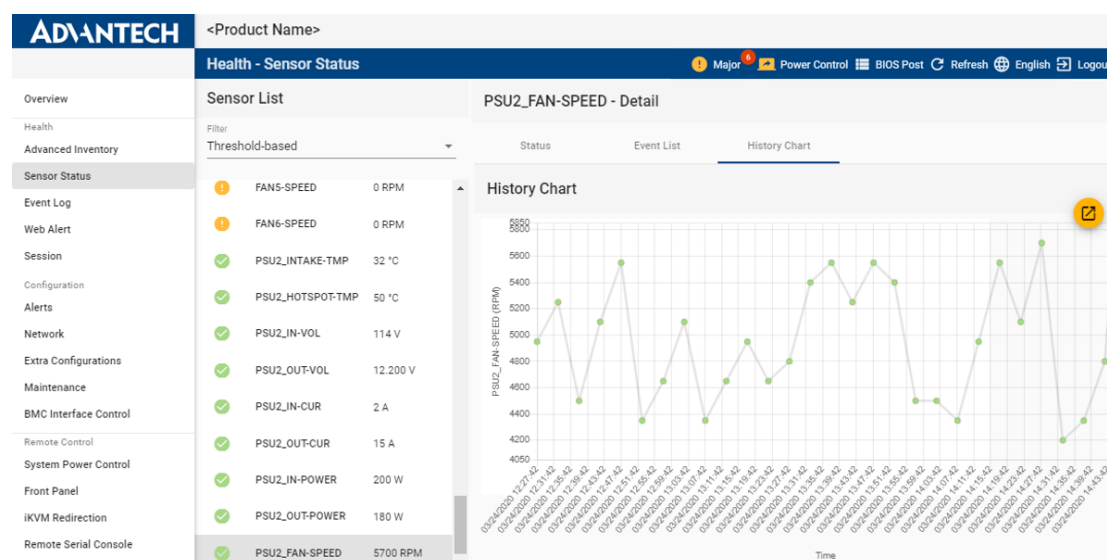
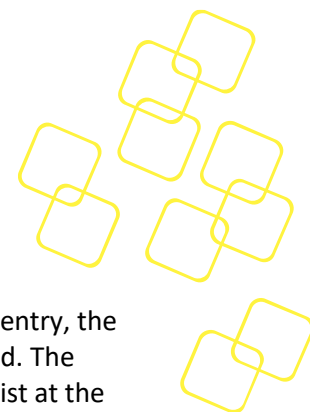


Figure 8: Plotted-Out History Curve for Downloading



3.3.3 Event Log

The **Event Log** page shows the system event log (SEL) of the platform. For each SEL entry, the event ID, time stamp, sensor name, sensor type, and event description are displayed. The number of displayed events per page can be adjusted by using the **Items per page** list at the bottom-right corner of the page.

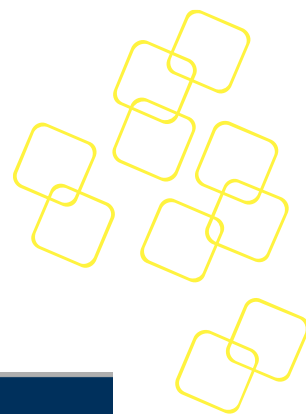
ID	Timestamp	Sensor	Type	Description
1	09/28/2020 03:05:06	INTEGRITY	OEM	assert: BMC FW, Update, Successful
2	09/28/2020 03:05:06	VERSION_CHANGE	Version Change	assert: Firmware or software change detected with associated entity, BMC FW
3	09/28/2020 03:05:06	INTEGRITY	OEM	assert: BMC FW, Boot, Successful
4	09/28/2020 03:05:07	PSU1	Power Supply	deassert: Power supply input lost
5	09/28/2020 03:05:07	PSU2	Power Supply	assert: Presence detected
6	09/28/2020 03:05:07	PSU2	Power Supply	deassert: Power supply input lost
7	09/28/2020 08:20:14	INTEGRITY	OEM	assert: BMC FW, Update, Successful
8	09/28/2020 08:20:14	VERSION_CHANGE	Version Change	assert: Firmware or software change detected with associated entity, BMC FW
9	09/28/2020 08:20:14	INTEGRITY	OEM	assert: BMC FW, Boot, Successful
10	09/28/2020 08:20:15	PSU1	Power Supply	deassert: Power supply input lost

Figure 9: Event Log Page

Users can jump to next/previous/first/last page by clicking the navigation icons at bottom-right corner of the page.

More operations can be opened by clicking the **More** options icon

- Refresh the event list
- Clear all events
- Download the event list as .csv file



Select an event to get more details (e.g., SEL name, sensor type, event code) and to download the details as “JSON-File sel_<ID>.json”

Health - Event Log

System Event Log

Type Filter

ID	Timestamp		
2142	04/05/2018 06:5		
2143	04/05/2018 06:5		
2144	04/05/2018 06:5		
2145	04/05/2018 06:5		
2146	04/05/2018 06:5		
2147	04/05/2018 06:5		
2148	04/05/2018 06:5		
2149	04/05/2018 06:5		
2150	04/05/2018 06:54:03	C0_DIMM_D1_PRSENT	Entity Presence
2151	04/05/2018 06:54:03	C0_DIMM_D2_PRSENT	Entity Presence

Sensor Event Detail

> SEL ID

2144

> Sensor Name

INTEGRITY

> Timestamp

April 5, 2018 06:54:02 +02:00

> Sensor Type

OEM

> Sensor Type Code

192

> Event Code

0x70

> Data Code

0xa0 0x01 0x90

> Description

Assert: BMC FW, Power, Successful, INTEGRITY

Download

Close

Figure 10: Save Details as a .Json File



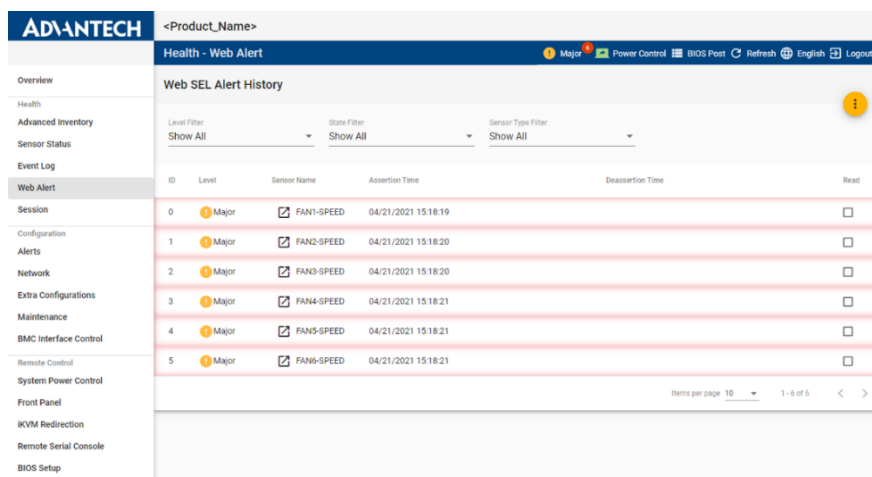
3.3.4 Web Alert

The web alert notification history of the platform is shown on this page. The displayed alerts can be filtered by using the **Level Filter** (critical, major, warning), **State Filter** (all, checked, new), and **Sensor Type Filter**. For each entry, the event ID, alarm level (see Figure 11), sensor name, assertion time, desertion time, and read status are shown

Note: Web SEL History page only shows **threshold-related** events.

More operations can be opened by clicking the **More** options icon. 

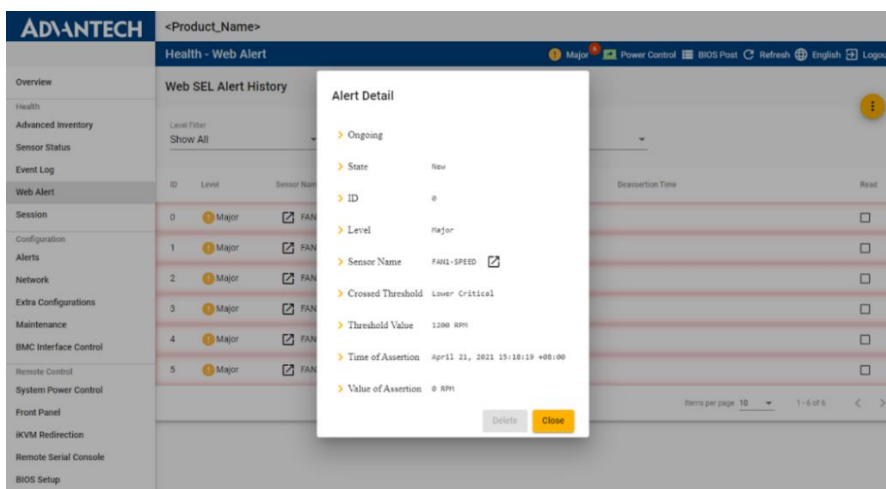
-  Refresh the list
-  Mark all past alerts as read (the status will then change to )
-  Delete all past alerts and read alerts



The screenshot shows the 'Web SEL Alert History' page. It features a sidebar with navigation options like Overview, Health, Advanced Inventory, Sensor Status, Event Log, Web Alert, Session, Configuration, Alerts, Network, Extra Configurations, Maintenance, BMC Interface Control, Remote Control, System Power Control, Front Panel, IKVM Redirection, Remote Serial Console, and BIOS Setup. The main content area displays a table of alerts with columns for ID, Level, Sensor Name, Assertion Time, Desertion Time, and Read status. There are filters for Level, State, and Sensor Type, each with a 'Show All' button. A 'More' icon (three dots in a circle) is visible in the top right corner of the table area.

ID	Level	Sensor Name	Assertion Time	Desertion Time	Read
0	Major	FAN1-SPEED	04/21/2021 15:18:19		☐
1	Major	FAN2-SPEED	04/21/2021 15:18:20		☐
2	Major	FAN3-SPEED	04/21/2021 15:18:20		☐
3	Major	FAN4-SPEED	04/21/2021 15:18:21		☐
4	Major	FAN5-SPEED	04/21/2021 15:18:21		☐
5	Major	FAN6-SPEED	04/21/2021 15:18:21		☐

Figure 11: Web Alert Page

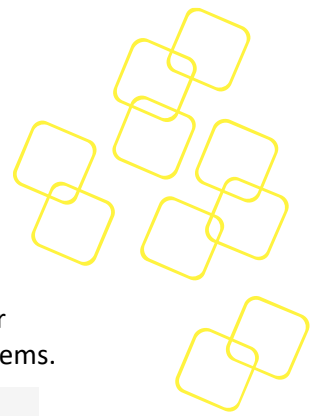


The screenshot shows the 'Alert Detail' dialog box overlaid on the Web SEL Alert History page. The dialog box contains the following information:

- Ongoing
- State: New
- ID: 0
- Level: Major
- Sensor Name: FAN1-SPEED
- Crossed Threshold: Lower Critical
- Threshold Value: 1200 RPM
- Time of Assertion: April 21, 2021 15:18:19 +08:00
- Value of Assertion: 0 RPM

At the bottom of the dialog box, there are 'Delete' and 'Close' buttons.

Figure 12: Details in Event Log



3.3.5 Session

The **Session** page is to show current user and user status. You can get the more user information (e.g. user name, user level, log in time) by double clicking on the user items.

Username	User Level	Created At	Expected Expiration	Attached Sessions
administrator	Administrator	04/21/2021 15:50:35	04/28/2021 16:03:54	iKVM Serial Console
administrator	Administrator	04/21/2021 15:38:05	04/28/2021 15:44:40	
administrator	Administrator	04/21/2021 15:22:06	04/28/2021 15:48:55	

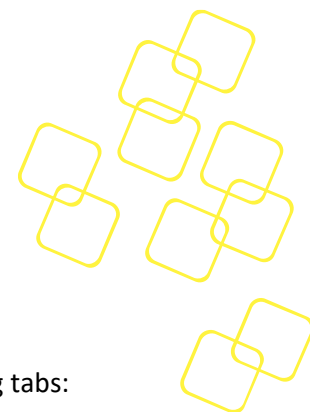
Figure 13: Session List Page

In addition, if the user opens iKVM or serial console session, it will be displayed in the Attached Sessions in user list and the control button will be shown in pop-up **Session Detail** dialog.

Session Detail	
This is the current session	
Username	administrator (UID: 5)
User Level	Administrator
Last Checked At	April 21, 2021 16:07:01 +08:00
Session Identity	
Session Lifetime	
iKVM	
Serial Console	
Session ID	7c9868ca581c907a5a96be3e0913f5
Session Lifetime	0 Hours 5 Minutes 0 Seconds
Rest Time Since Check	0 Hours 4 Minutes 58 Seconds
Close End All Recheck	

Figure 14: Session details

You can end any sessions by pressing the [End](#) button and there will be a warning message “Ending a session will cause unexpected results. Continue to end xxx session?” before the session has ended. You can also end all node explore/iKVM/serial console sessions by pressing the [End All](#) button. Before all the sessions are ended, including node explorer, you have to double confirm the warning message “The current session and all its associated sessions will also be closed down. This page will then be logged out. Continue?”



3.4 Configuration

3.4.1 Alerts

This page allows you to set and modify the advanced alert settings via the following tabs:

- **Event Filter Table**
- **Alert Policy Table**
- **Destinations**

ADIANTECH

<Product_Name>

Configuration - Alerts

Major

Power Control

BIOS Post

Refresh

English

Logout

Overview

Health

Advanced Inventory

Sensor Status

Event Log

Web Alert

Session

Configuration

Alerts

Network

Extra Configurations

Maintenance

BMC Interface Control

Remote Control

System Power Control

Front Panel

iKVM Redirection

Remote Serial Console

BIOS Setup

Event Filter Table

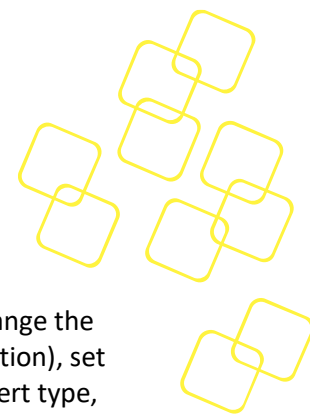
Alert Policy Table

Destinations

Event Filter Table

ID	Event Severity	Sensor Name	Actions	Policy Number	Enabled
1	Critical Condition	Any	Alert, OEM action	1	☒
2	Critical Condition	Any	Alert, OEM action	1	☒
3	Critical Condition	CASE_INTRUSION	Alert	1	☒
4	Critical Condition	Any	Alert, OEM action	1	☒
5	Critical Condition	Any	Alert, OEM action	1	☒
6	Unspecified			0	☐
7	Unspecified			0	☐
8	Unspecified			0	☐
9	Unspecified			0	☐
10	Unspecified			0	☐
11	Unspecified			0	☐

Figure 15: Alerts Page



3.4.1.1 Event Filter Table

Each alert entry can be clicked to enable/disable the platform event filter (PEF), change the policy number, adjust the severity, perform corresponding actions (alert or OEM action), set a sensor type and name, and view detailed event information. Depending on the alert type, further settings are available. For a definition of the event severity, refer to: “IPMI Platform Event Trap Format Specification v2.0.”

Policy Number: [Policy number in Alert policy table]. The total number of policies with the same policy number (i.e. how many policies are enabled). This can be set in the alert policy table.

The screenshot shows the 'Configuration - Alerts' interface. The 'Event Filter Table' is active, displaying a table with columns: ID, Event Severity, Actions, Policy Number, and Enabled. The table contains 9 rows. A modal window titled 'Event Filter #1' is open, showing settings for the selected filter. The modal has tabs for General, Severity, Actions, Sensor, and Event. The 'General' tab is selected, showing 'Enable this filter.' checked, 'Policy Number *' set to '[1]: 16 policies (1 enabled)', and 'Save', 'Clear', and 'Cancel' buttons.

ID	Event Severity	Actions	Policy Number	Enabled
1	Critical Condition	Alert, OEM action	1	☒
2	Critical Condition	Alert, OEM action	1	☒
3	Critical Condition	Alert	1	☒
4	Critical Condition	Alert, OEM action	1	☒
5	Critical Condition	Alert, OEM action	1	☒
6	Unspecified		0	☐
7	Unspecified		0	☐
8	Unspecified		0	☐
9	Unspecified		0	☐

Figure 16: Alert Setting Modification (Event Filter Table)



3.4.1.2 Alert Policy Table

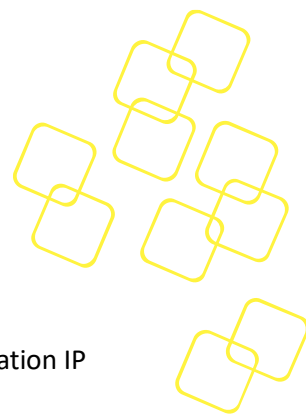
In the table, the alert policy can be enabled and the corresponding action can be selected (e.g. [Always send], [Next entry], [Stop on success], etc.)

- Enable/disable the alert policy: checking/clearing the box
- Destination: [Channel – Destination ID] IP or [Channel – Destination ID] email address is defined in the **Destinations** tab in the **Alerts** page
- Policy: Different alert policy as described in Figure 17.

The screenshot shows the 'Configuration - Alerts' interface. On the left, there's a table titled 'Alert Policy Table' with columns: ID, Policy Number, and Policy. The table lists 13 entries, all with Policy Number 1 and Policy 'Always Send'. A modal window titled 'Alert Policy #1' is open, showing options to enable the policy, set a destination, and choose an action from a list: [Always Send], [Next Entry], [Stop on Success], [Next Channel], and [Next Destination Type]. The background table has columns for 'Destination ID', 'Destination', and 'Enabled'.

ID	Policy Number	Policy	Destination ID	Destination	Enabled
1	1	Always Send		0.0.0.0	☒
2	1	Always Send		0.0.0.0	☐
3	1	Always Send		0.0.0.0	☐
4	1	Always Send		0.0.0.0	☐
5	1	Always Send		0.0.0.0	☐
6	1	Always Send		0.0.0.0	☐
7	1	Always Send		0.0.0.0	☐
8	1	Always Send		0.0.0.0	☐
9	1	Always Send		0.0.0.0	☐
10	1	Always Send		0.0.0.0	☐
11	1	Always Send		0.0.0.0	☐
12	1	Always Send		0.0.0.0	☐
13	1	Always Send		0.0.0.0	☐

Figure 17: Alert Setting Modification (Alert Policy Table)



3.4.1.3 Destinations

- Destination type: PET Trap or SMTP mail
- Different settings regarding the network management protocol type: destination IP or email receiver address, subject, and message body mail address

Note: **Send Test** button is important to check if the destination actually works. Check SMTP setting if SMTP does not work.

Configuration - Alerts

Event Filter Table | Alert Policy Table | **Destinations**

Destinations

LAN Channel: 1

ID	Destination Type
1	PET Trap
2	PET Trap
3	PET Trap
4	PET Trap
5	PET Trap
6	PET Trap
7	PET Trap
8	PET Trap

Destination #2 in Channel #1

Destination Type: PET Trap

IP Address Type: IPv4 Address

IP Address: 0.0.0.0

Figure 18: Destinations Settings (PET Trap)

Configuration - Alerts

Event Filter Table | Alert Policy Table | **Destinations**

LAN Channel: 1

ID	Destination Type
1	PET Trap
2	PET Trap
3	PET Trap
4	PET Trap
5	PET Trap
6	PET Trap
7	PET Trap
8	PET Trap

Destination #1 in Channel #1

Destination Type: SMTP Email

Receiver Email Address: receiver@mail.com

Email Subject: Alert

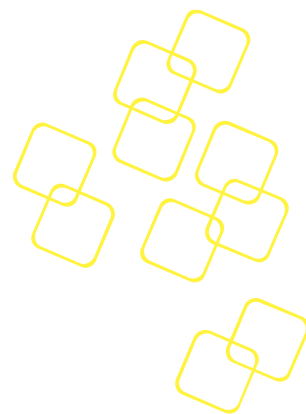
Email Body: This is an alert message.

Replace Words Usage

The replace words (the bold words below with double curly braces) can be put into Email Subject and Body, and will be replaced with actual information of the triggering alert when the Email is sent. It is not limited how many time a word could be used.

Note: These words must be used with their double

Figure 19: Destinations Settings (SMTP Email)



Configuration - Alerts

Event Filter Table

Destinations

ID	Destination Type
1	PET Trap
2	PET Trap
3	PET Trap
4	PET Trap
5	PET Trap
6	PET Trap
7	PET Trap
8	PET Trap
9	PET Trap
10	PET Trap

Destination #1 in Channel #1

Note: These words must be used with their double braces.

{{SensorName}}
The name of the sensor who generates the event.

{{SensorType}}
The type of the sensor who generates the event.

{{SensorNumber}}
The number of the sensor who generates the event.

{{Direction}}
Direction of the event: "Assert" or "Deassert".

{{Threshold}}
The threshold of the sensor that is crossed in the event. "N/A" if the event is not threshold-based.

{{Severity}}
The severity set in the filter.

{{Description}}
The description of the event.

{{IPv4Address}}
The IPv4 address of the LAN channel that sends this alert.

{{Timestamp}}
The timestamp of the event generation.

{{Hostname}}
The hostname of the BMC.

Send Test

Save

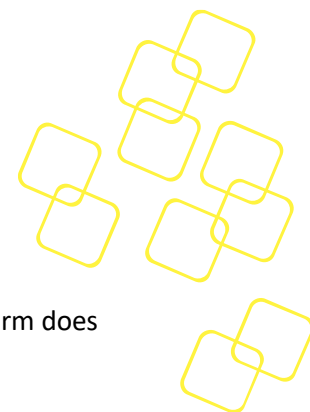
Clear

Cancel

Figure 20: Destinations Settings (SMTP Email)

Advantech Node Explorer allows you to edit alert messages with some keywords, such as SensorName, SensorType, Description, etc. (see Figure 19 and Figure 20), which will be replaced with actual information. This will give you clearer notifications with regard to what the warning is for. If you change the alert settings, the message "Alert settings with IDx have been updated" will appear to inform you about the new configuration and change.

If you change the alert settings, the message "Alert settings with ID x have been updated" will appear to inform you about the new configuration and change.



3.4.2 Network

BMC network settings per LAN channel can be configured on this page. If the platform does not support IPv6, then the IPv6 configuration session will not be displayed.

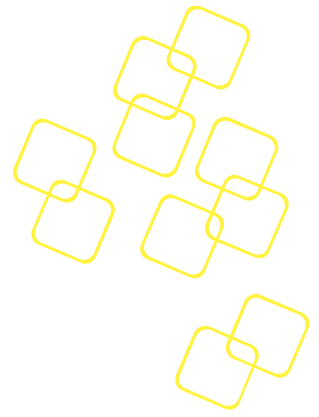
LAN channels	Selectable if there are more than two LAN channels
IPv4 configuration per channel	IP source (DHCP or Static IP) selection, setting of IP address, default gateway address for static IP
IPv6 configuration per channel	Enable/disable DHCP, set static IPv6 activated, SLAAC and default gateway (Static/Dynamic)
General setting	Specify primary and secondary name servers (DNS) for both IPv4 and IPv6
VLAN setting	Enable/disable VLAN per channel, specify VLAN priority and ID

Figure 21: Network Page

*Note: Click **Save** to save your network changes. Otherwise, any unsaved changes will be discarded and the network settings will be reset to the last saved value.*

If you change the network settings, the following message will appear: “Changing network settings may cause disconnection of Node Explorer and other products. You might not be able to return to this page to restore the settings.”

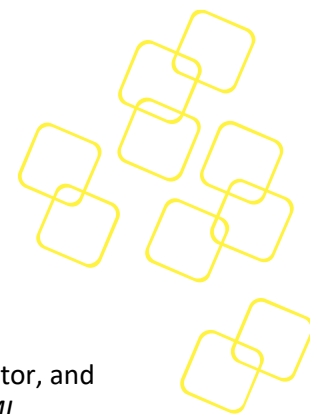
If the BMC receives an IPv6 router advertisement multicast packet from one LAN port, all LAN interfaces will be assigned to the IPv6 SLAAC address with the same domain as Figure 22.



IPv6 Configuration of Channel 1	IPv6 Configuration of Channel 2
DHCPv6 ☒ Enable DHCPv6 IPv6 Address :: IPv6 Prefix Length 0	DHCPv6 ☒ Enable DHCPv6 IPv6 Address :: IPv6 Prefix Length 0
Static IPv6 ☒ Static IPv6 Activated IPv6 Address <u>fd00::1:0:0:6170:1</u> IPv6 Prefix Length 64	Static IPv6 ☒ Static IPv6 Activated IPv6 Address <u>fd00::2:0:0:6170:2</u> IPv6 Prefix Length 64

Figure 22: IPv6 information per LAN Interface

The setting of IPv6 default gateway is only available after nodeexp-1.19.7.



3.4.3 Extra Configurations

3.4.3.1 The User Management Tab

Four unique user names/passwords with four privilege levels (call back, user, operator, and administrator) can be edited from the **User Management** tab. According to the *IPMI specification v.2.0*, which functionalities are visible or controllable depends on the privilege level of the user (e.g. different user permissions of the PAM module.)

In the **Service User Management** column, provide the user manager for different services. We only support a user named "vnc" here if the Native VNC feature is enabled. The password can be adjusted for the VNC user to control the authentication of the VNC service. The VNC Service is available after nodeexp-1.21.0.

<

User Management

LDAP

RADIUS

Time

SSL Certificate

SSH Key Management

SMTP

>

User Management

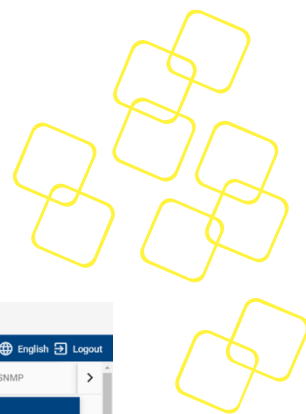
ID	Username	Privilege Level	Enabled
2	callback	Callback	☒
3	user	User	☒
4	operator	Operator	☒
5	administrator	Administrator	☒
6		No Access	☐
7		No Access	☐
8		No Access	☐
9		No Access	☐
10		No Access	☐
11		No Access	☐

Items per page 10 1 - 10 of 14 < > >>

Service User Management

ID	Username	Enabled
201	vnc	☒

Figure 23: User Management Tab



3.4.3.2 The LDAP Tab

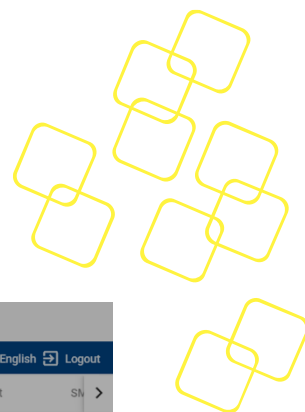
The screenshot displays the Advantech web interface for configuring LDAP settings. The interface is organized into three main panels:

- LDAP Settings:**
 - LDAP Disabled:** A toggle switch to enable or disable LDAP.
 - Current Server Host List:** A list showing the current server hosts, with a red message indicating "No server host..." and a link to "Add LDAP Server Host".
 - Add LDAP Server Host:** A form to add a new LDAP server host, including fields for "Connect Type" (set to "ldap://"), "LDAP Server URI with the server na...", "LDAP Server Port", and "LDAP Version".
 - LDAP Search Base:** A field for the LDAP search base, set to "dc=test,dc=ldap".
 - LDAP Bind DN:** A field for the LDAP bind DN, set to "uid=ruth,ou=People,dc=test,dc=ldap".
 - LDAP Bind PW:** A field for the LDAP bind password, masked with asterisks.
- LDAP Settings Cont.:**
 - PAM Filter:** A field for the PAM filter, set to "Filter to AND with uid=\\s".
 - PAM Login Attribute:** A field for the PAM login attribute, set to "The user ID attribute".
 - PAM Lookup Policy:** A dropdown menu set to "Unset".
 - PAM Check Host Attribute:** A dropdown menu set to "Unset".
 - PAM Check Service Attribute:** A dropdown menu set to "Unset".
 - PAM Group DN:** A field for the PAM group DN, set to "Group to enforce membership of".
 - PAM Member Attribute:** A field for the PAM member attribute, set to "Group member attribute".
- LDAP Group Settings:**
 - Login Group DN:** A field for the Login group DN, set to "The distinguished name(DN) of the Login group".
 - Redfish Group DN:** A field for the Redfish group DN, set to "The distinguished name(DN) of the Redfish group".
 - SSH Group DN:** A field for the SSH group DN, set to "The distinguished name(DN) of the SSH group".
 - Web Group DN:** A field for the Web group DN, set to "The distinguished name(DN) of the Web group".
 - Admin Group DN:** A field for the Admin group DN, set to "The distinguished name(DN) of the Admin group".
 - Operator Group DN:** A field for the Operator group DN, set to "The distinguished name(DN) of the Operator group".
 - User Group DN:** A field for the User group DN, set to "The distinguished name(DN) of the User group".

Figure 24: LDAP Tab (Authentication via Remote LDAP Server)

LDAP is a software protocol used for authentication and communication in directory services. To support authentication via remote LDAP server, appropriate configurations with remote LDAP server can be edited from the **LDAP** tab, including LDAP settings and LDAP group settings.

The settings of remote LDAP server are available after nodeexp-1.22.0.



3.4.3.3 The RADIUS Tab

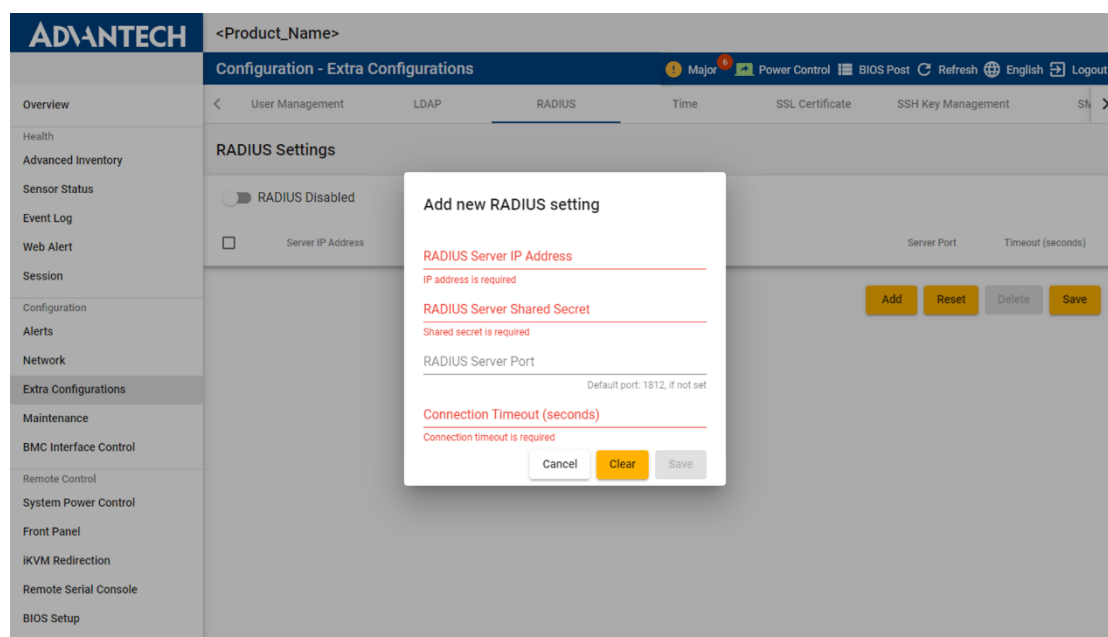


Figure 25 RADIUS Tab (Authentication via Remote RADIUS Server)

RADIUS is a software protocol that is also used in a wide range of remote authentication scenarios. You can easily configure remote RADIUS server settings from the **RADIUS** tab by pressing the **Add** button to add a setting entry or pressing **Delete** button to delete the setting you checked. There is also a switch toggle button to determine if the remote authentication will be activated or not.

The settings of remote RADIUS server are available after nodeexp-1.22.0.



3.4.3.4 The Time Tab

The screenshot shows the Advantech web interface with the 'Time' tab selected. The left sidebar contains a navigation menu with options like Overview, Health, Advanced Inventory, Sensor Status, Event Log, Web Alert, Session, Configuration, Alerts, Network, Extra Configurations (highlighted), Maintenance, BMC Interface Control, Remote Control, System Power Control, Front Panel, iKVM Redirection, Remote Serial Console, and BIOS Setup. The main content area is titled 'Configuration - Extra Configurations' and has sub-tabs for User Management, LDAP, RADIUS, Time (selected), SSL Certificate, and SSH Key Management. The 'Time' sub-tab is divided into two panels: 'System Time' and 'NTP Settings'. The 'System Time' panel shows 'Timezone' settings with 'Top Level Timezone' set to 'Asia' and 'Second Level Timezone' set to 'Taipei'. It also displays the 'Date Time' as '04/22/2021 11:06:56 +08:00' and 'Modify Date' as '4/22/2021'. There are 'Detect' and 'Save' buttons for the timezone and 'Local Time' and 'Save' buttons for the date/time. The 'NTP Settings' panel shows 'Primary Host Address' as 'ntp.server', 'Primary Host Port' as '123', and 'Secondary Host Address' as 'ntp.server'. It also has 'Secondary Host Port' as '123' and 'Default port: 123'. There is a checkbox for 'NTP Client Activated' which is unchecked. Below this, it shows 'Update Interval (seconds)' as '0', 'Last Updated Time' as 'Not Available', 'Last Update Status' as 'Success', and 'Next Update' as 'Not Available'. There are 'Test Server' and 'Save' buttons at the bottom of the NTP Settings panel.

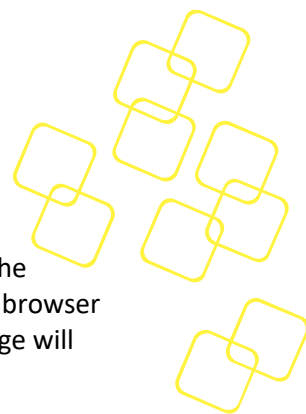
Figure 26: Time Tab (System Time and NTP Settings)

3.4.3.4.1 System Time

To make reading all the information easier, you can convert the time display in Advantech Node Explorer between different time zones. To do this, simply click on the **Time** tab and select the corresponding time zone in the drop down list or detect the local time zone of the browser by pressing **Detect**. Once the time zone has been saved, a message that the change has been successful will appear (see Figure 27) and all times in the sensor, event log, alert page, and system date time on this page will be converted. For time zone settings, refer to <https://www.iana.org/time-zones>.

The screenshot shows a 'Timezone' dialog box with a green checkmark icon and the text 'Timezone setting has been changed.' Below the message is an 'OK' button. The background shows the 'System Time' panel from Figure 26, with the 'System Date Time' now updated to '04/22/2021 11:09:44 +08:00'.

Figure 27: Time Zone Successfully Set



The BMC date and time in the product system can be set manually in the dialog of the **Modify Date** and **Modify Time** fields. You can also detect the local time zone of the browser by pressing **Local Time**. After the modified date and time have been saved, a message will appear asking you to confirm the time offset (see Figure 28)

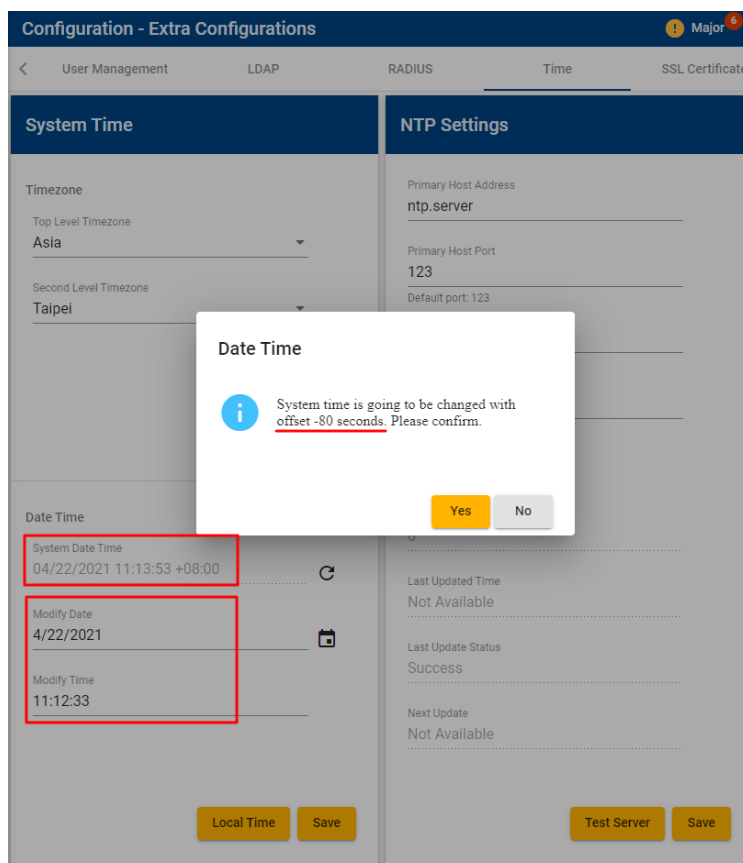
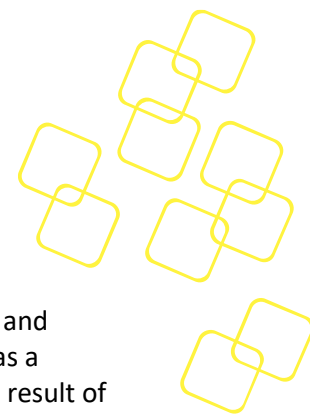


Figure 28: Offsetting the System Time



3.4.3.4.2 NTP

Network Time Protocol (NTP) is for clock synchronization between Advantech BMC and computer systems over packet-switched and variable-latency data networks. Host as a server name, port, and update interval of NTP client (min. 300 s) can be set and the result of synchronization will be shown as the last updated time, update status, and next update on the page. Click **Test Server** to verify connection with the host server.

NTP Settings

Primary Host Address

tock.stdtime.gov.tw

Primary Host Port

123

Default port: 123

Secondary Host Address

time.stdtime.gov.tw

Secondary Host Port

123

Default port: 123

☒ NTP Client Activated

Update Interval (seconds)

300

Minimal interval: 300 seconds

Last Updated Time

April 22, 2021 14:23:17 +08:00

Last Update Status

Success

Next Update

April 22, 2021 14:28:17 +08:00

Test Server

Save

Figure 29: NTP Settings

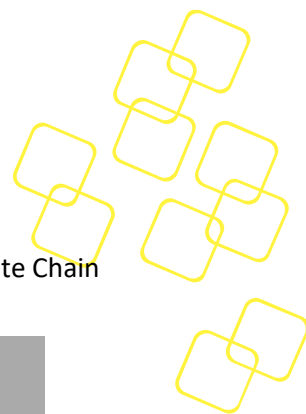


3.4.3.5 The SSL Certificate Tab

The **SSL Certificate** tab is for uploading SSL private keys and certificate files, which can be done by clicking the **Upload** icon . The tab can also be used to view SSL information.

The screenshot displays the Advantech management interface. The top navigation bar includes the Advantech logo, a product name placeholder, and various system status icons (Major, Power Control, BIOS Post, Refresh, English, Logout). The left sidebar lists navigation categories: Overview, Health, Advanced Inventory, Sensor Status, Event Log, Web Alert, Session, Configuration, Alerts, Network, Extra Configurations (highlighted), Maintenance, BMC Interface Control, Remote Control, System Power Control, Front Panel, iKVM Redirection, Remote Serial Console, and BIOS Setup. The main content area is titled 'Configuration - Extra Configurations' and features a tabbed interface with 'SSL Certificate' selected. The 'SSL Certificate' tab shows 'X.509 Fields of Current SSL Certificate' with an 'Upload' icon. The fields are organized into three sections: Common Fields (Subject Public Key Information, Serial Number, Signature, Valid From, Valid To, X.509 Version), Issuer Fields (Country Name, Common Name, Organization Name, Organization Unit Name, State Or Province Name), and Subject Fields (Country Name, Common Name, Locality Name, Organization Name, Organization Unit Name, State Or Province Name).

Figure 30: SSL Certificate Tab



To upload a SSL certificate, you need to click private key and certificate. CA Certificate Chain is a customization feature only required for some customers.

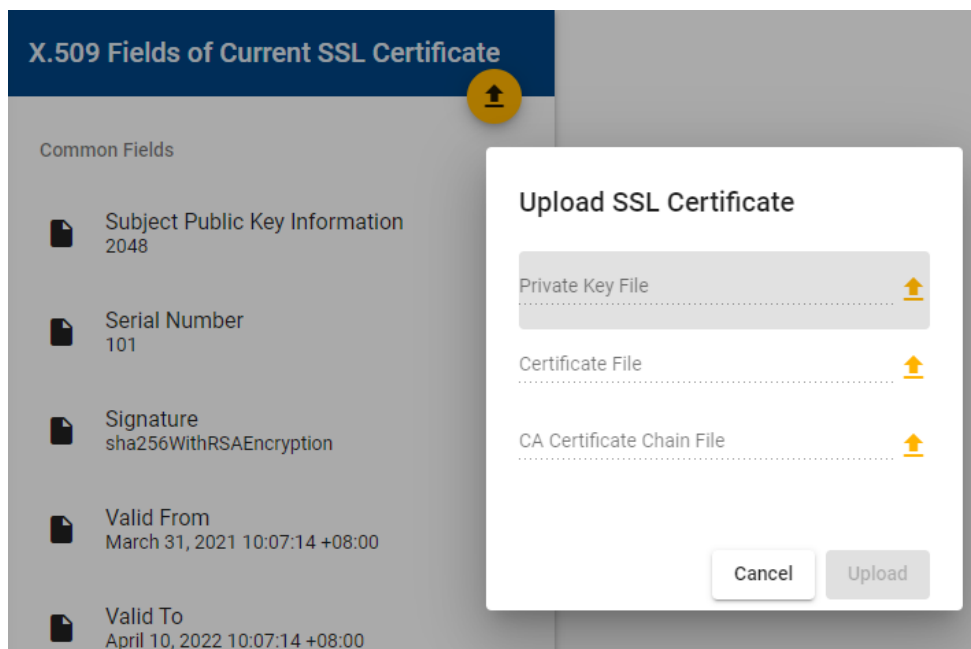


Figure 31: Upload SSL

Node Explorer will show the message "The uploaded files are not valid" if the key and the certificate do not match. If you only upload a private key or certificate file, the **Upload** button will be disabled.



3.4.3.6 The SSH Key Management

The **SSH Key Management** tab is used to upload a SSH private key file which can be done by clicking the **Upload** icon . This feature is available after nodeexp-1.20.1.

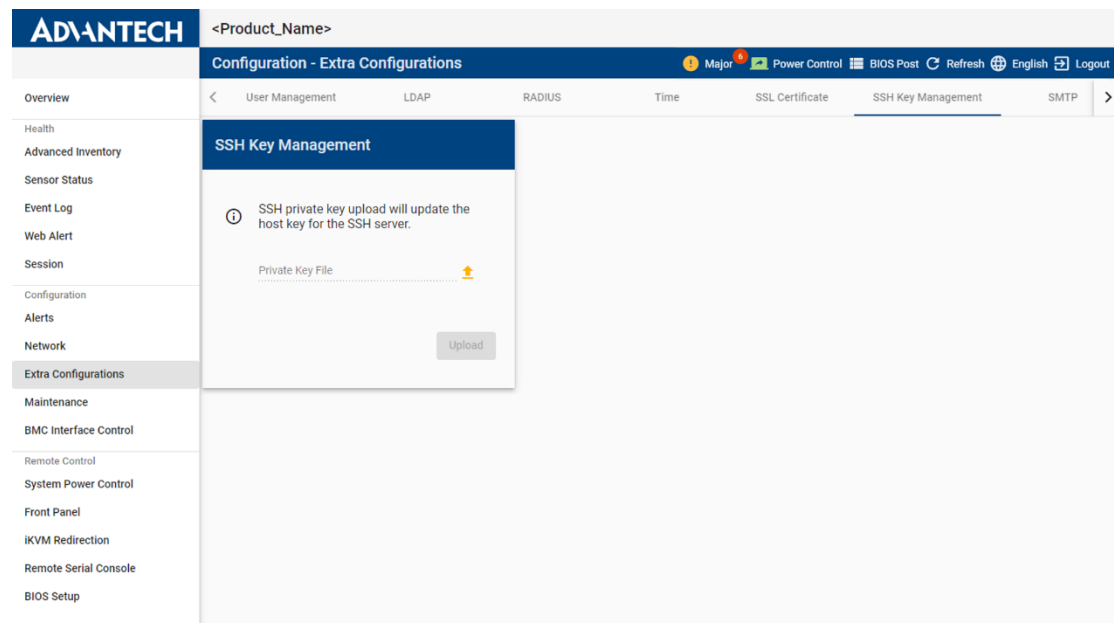
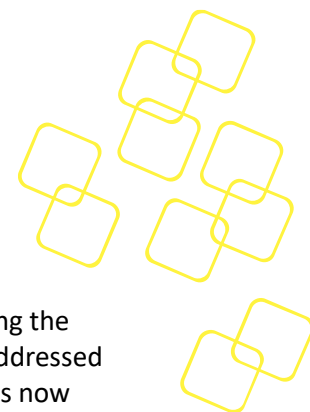


Figure 32: SSH Key Management Tab



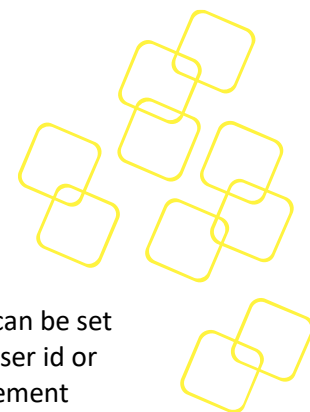
3.4.3.7 The SMTP (Simple Mail Transfer Protocol) Tab

SMTP authentication-related settings, such as enabling SSL authentication, specifying the server address, port number, user name, password, and sender's address, can be addressed on the **SMTP** tab. If you change the SMTP settings, the message "Your new setting is now saved in BMC" will appear to inform you about the new configuration and changes.

You can modify alert email templates with some replaceable keywords in both the email subject and email body. These words will be replaced by real values when the email is sent. See 3.4.1.3 Destinations for information on how to edit alert email notifications in the Alerts/Destinations tab.

The screenshot displays the Advantech BMC web interface. The top navigation bar includes the Advantech logo, a breadcrumb trail "<Product_Name> Configuration - Extra Configurations", and various system status icons (Major, Power Control, BIOS Post, Refresh, English, Logout). A secondary navigation bar lists tabs: element, LDAP, RADIUS, Time, SSL Certificate, SSH Key Management, and SMTP (which is currently selected). On the left, a sidebar menu contains categories like Overview, Health, Configuration, Alerts, Network, Extra Configurations (highlighted), Maintenance, and Remote Control. The main content area is titled "SMTP Authentication Setting" and contains the following fields: "Server Address" (smtp.mail.com), "Port" (25), "Username" (admin@mail.com), "Password" (masked with dots and a toggle icon), and "Sender Name" (admin@mail.com). There is a checked checkbox for "Use SSL Authentication" and a "Save" button at the bottom right.

Figure 33: SMTP Tab

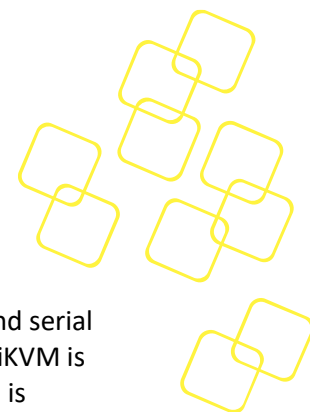


3.4.3.8 The SNMP (Simple Network Management Protocol) Tab

The **Configuration** page is for SNMP-related settings. The SNMP community string can be set to read only (public) or read/write (private) for each channel, which is similar to a user id or password that allows access to a device's statistics. In addition, SNMP MIB (Management Information Base) files can be downloaded in the tab.

Note : SNMP community strings are used only by devices that support SNMPv1 and SNMPv2c. SNMPv3 uses username/password authentication, along with an encryption key. In addition, SNMP MIB (Management Information Base) files can be downloaded from the tab.

Figure 34: SNMP Tab



3.4.3.9 The Session Timeout Tab

The **Session Timeout** tab is to set to timeout in seconds for node explorer, iKVM, and serial console session. The default timeout of node explorer is 7 days, default timeout of iKVM is 15 minutes and default timeout of serial console session is 15 minutes. This feature is available after nodeexp-1.19.1.

Figure 35: Session Timeout Tab

Note: the range of the session timeout for each component is restricted as below:

- Node Explorer Session Timeout: 300 – 604800 seconds
- iKVM Session Timeout: 300 – 3600 seconds
- Serial Console Session Timeout: 300 – 3600 seconds

After saving the settings successfully, the following message will pop out and remind you of the new timeout, which will be applied from the next session onwards.

Default Serial Console Session Timeout



The new timeout value has been saved. This will not affect existing sessions.

OK

Figure 36: Session Timeout Success



3.4.3.10 The Firewall Tab

The **Firewall** tab is to set port/IPv4/IPv6 firewall rule on different LAN Channel. The feature is available after nodeexp-1.20.1.

By clicking “**Add Rule**” button, you can set rule of port firewall with protocol (TCP or UDP), TCP/IP version (IPv4, IPv6, or both), port number from 1- 65535, rule (block or allow) and its time schedule. The time scheduling for firewall is only available after nodeexp-1.22.0.

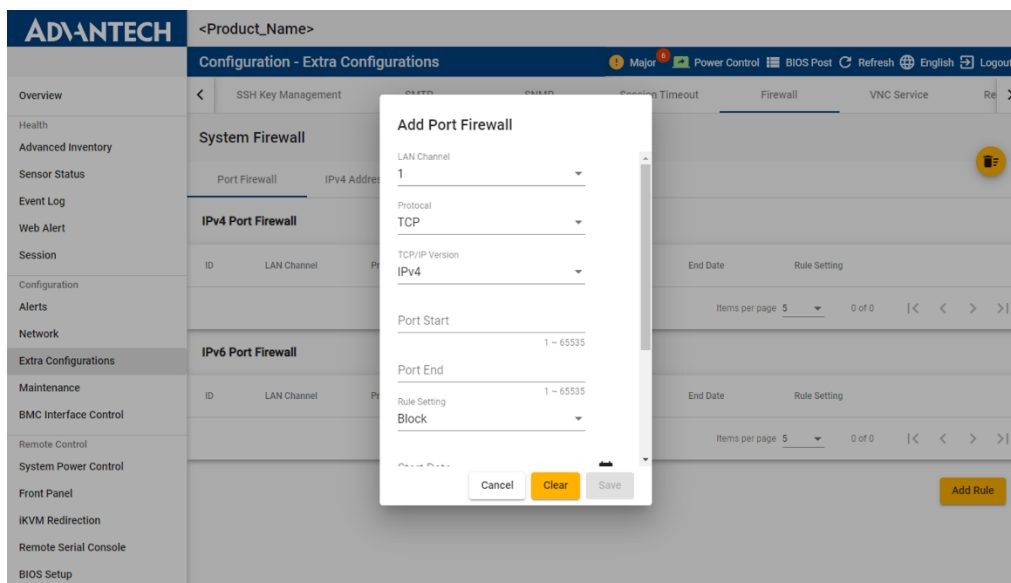


Figure 37: Add Port Firewall

To add firewall rule per channel, you can specify the rule on a range of IP addresses.

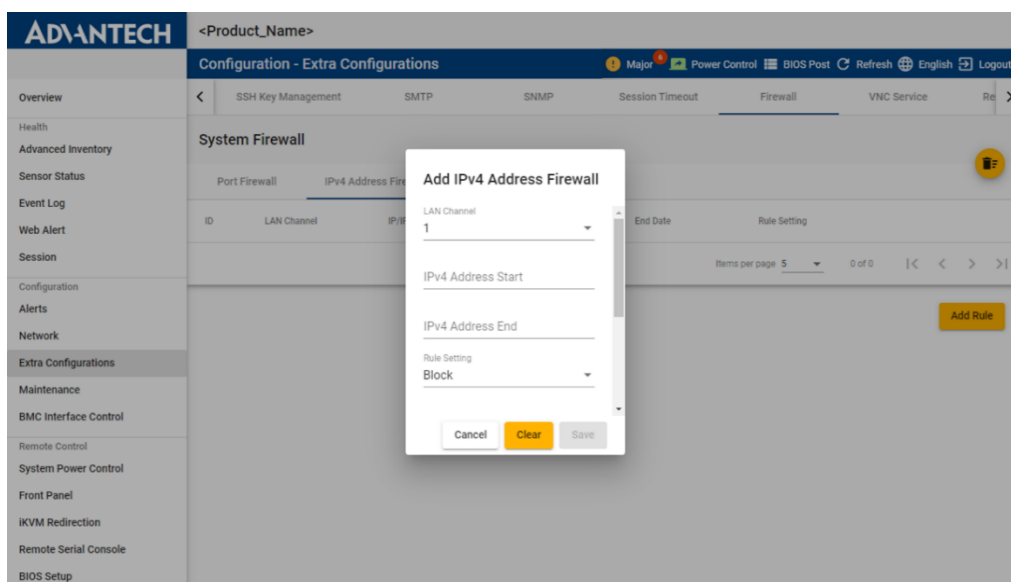
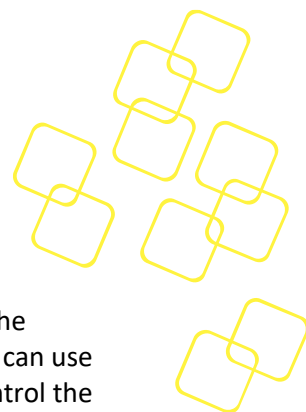


Figure 38: Add IPv4/IPv6 Address Firewall

By clicking the icon  , all of the firewall rules can be deleted.



3.4.3.11 The VNC Service Tab

The **VNC Service** tab is only available if the Native VNC feature had been enabled. The service port and session timeout of VNC service can be configured in this tab. Users can use the VNC client (TightVNC Viewer, see Figure 40) that we only support to remote control the OS system.

The VNC Service is available after nodeexp-1.21.0.

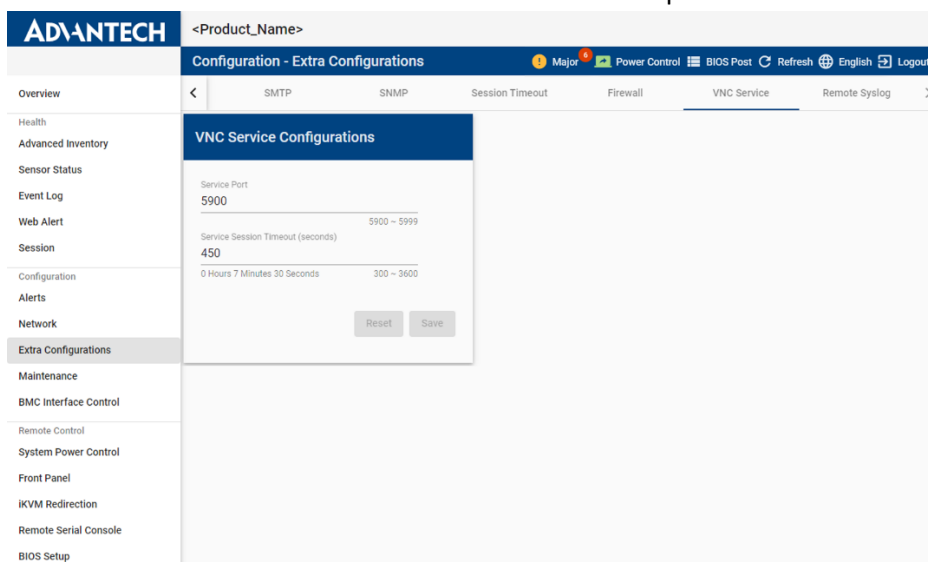


Figure 39: VNC Service Tab

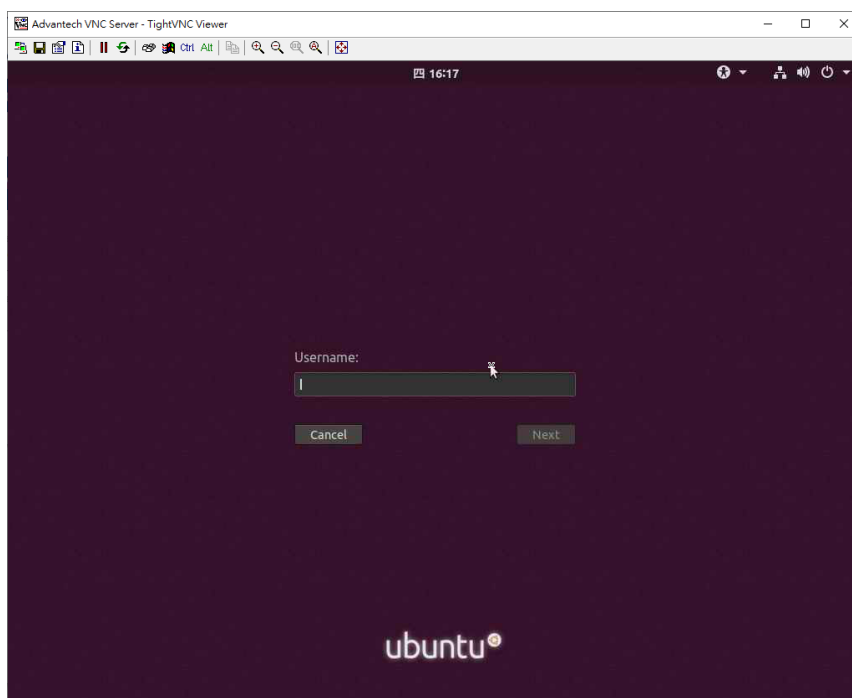


Figure 40: TightVNC Viewer



3.4.3.12 The Remote Syslog Tab

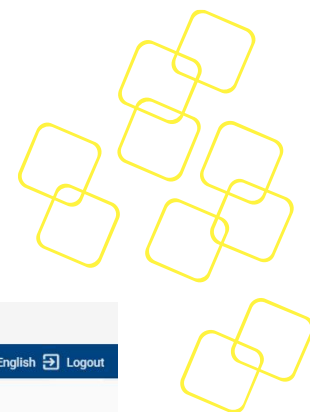
All the logs of this BMC are originally stored in flash. Node Explorer provides a way of redirecting the logs to a remote log server and can be configured via the **Remote Syslog** tab.

The screenshot shows the Advantech Node Explorer interface. The left sidebar contains a navigation menu with categories: Overview, Health, Configuration, Alerts, Network, Extra Configurations (selected), Maintenance, Remote Control, and BIOS Setup. The main content area is titled 'Configuration - Extra Configurations' and includes a sub-tab 'Remote Syslog Settings'. The settings are as follows:

Setting	Value
Enable Remote Syslog	☐
IPv4 or IPv6 Address	127.0.0.1
Port	514

A 'Save' button is located at the bottom right of the settings panel. The top of the interface shows the Advantech logo, product name placeholder, and various system status icons like Major, Power Control, BIOS Post, Refresh, English, and Logout.

Figure 41: Remote Syslog Tab



3.4.4 Maintenance

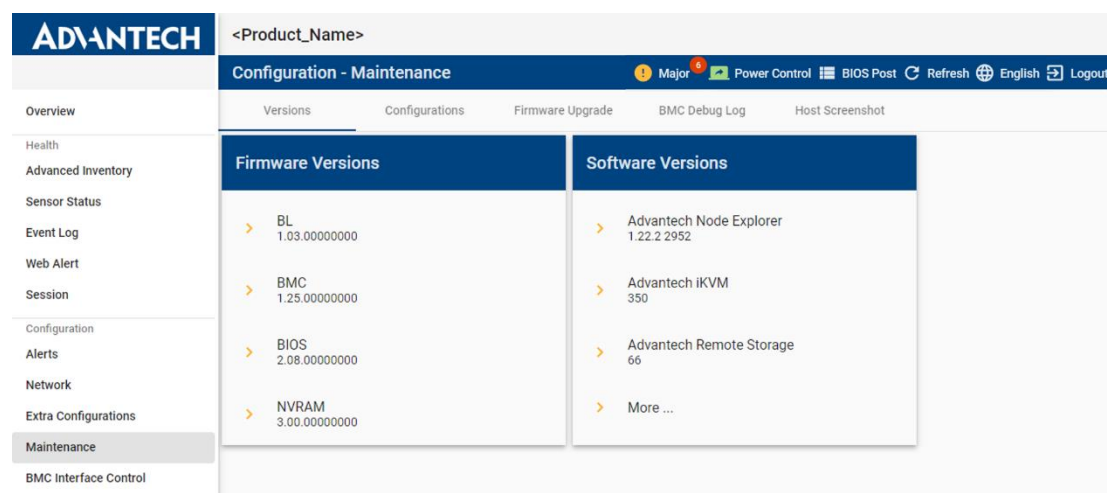


Figure 42: Maintenance page

3.4.4.1 The Version Tab

The **Versions** tab on the **Configuration-Maintenance** page will show version information of the platform management firmware and components supported in Node Explorer, including iKVM, remote storage, and so on.

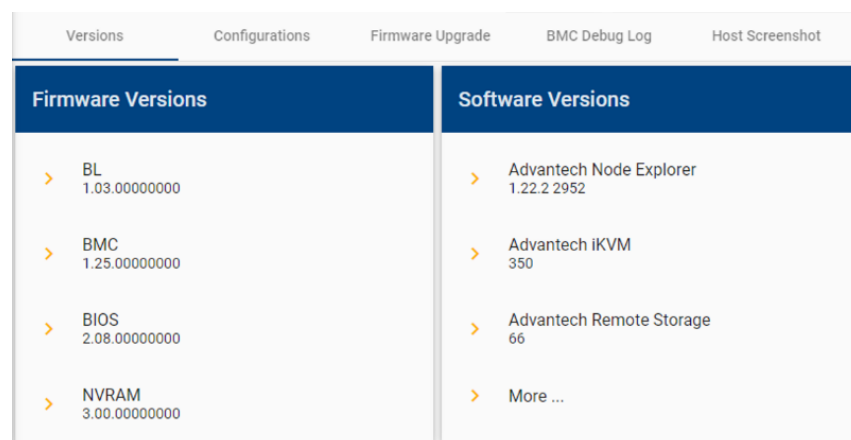


Figure 43: The Version Tab

Additional information on the version of other SW components will be shown in a pop-out dialog when you click **More...**

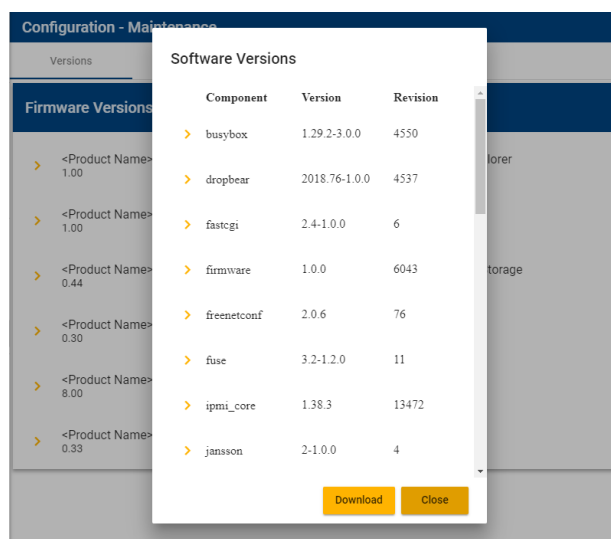
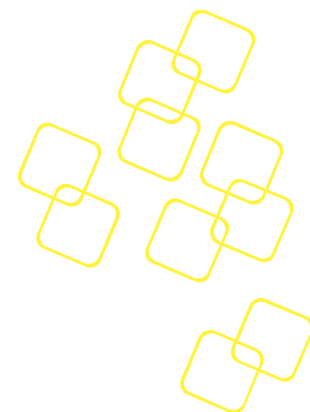


Figure 44: More Version Information on Other FW/SW

Version details can be downloaded as a file in JSON format.

3.4.4.2 The Configuration Tab

You can roll back to the default configuration in the **Configurations** tab. To save time configuring different products, you can also download the current configuration file from the platform and upload the configuration file to another platform via Node Explorer. BIOS configurations backup and rollback will be supported if BIOS feature has been enabled (only available after nodeexp-1.22.0.)

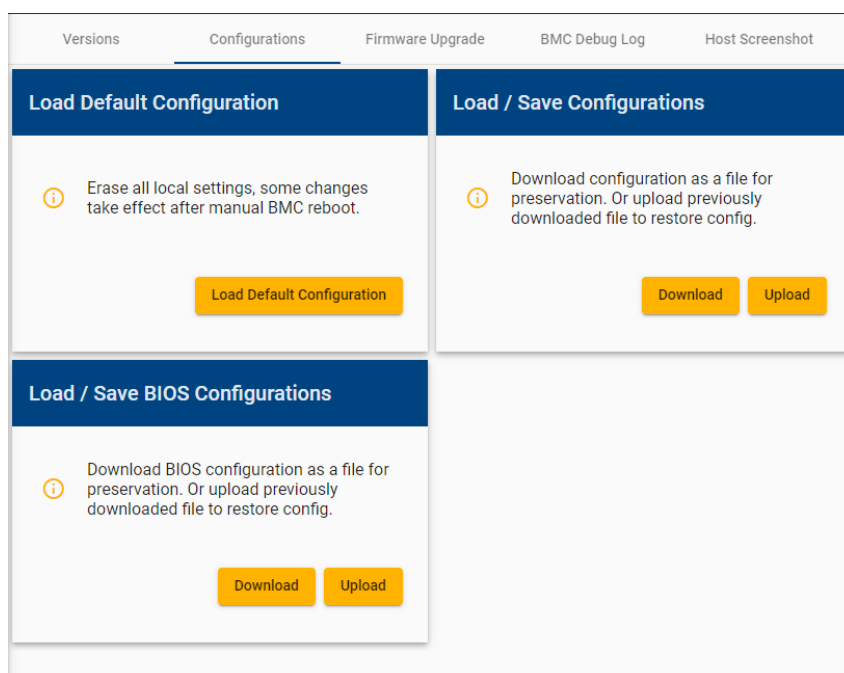
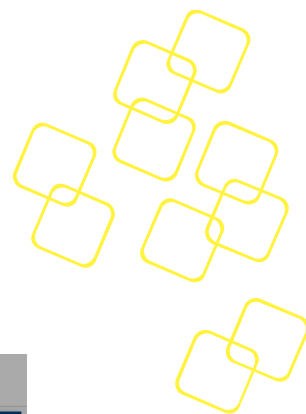


Figure 45: The Configuration Tab

Note: Security key related steps in the tab are only available from nodeexp-1.18.0 onwards. This feature is not available in earlier versions.



3.4.4.2.1 Load Default Configuration

All configuration settings will be restored to the factory defaults.

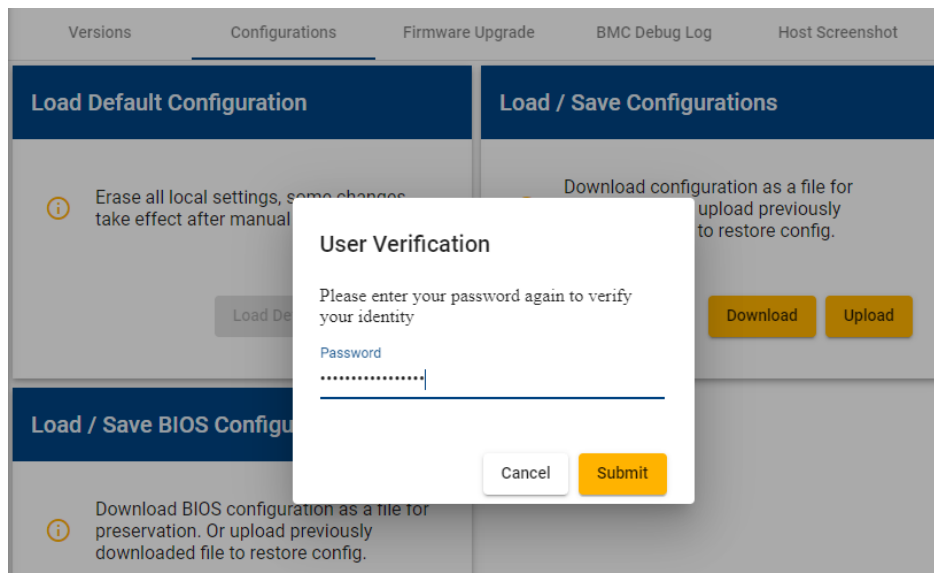


Figure 46: Enter Your Password for Confirmation

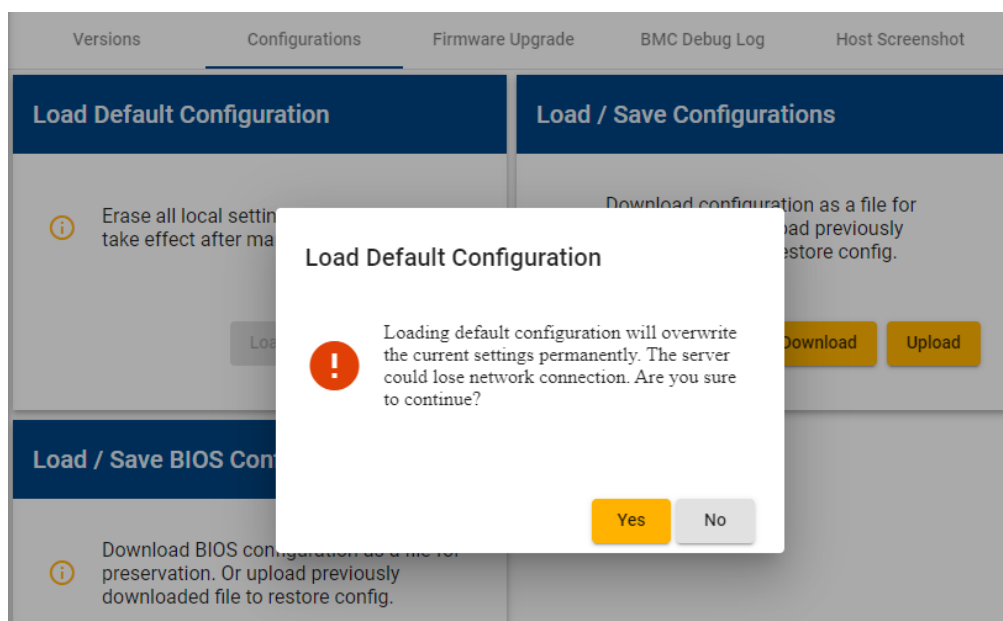


Figure 47: Re-confirm Loading the Default Settings

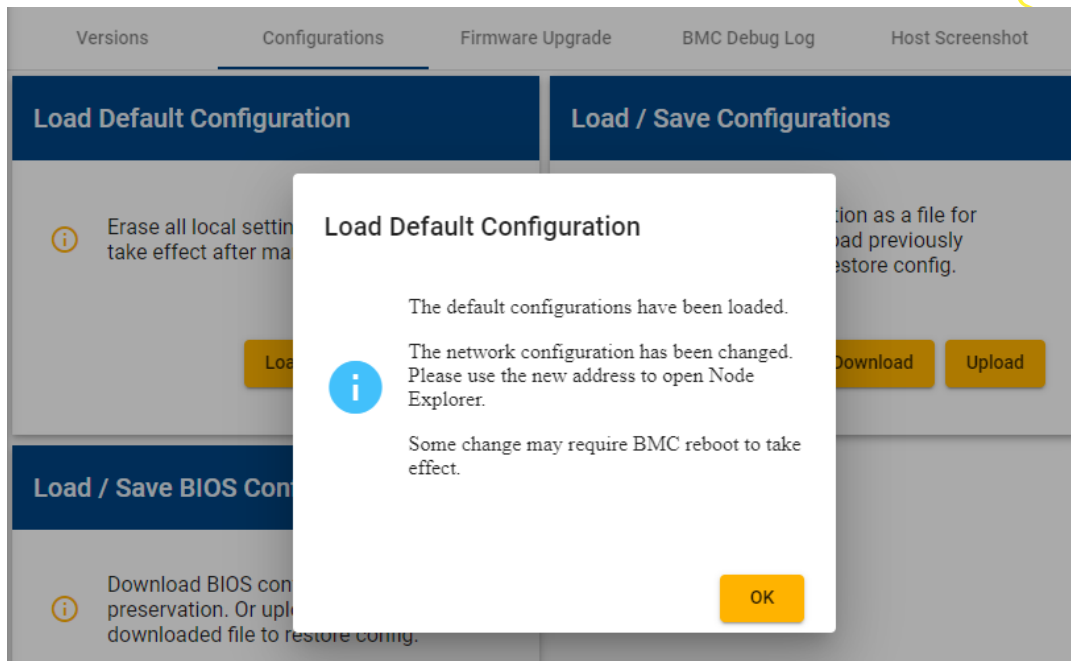
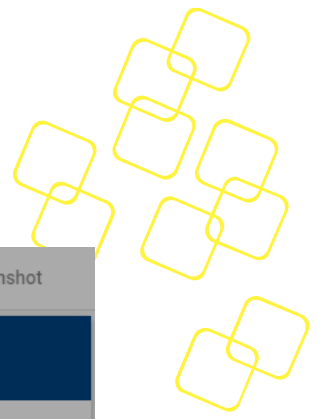
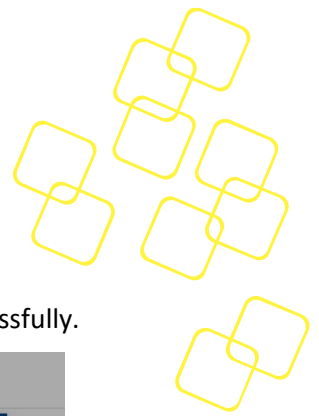


Figure 48: Default Settings Successfully Loaded



3.4.4.2.2 Download Configuration

A message will pop-up as shown below when downloading configuration files successfully.

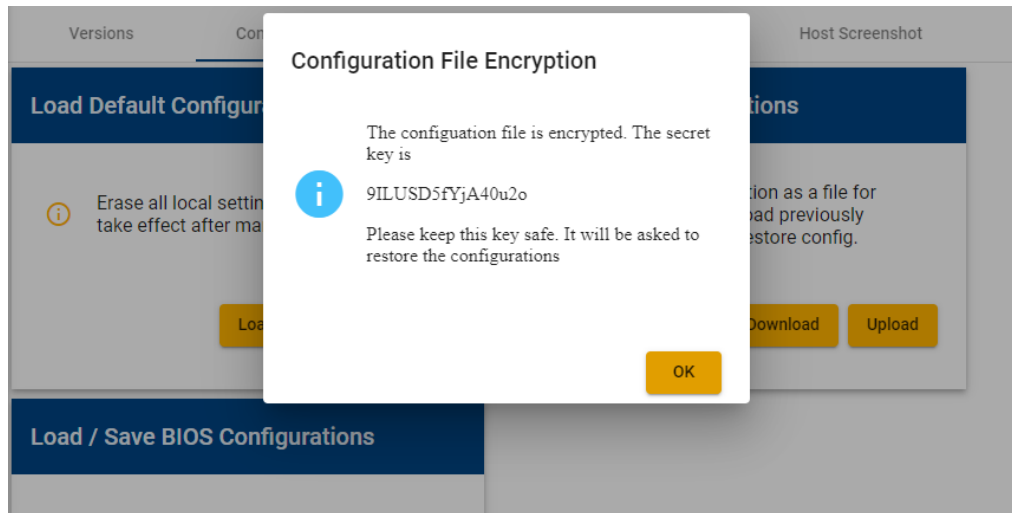


Figure 49: Encryption Key Popup

After clicking the **Download** and **OK** button, you can get two files:

- Nodeexp_config_MM_DD_YYYY.key
- Nodeexp_config_MM_DD_YYYY.config

Note: There will be only one configurations file in nodeexp-1.17.x. The .key file is available after nodeexp-1.18.0 and later versions. If you don't get the .key file via nodeexp-1.18.0 and later versions, please check if it's blocked by your web Brower as shown in Figure 50: Check the Always Allow Button to Download Multiple File. [Click to download the files.](#)

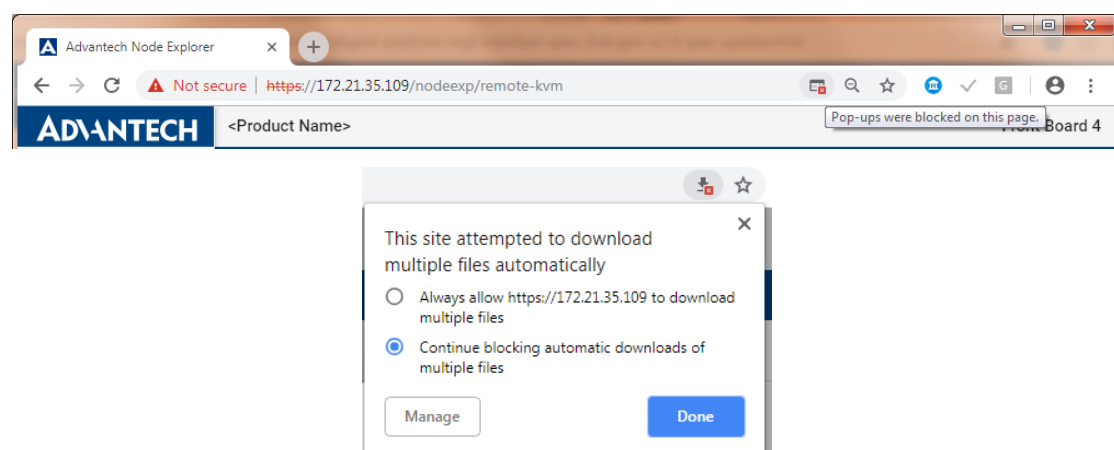
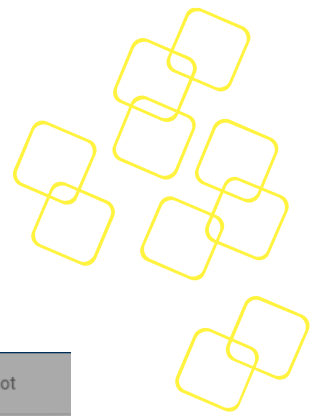


Figure 50: Check the Always Allow Button to Download Multiple File



3.4.4.2.3 Upload Configuration

Upload the configuration file by following these steps.

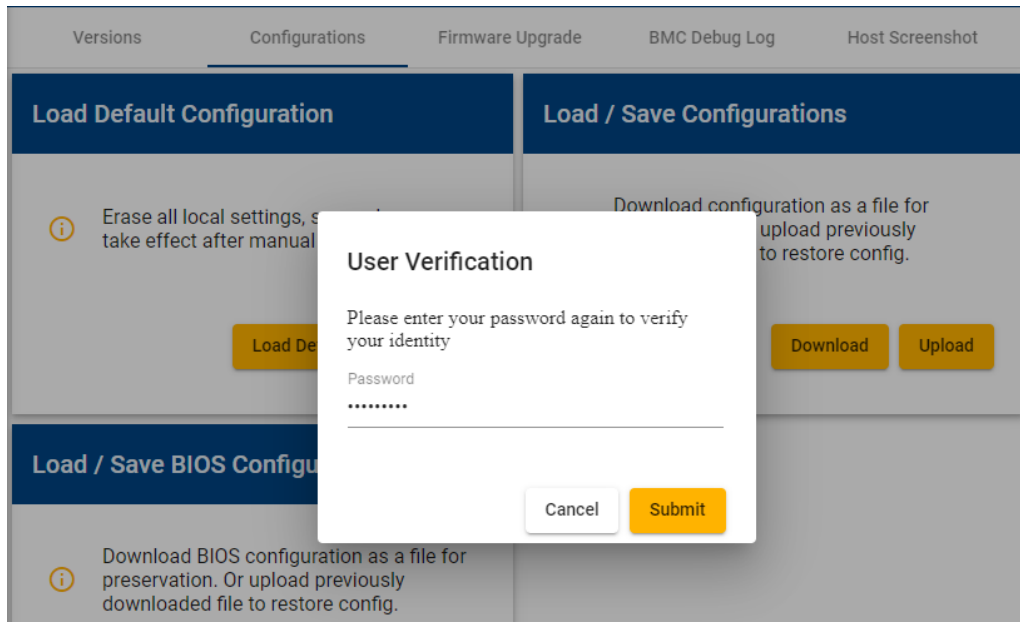


Figure 51: Enter Login Password for Confirmation

Click the upload icon  to upload the configuration file.

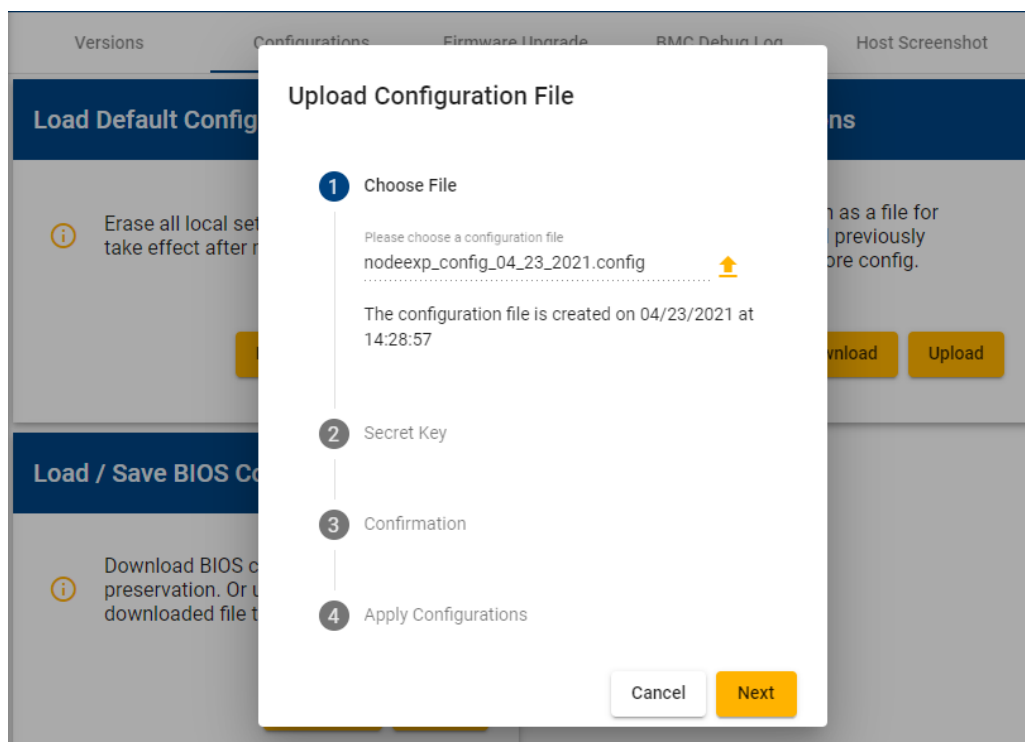


Figure 52: Select File then Press Next to Upload Configuration File

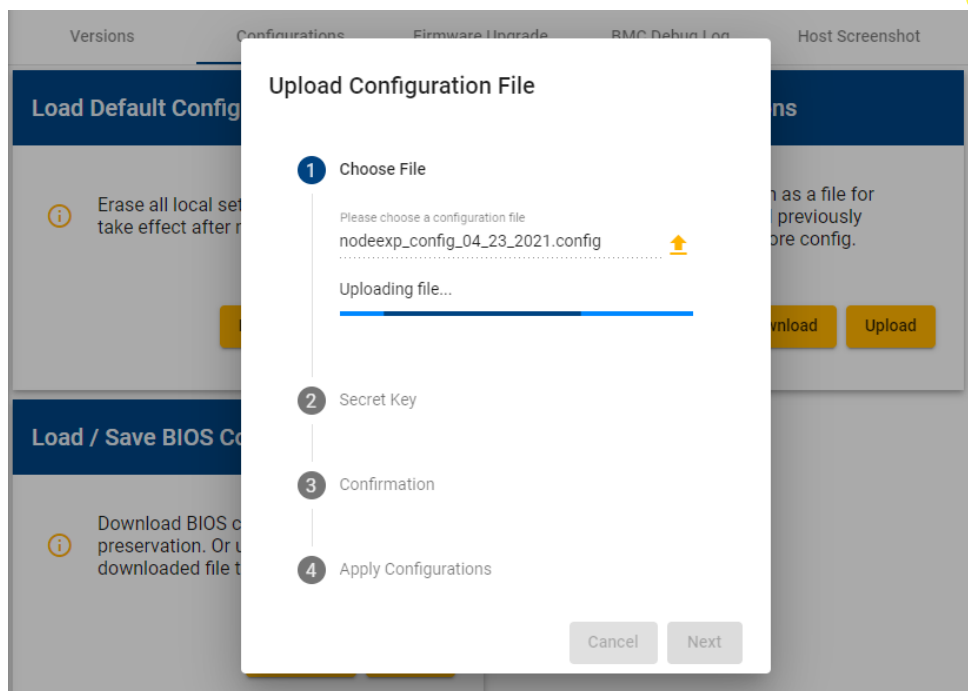
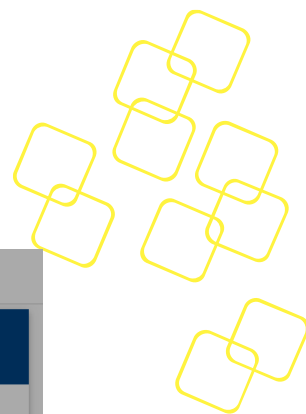
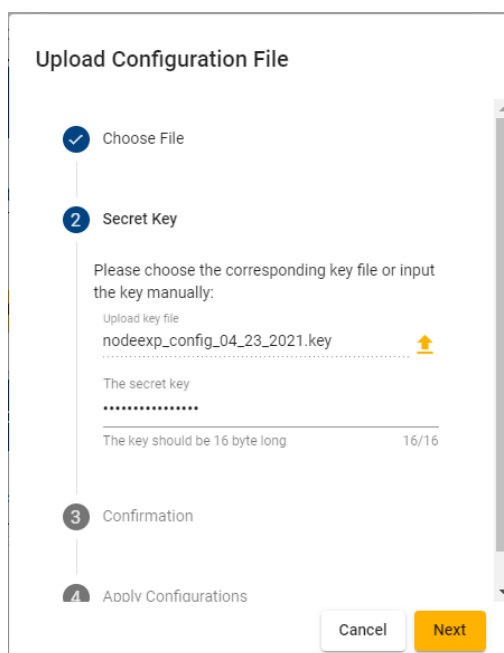


Figure 53: Uploading the Configuration File

Upload the key file  or enter the key in the text field. If the decryption has failed, it will show "Decryption failed with current key." Please double check if you have used the correct key downloaded with the paired configuration file. If the decryption is successful, it will go to the confirmation screen as in Figure 56: Confirmation of the Applied Update.



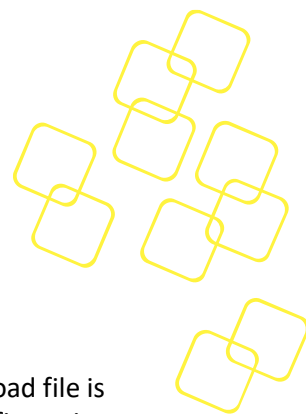


Figure 54: Enter the Encryption Key

If the configuration file is mismatched or invalid, it will show the message, "The upload file is not a valid configuration file." Please double check if you have used the correct configuration file downloaded from the Advantech website. If the confirmation check is successful, all components that the settings will be applied to will be listed.

The screenshot shows a dialog box titled "Upload Configuration File". It has a vertical progress bar on the left with four steps: "Choose File" (completed with a checkmark), "Secret Key" (completed with a checkmark), "Confirmation" (active step, indicated by a blue circle with the number 3), and "Apply Configurations" (indicated by a grey circle with the number 4). Below the progress bar, a red error message states: "The uploaded file is not a valid configuration file." At the bottom right, there are two buttons: "Cancel" and "Next".

Figure 55: Confirmation Failed

Click **Next** to apply the confirmation of the selected components.

Note: applying confirmation to some components could break the connection.

The screenshot shows the same "Upload Configuration File" dialog box, but now the "Confirmation" step is successful. The progress bar shows the first two steps completed and the third step active. Below the progress bar, the text "Please check components to be applied" is displayed. A list of components with checkboxes is shown: "Alert Configurations (77)", "Timezone (1)", "NTP Client Configurations (1)", and "SMTP Server Configurations (1)". All checkboxes are checked. At the bottom right, there are two buttons: "Cancel" and "Next".

Figure 56: Confirmation of the Applied Update

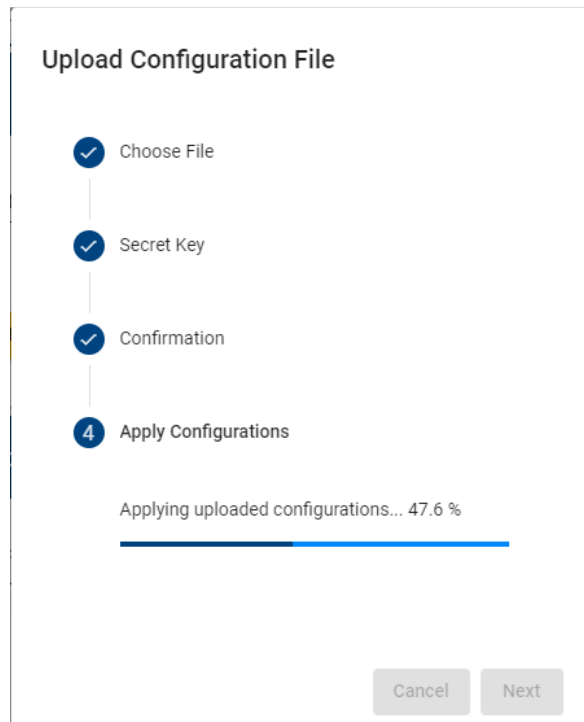
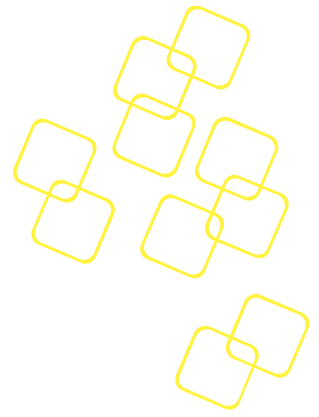


Figure 57: Applying the Configuration

Once the configuration has been applied successfully, the Advantech web interface will also download nodeexp_apply_config_report_YYYY-MM-DD.txt.

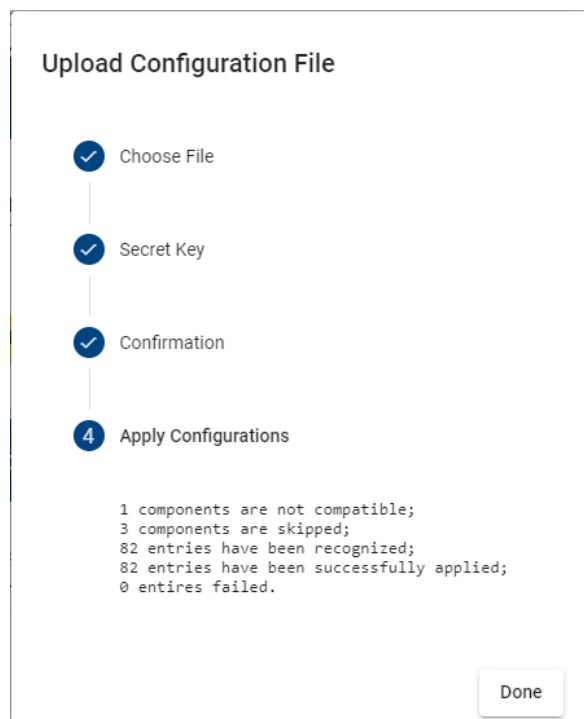
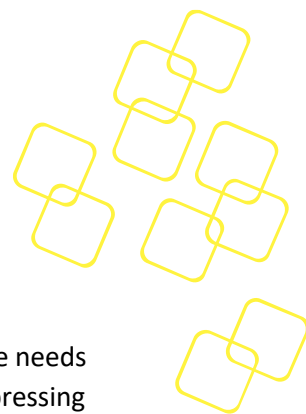


Figure 58: Configuration Successfully Applied



3.4.4.3 The Firmware Upgrade Tab

Firmware (NVRAM, CPLD/FPGA image, BIOS and BMC images) can be specified and upgraded/downgraded through Advantech Node Explorer. First, the firmware image needs to be uploaded to the BMC by clicking the **Upload** icon  to select the image, and pressing **Upload**.

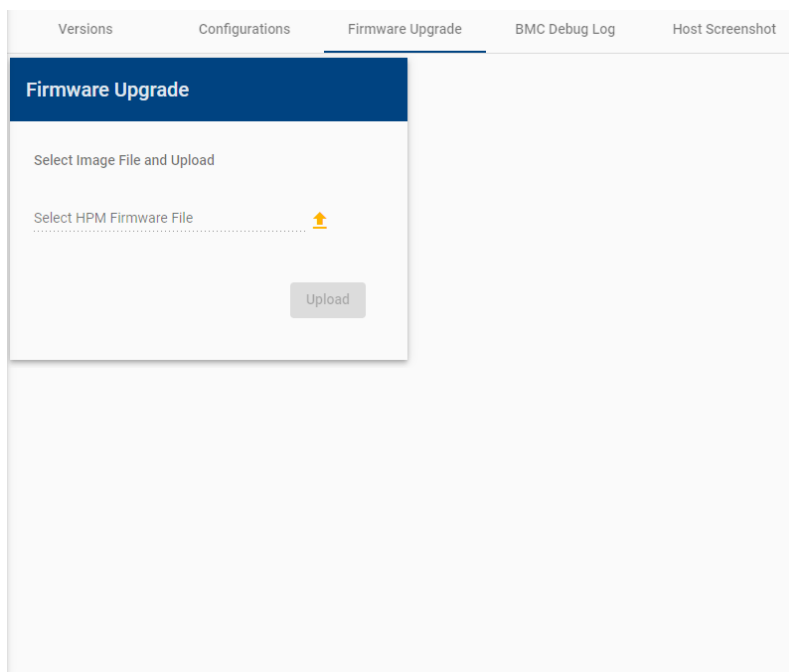


Figure 59: Firmware Upgrade Tab

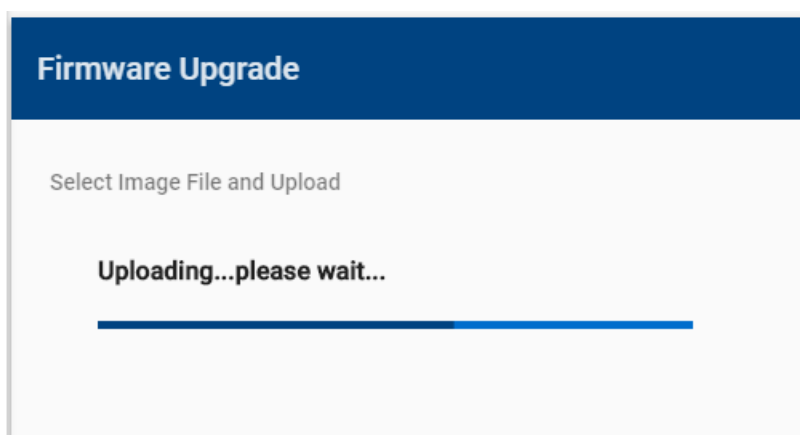


Figure 60: Firmware Image Uploading to the BMC



A dialog box to force the upgrade will appear if you press **Upgrade** when the selected firmware version is the same as the current version, as shown in Figure 61.

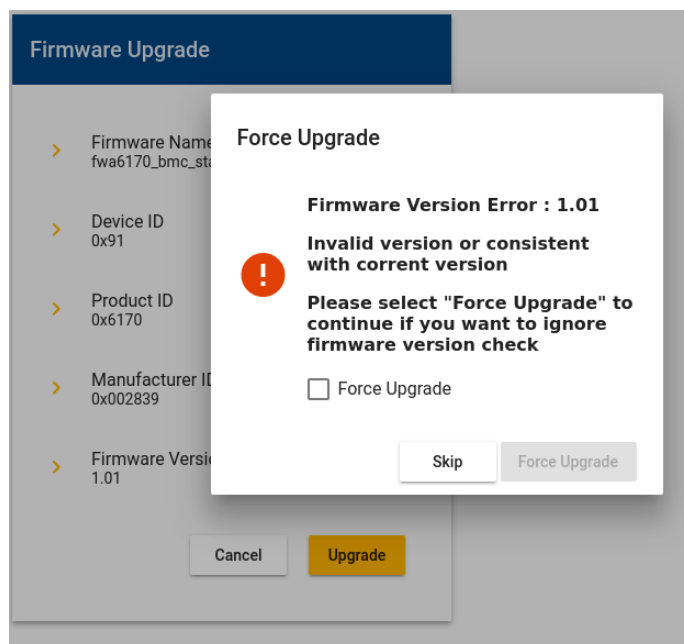


Figure 61: Confirmation of Upgrade

As shown in Figure 62, a dialog box to force the upgrade will appear if you press **Upgrade** when the device ID of the selected firmware does not match the current firmware (i.e., you upgrade the firmware of Product B by using the firmware of Product A).

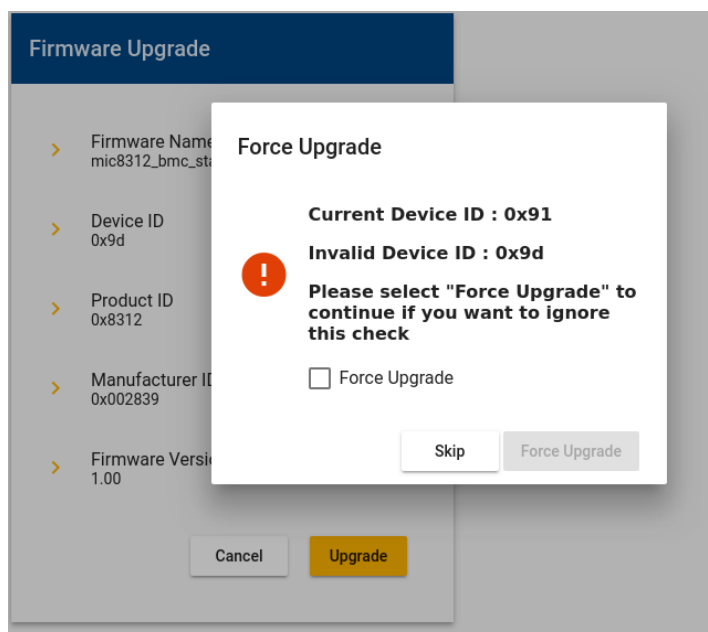


Figure 62: Error Message during Upgrade

While the firmware is upgrading, a dialog box will appear as shown in Figure 63. All other operations by different users or from different tabs will not be accessible during this time.

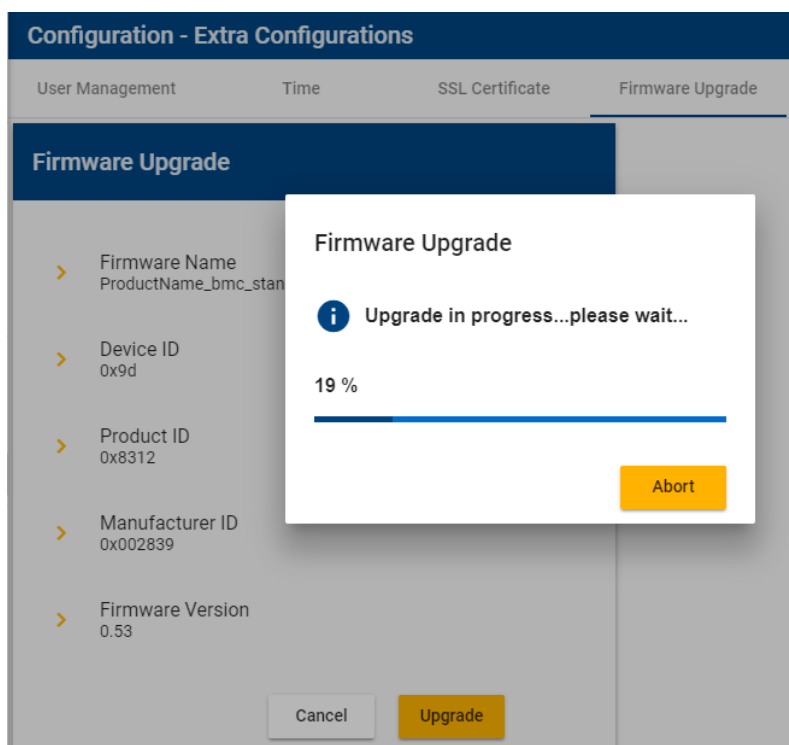
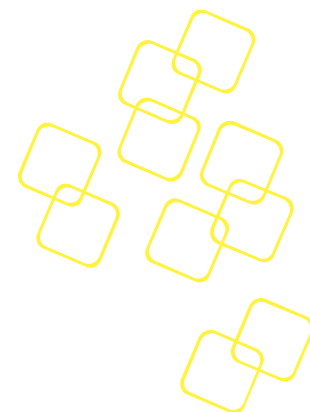


Figure 63: Firmware Upgrade in Progress

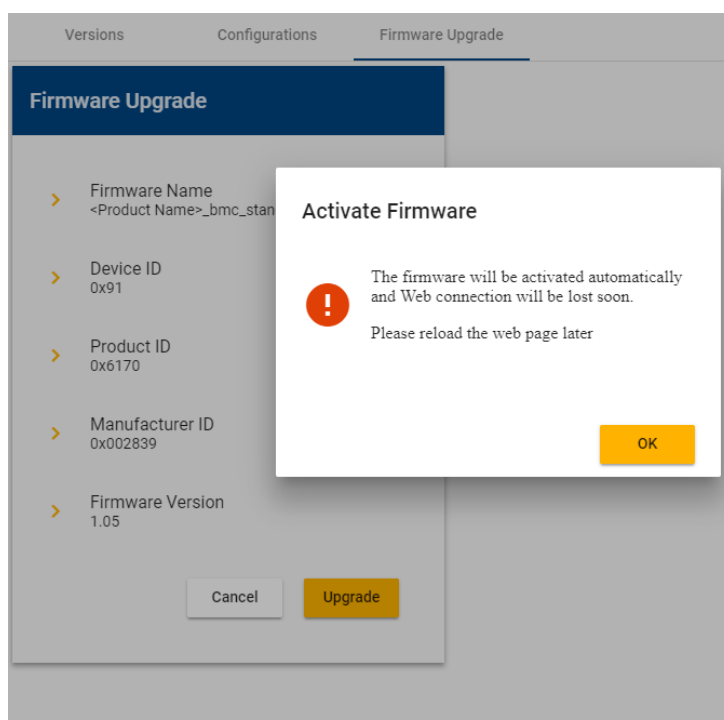


Figure 64: Firmware Upgrade Successful

While the firmware is being activated, the web connection will be lost and you will need to log in again. The web page will be refreshed automatically after activation; alternatively, you can press **F5** to refresh the page.



3.4.4.4 The BMC Debug Log Tab

In the **BMC Debug Log** tab, user review or download the single debug log by clicking the specific file. Click the **Download All** button for archived BMC log files, including “debug.archive” as bmc_log_MM_DD_YYYY.tar.gz for debugging purposes.

For flexible usage, BMC debug log is supported to output to a Syslog log file so that it can be redirected to the remote log server (see 3.4.3.12). (Output to Syslog is available after nodeexp-1.21.0.)

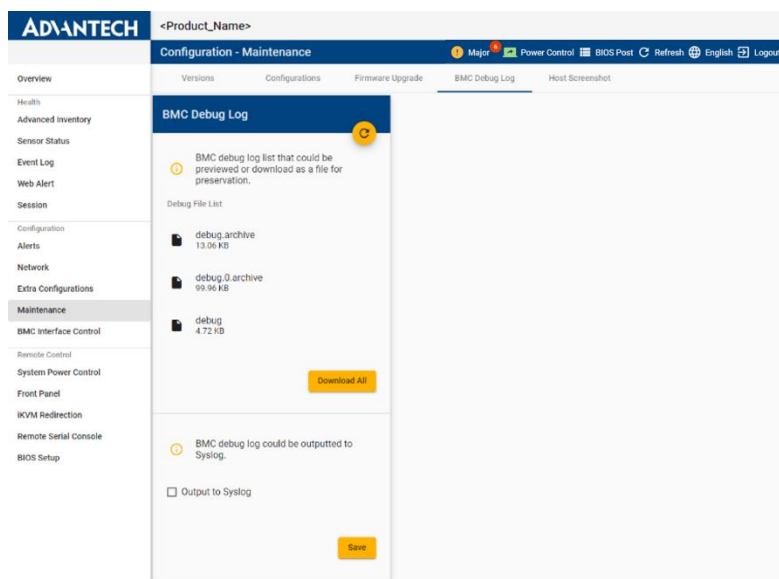


Figure 65: BMC Debug Log

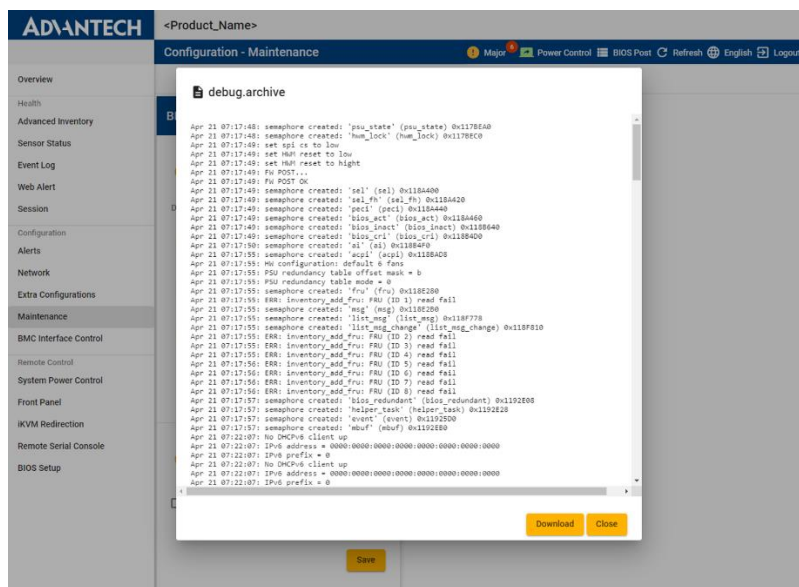
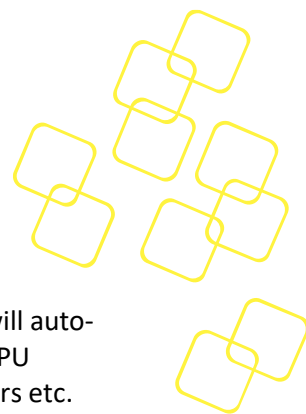


Figure 66: Check debug.archive



3.4.4.5 The Host Screenshot Tab

The **Host Screenshot** tab provides functionality for troubleshooting your OS. BMC will auto-capture the x86 host screenshot when detects x86 critical errors, like CPU IERR or CPU MCERR, and some scenarios that are driven by BIOS, like PCI Express AER, boot errors etc. Screenshots can be easily reviewed, downloaded, and removed via this tab.

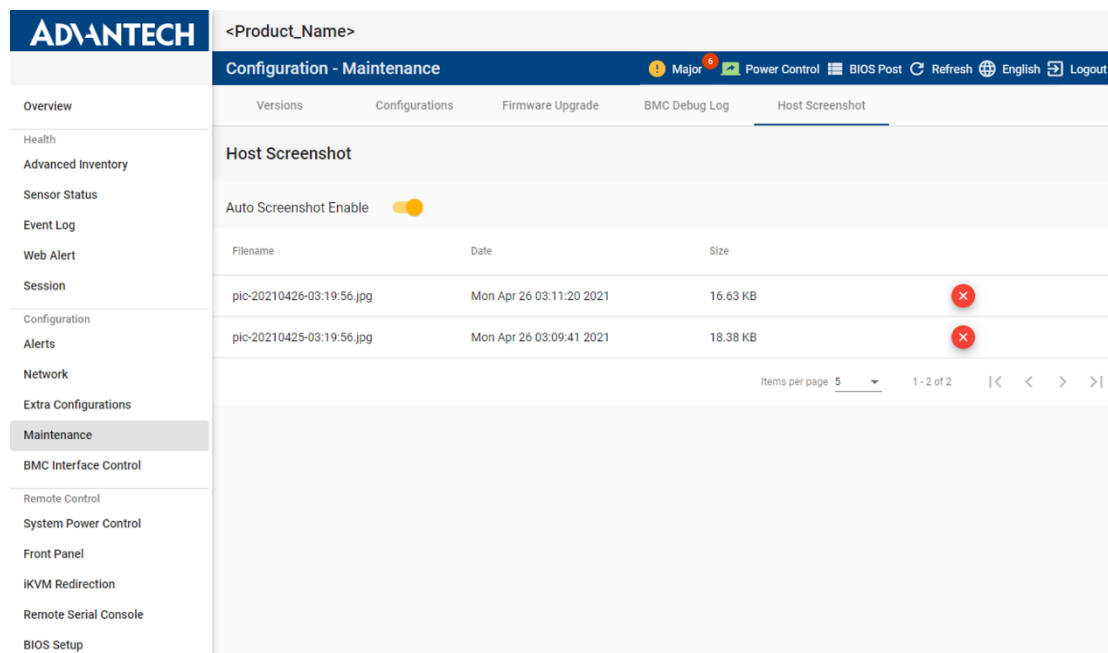


Figure 67: The Host Screenshot Tab

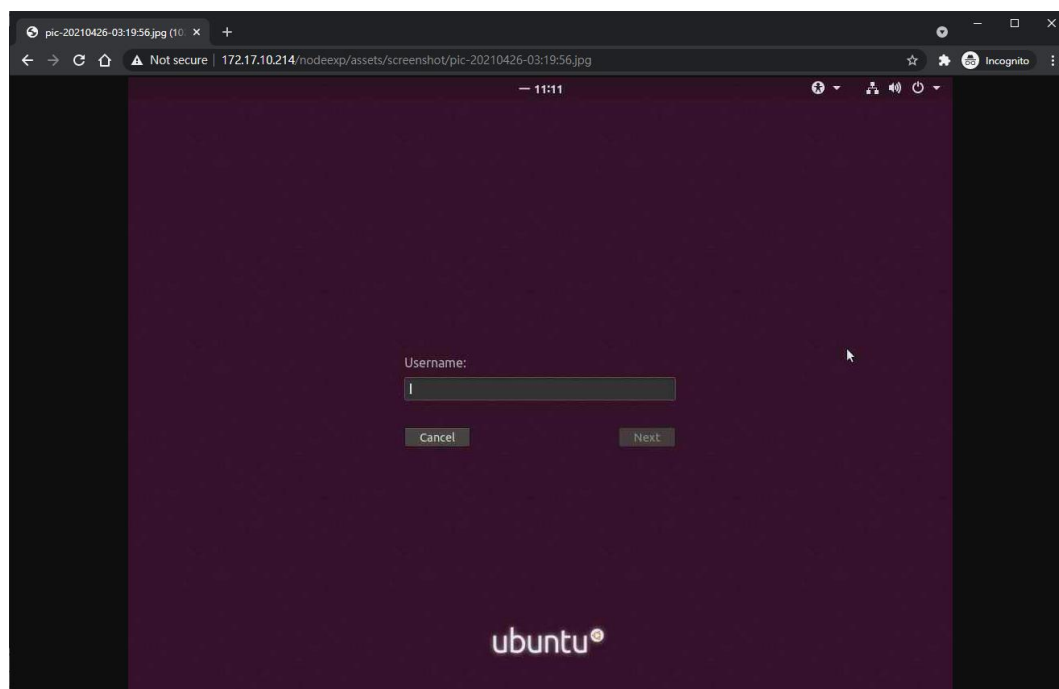
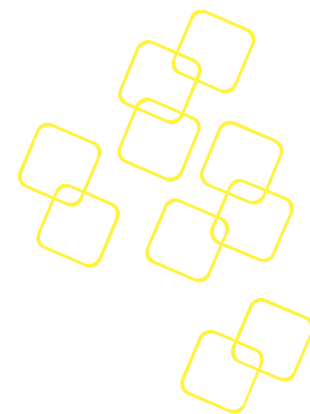


Figure 68: Reviewed Screenshot by One Click



3.4.5 BMC Interface control

This page provides BMC interface management / configuration options.

3.4.5.1 Interface tab

Users can enable/disable BMC functions (e.g. IPMI Over LAN, Serial Over LAN) in the **BMC Interface Control tab**.

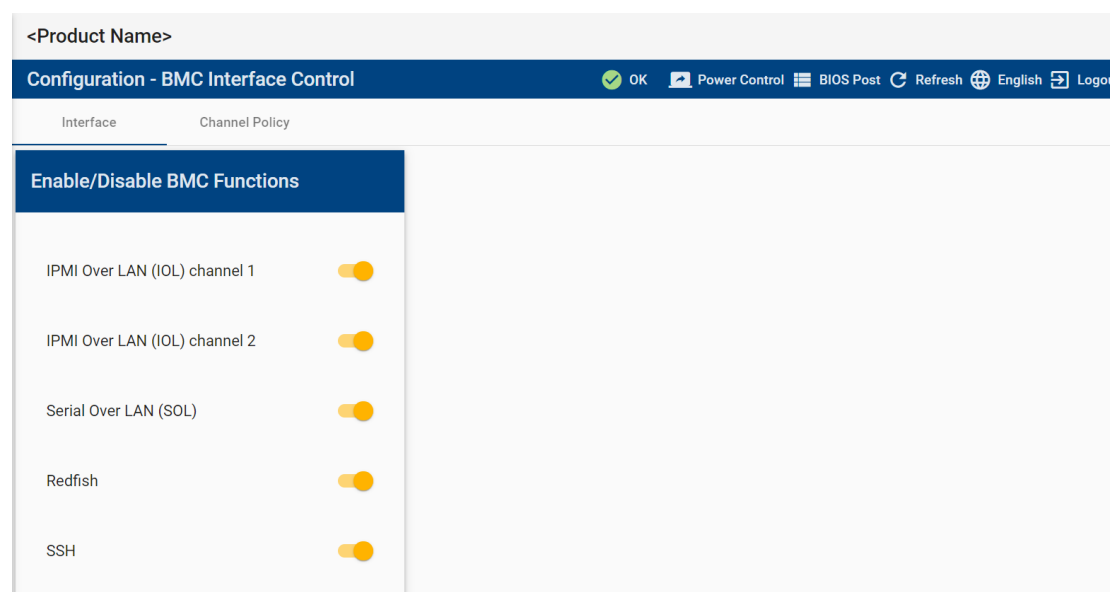


Figure 69: BMC Interface Control

3.4.5.2 Channel Policy tab

This page lists all unauthenticated BMC channels and provides the configuration options so user can change the policy for these unauthenticated channels according to needs.

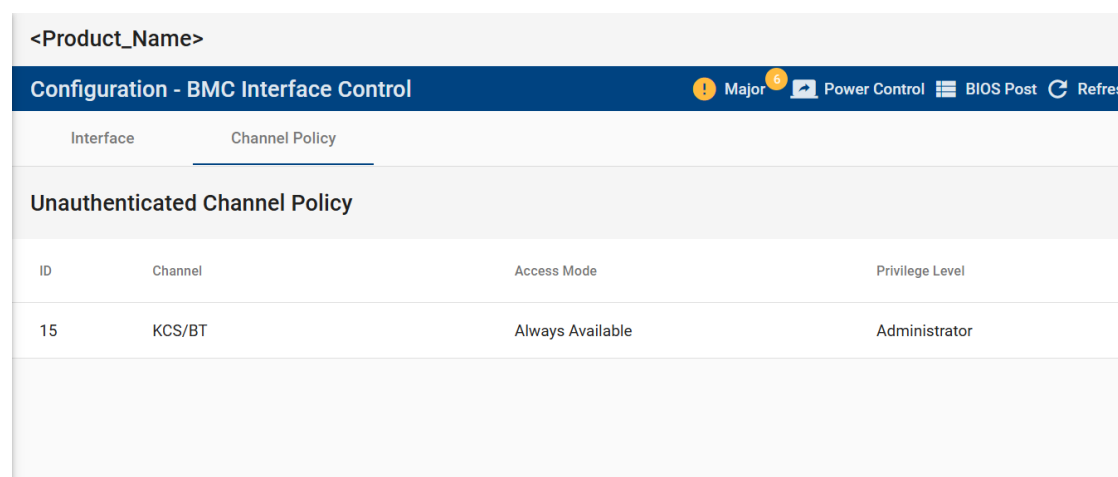
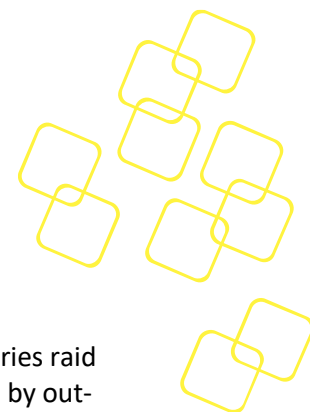


Figure 70: BMC Channel Policy



3.4.6 RAID Management

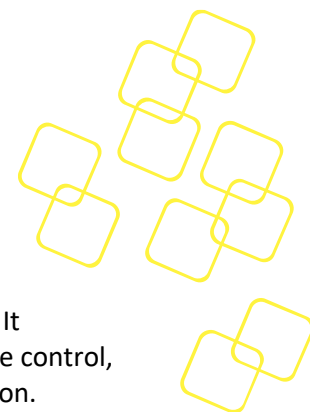
The **Configuration – RAID Management** page provides RAID Information and RAID Configuration. This configuration supports for Broadcom AVAGO MegaRAID SAS series raid card. It helps user to simply obtain RAID related information, and control RAID card by out-of-band management. The feature is available after nodeexp-1.24.0.

3.4.6.1 RAID INFO Tab

RAID INFO tab provides drive group information. Each group includes the drive group index number, RAID level, logical device (virtual drive) count, physical device count, hot-spare drive count, and available free size. It also provides detailed information of sub-category, including which logical devices belong to this virtual drive group, which physical devices to construct this virtual drive group, and also hot-spare drives to support this virtual drive group.

Configuration - RAID Management		
- Overview - Health - Advanced Inventory - Sensor Status - Event Log - Web Alert - Session - Configuration - Alerts - Network - Extra Configurations - Maintenance - BMC Interface Control RAID Management - Remote Control - System Power Control - Front Panel - iKVM Redirection - Remote Serial Console	RAID INFO	
	Drive Groups #0	Drive Groups #1
	- RAID Level 1 - LD Count 1 - PD Count 2 - HS Drive Count 1 - Available Size 272.5625 GB	- RAID Level 10 - LD Count 1 - PD Count 4 - HS Drive Count 1 - Available Size 57.4375 GB
	Logical Drives - Logical Drives #0 - Virtual Drive ID : 0 - Name : RAID_BIOS - Size : 25.0000 GB	Logical Drives - Logical Drives #0 - Virtual Drive ID : 1 - Name : RAID_Nodeexp - Size : 180.0000 GB
	Physical Drives - Physical Drives #0 - Physical Drive ID : 68 - Slot : P0:01:01 - PD State : ONLINE - Size : 297.5625 GB - Physical Drives #1 - Physical Drive ID : 97 - Slot : P0:01:00 - PD State : ONLINE - Size : 465.2500 GB	Physical Drives - Physical Drives #0 - Physical Drive ID : 67 - Slot : P0:01:02 - PD State : ONLINE - Size : 118.7188 GB - Physical Drives #1 - Physical Drive ID : 98 - Slot : P0:01:03 - PD State : ONLINE - Size : 698.1250 GB
	HS Drives - HS Drives #0 - HS Drive ID : 73 - Slot : P1:01:05 - Type : Global, Affinity	- Physical Drives #2 - Physical Drive ID : 74 - Slot : P1:01:04 - PD State : ONLINE - Size : 931.0000 GB - Physical Drives #3

Figure 71: Configuration - RAID Management –RAID INFO Page



3.4.6.2 RAID CONFIG Tab

RAID CONFIG tab provides configuration of virtual drive out-of-band management. It provides most important features, including creating RAID, assigning hot-spare drive control, locating the drive with lighting up drive LED, deleting RAID, and clearing configuration.

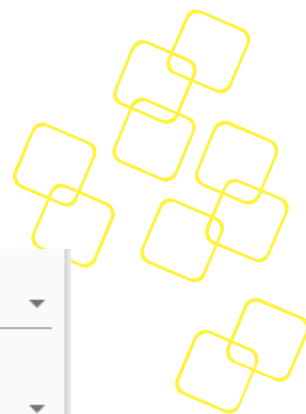
The screenshot displays the 'Configuration - RAID Management' interface. The left sidebar contains a navigation menu with categories like Health, Configuration, Alerts, Network, Extra Configurations, Maintenance, BMC Interface Control, RAID Management (selected), Remote Control, System Power Control, Front Panel, iKVM Redirection, and Remote Serial Console. The main content area is divided into several functional tabs: 'Create RAID', 'Hot Spare Control', 'Locate Drive', 'Delete RAID', and 'Clear Configuration'. The 'Create RAID' tab is active, showing fields for 'Virtual Drive Name' (with a 15-character limit), 'Enable Span' checkbox, 'RAID Level' dropdown, 'Physical Device Per-Span' dropdown, 'Select Drive' dropdown, 'Virtual Drive Size' (256K), 'Unit in Gigabyte' (0 GB), 'Max Available Size' (0 GB), 'Read Policy' (Read Ahead), 'Write Policy' (Write Back), 'I/O Policy' (Direct), 'Disk Cache Policy' (Unchanged), 'Emulation Type' (Default), 'Disable BGI' (No), 'Default Initialization' (No), and 'Enable Data Protection' (Disable). The 'Hot Spare Control' tab includes 'Assign Global Hot Spare', 'Remove Global Hot Spare', 'Assign Dedicated Hot Spare', and 'Remove Dedicated Hot Spare' sections. The 'Locate Drive' tab has 'Start Locate Physical Drive', 'Stop Locate Physical Drive', 'Start Locate Virtual Drive', and 'Stop Locate Virtual Drive' sections. The 'Delete RAID' tab has a 'Delete' button. The 'Clear Configuration' tab has a 'Clear' button and a confirmation message.

Figure 72: Configuration - RAID Management –RAID CONFIG Page

3.4.6.2.1 Create RAID

To create RAID by user input parameters, all parameters are required to activate the create button.

- 1) Virtual drive name should be less than 15 characters.
- 2) Enable span checkbox can control whether to use span raid level.
(Span: 00/10/50/60, Not Span: 0/1/5/6)
- 3) If span is enabled, user needs to decide how many physical devices per-span to be used.
- 4) By different raid level selection, providing minimum device count to indicate user how many physical devices is needed.
- 5) By different raid level and physical drive selection, providing maximum available virtual drive size to indicate user how many space is available after this virtual drive is created.



Create RAID	
Virtual Drive Name	
Max 15 Characters	0/15
☐ Enable Span	
RAID Level	▼
Physical Device Per-Span	▼
Select Drive	▼
Min Device Count : 0	
Virtual Drive Size	GB
Unit in Gigabyte	Max Available Size : 0 GB
Strip Size	
256K	▼
Read Policy	
Read Ahead	▼
Write Policy	Write Back ▼
I/O Policy	Direct ▼
Disk Cache Policy	Unchanged ▼
Emulation Type	Default ▼
Disable BGI	No ▼
Default Initialization	No ▼
Enable Data Protection	Disable ▼
Create	

Figure 73: RAID Management - RAID CONFIG – Create RAID

3.4.6.2.2 Delete RAID

To delete RAID by selecting virtual drives and activating the delete button.

Delete RAID
Select Virtual Drive ▼
Delete

Figure 74: RAID CONFIG – Delete RAID

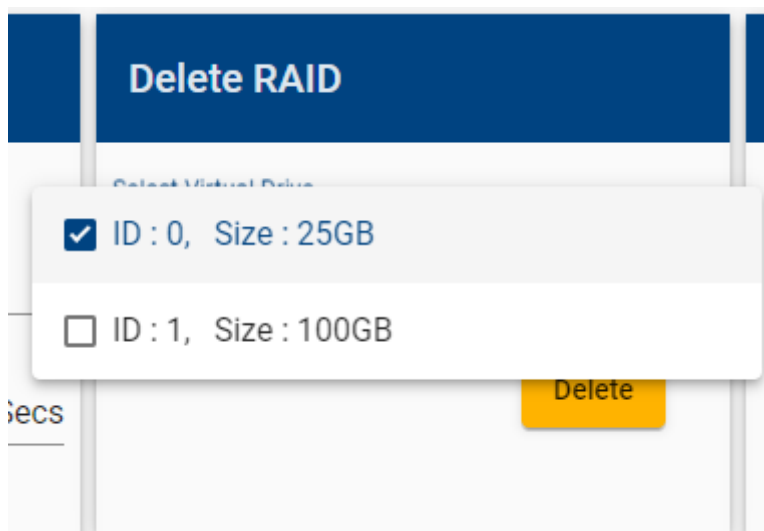
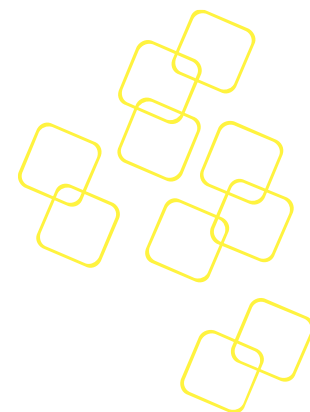


Figure 75: RAID CONFIG – Delete RAID – Select Virtual Drive

3.4.6.2.3 Clear Configuration

Clear configuration will delete all configurations on the raid controller, including virtual drive group setting, virtual drive setting, physical drive setting and hot-spare drive setting.

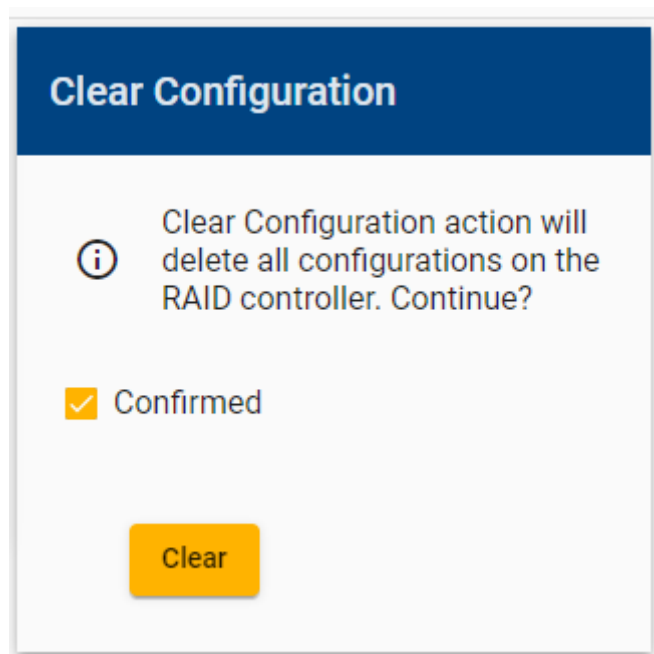
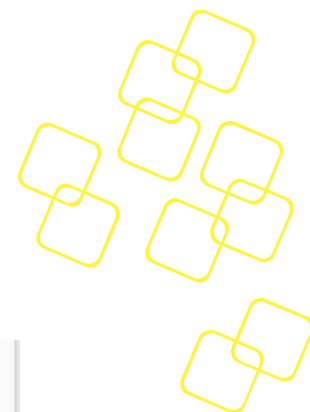


Figure 76: : RAID CONFIG – Clear Configuration

3.4.6.2.4 Hot Spare Control

Hot spare control can assign and remove the dedicated or global hot spare drive to a specific virtual drive group or all virtual drive group.



Hot Spare Control

Assign Global Hot Spare

Select Drive

ID : 67, Available Size : 118.71875GB

Choose one drive to make global hot spare

Assign

Remove Global Hot Spare

Select Drive

ID : 73, Category : Global

Choose one global hot spare drive to remove

Remove

Assign Dedicated Hot Spare

Select Drive Group

ID : 0, RAID : 1, Not Span

Choose one drive group

Select Drive

ID : 72, Available Size : 465.25GB

Choose one drive to make dedicated hot spare

Assign

Remove Dedicated Hot Spare

Select Drive

ID : 74, Category : Dedicated

Choose one dedicated hot spare drive to remove

Remove

Figure 77: RAID CONFIG – Hot Spare Control

3.4.6.2.5 Locate Drive

Locate drive can start / stop locate physical drive and logical drive. The locate period is from 0 (locate forever) to 255 secs.

Locate Drive

Start Locate Physical Drive

Select Drive

1 Drive Selected

Choose physical drive to start locate

120 Secs

Locate Period :0~255 Secs (0 means forever)

Start Locate

Stop Locate Physical Drive

Select Drive

1 Drive Selected

Choose physical drive to stop locate

Stop Locate

Start Locate Virtual Drive

Select Virtual Drive

Choose virtual drive to start locate

120 Secs

Locate Period :0~255 Secs (0 means forever)

Start Locate

Stop Locate Virtual Drive

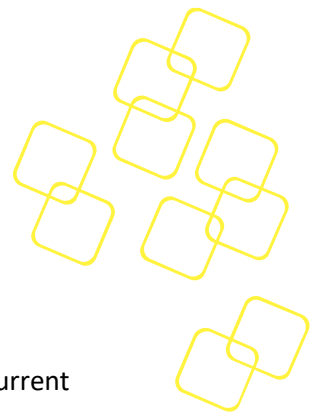
Select Virtual Drive

1 Virtual Drive Selected

Choose virtual drive to stop locate

Stop Locate

Figure 78: RAID CONFIG – Locate Drive



3.5 Remote Control Session

3.5.1 System Power Control

The x86 payload host status, including the host power state, BIOS POST code, and current BIOS boot device are displayed on the **System Power Control** page.

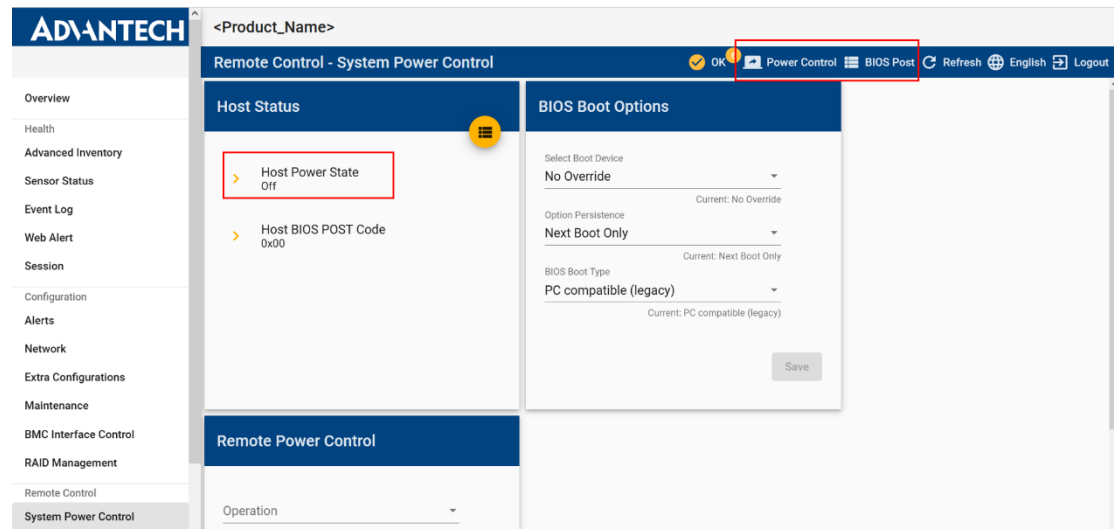


Figure 79: Server Power Control Page

BIOS POST code are data values used to indicate progress during the boot up phase. Beep codes and checkpoints for debugging can be found here:

[https://ami.com/ami_downloads/Aptio_4.x_Status_Codes_\(beep_checkpoint\).pdf](https://ami.com/ami_downloads/Aptio_4.x_Status_Codes_(beep_checkpoint).pdf)

By clicking the menu button , you can get, download or refresh the BIOS POST code history.

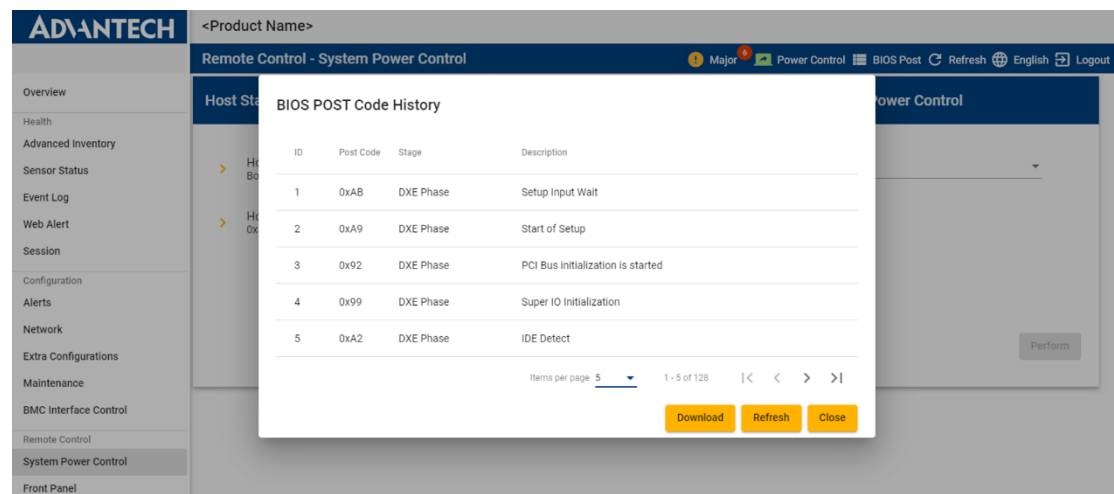
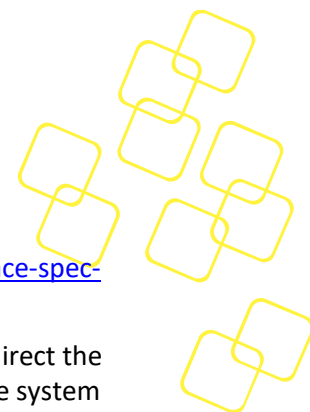


Figure 80: BIOS POST Code History dialog

For **BIOS Boot Options** see the definition of **Boot Option Parameters** (chapter 28.12 Set System Boot Options Commands and table 28-14) in IPMI specification v2.0 available from:



<https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-second-gen-interface-spec-v2-rev1-1.html>

You can select different BIOS boot devices, which are used to set parameters that direct the system boot following a system power up or reset. The boot flags only apply for one system restart. It is the responsibility of the system BIOS to read these settings from the BMC and then clear the boot flags. Press the **Save** button and the BIOS will save your boot options and boot from the selected device during the next boot.

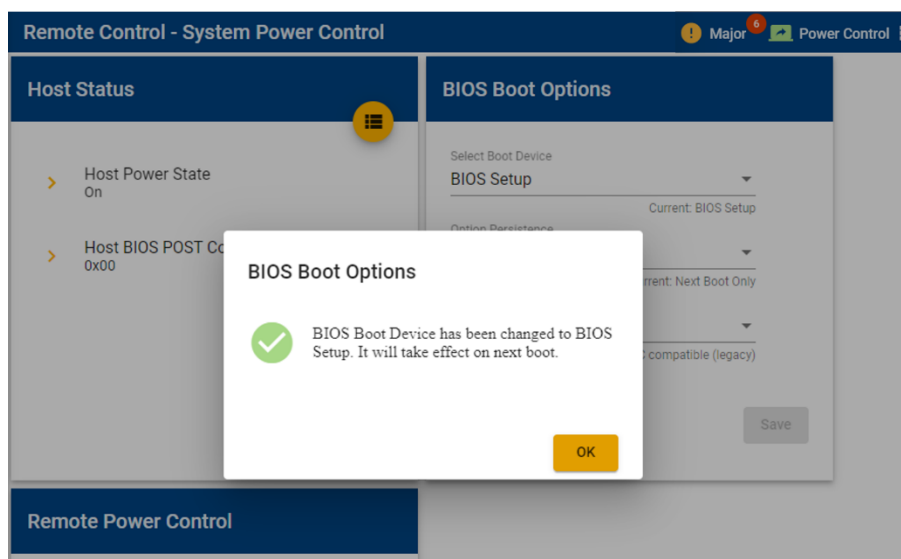
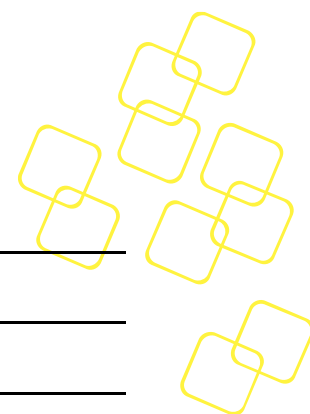


Figure 81: BIOS Boot Options are Saved

Please note some boot options are not supported with standard BIOS. If you need further features support, please send a customization request to your Advantech representative.

BIOS Boot Options	Support with Advantech standard BIOS
No Override	Supported
Force PXE	Supported
Remote Hard Drive	NA. Needs customized BIOS
Default Hard-drive	Supported (incl. USB-HDD)
Default Hard-drive, Safe Mode	Supported (incl. USB-HDD)
Default Diagnostic Partition	N.A.
Default CD/DVD	Supported (incl. USB-CD/DVD)
Remote CD/DVD	N.A. Needs customized BIOS
Primary Removable Media	N.A. Needs customized BIOS



Remote Primary Removable Media	N.A. Needs customized BIOS
Primary Remote Media	N.A. Need customized BIOS
BIOS Setup	Supported

The Host power status will be displayed in **Host Status** session and also as an icon at the right-topside of the web interface.

	Green	On (power is on and no error from BIOS)
	Gray	Off
	Red	Error

Power and reset control options can be controlled from the **Remote Power Control** session. Available options are as follows:

- Reset
- Power off
- Power cycle
- Power on
- Graceful shutdown
- Remote Boot

Select an appropriate power option and then click **Perform** to execute the command immediately.

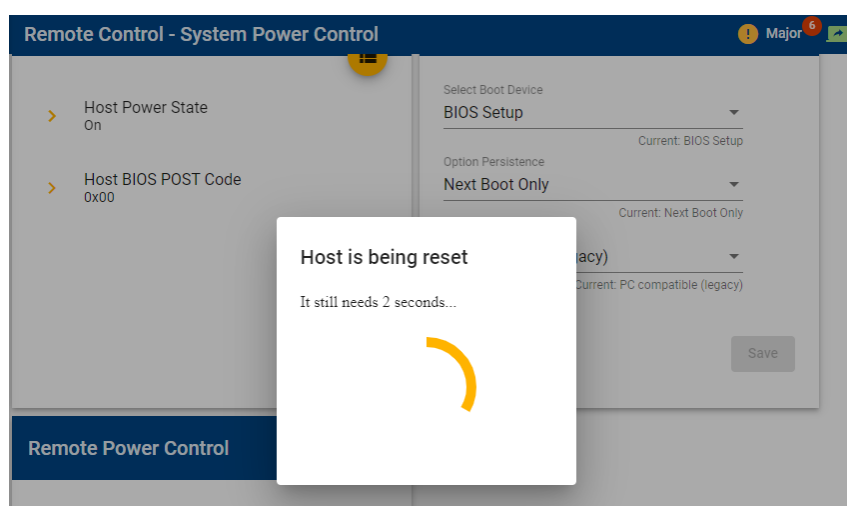
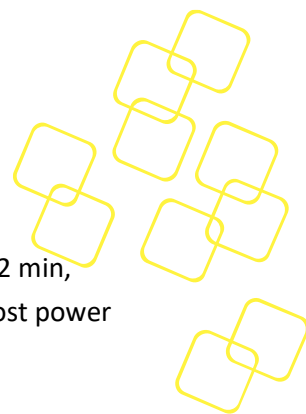


Figure 82: Server Power Action Countdown

For any control command, Node Explorer will disable all user inputs for 3 seconds (a countdown will be displayed) once **Perform** has been pressed, it will then wait until the selected power action is completed.



The host power status and icon will keep updating every 1s during operation. After 2 min, the status will only be updated when you press the **Refresh** button  beside the host power status icon.



3.5.2 Front Panel

This is a setting to identify what platform by controlling the LED light on the front panel.

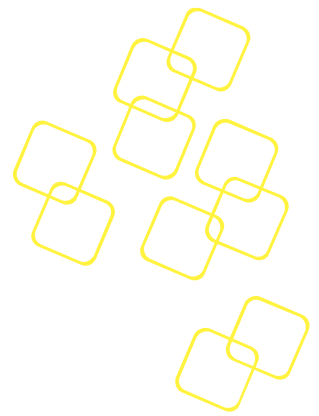
Figure 83: Front Panel Page

Users can set the Identify LED on the **Chassis Identification tab** as Figure 84. Options can be set as Force ON (always on) until you set Force OFF or set the interval of the LED blinking.

Figure 84: Chassis Identification tab

Users can set the Alarm Status LED (System LED) on the Chassis Alarm Status tab as Figure 85. Options can be set as Always On, or Always Off, or reset.

- Always On : Alarm Status LED forced on



- Always Off : Alarm Status LED forced off
- Reset : clear the asserted events to reset default behavior

A screenshot of a web interface titled "Chassis Alarm Status". Below the title is a section labeled "LED Control Options". This section contains three radio button options: "Reset", "Always On", and "Always Off". The "Reset" option is currently selected. At the bottom right of the form is a yellow "Submit" button.

Chassis Alarm Status

LED Control Options

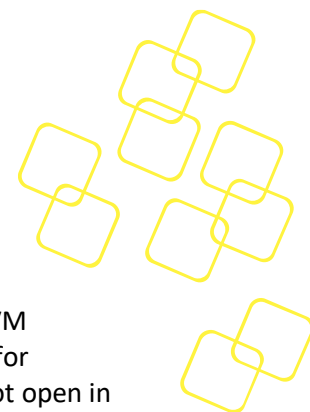
☒ Reset

☐ Always On

☐ Always Off

Submit

Figure 85: Chassis Alarm Status



3.5.3 iKVM Redirection

From this page, you can click **Open iKVM Redirection** to pop out the Advantech iKVM redirection client directly, which supports keyboard, video, and mouse redirection for remote control. The iKVM screen will open in a new tab. If the iKVM screen does not open in a new tab, check whether the pop-up window has been blocked by your browser.

Note 1: The iKVM inactive timeout is configurable; the default timeout is 900s (15 min).

Please refer to 3.4.3.9 The Session Timeout Tab.

Note 2: The iKVM mouse pointer will be a normal arrow.

After the splash screen appears, the iKVM console screen will be shown:

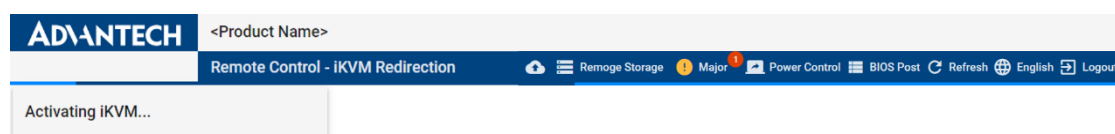


Figure 86: Redirecting

Please check if pop-ups were blocked on this page as shown below.

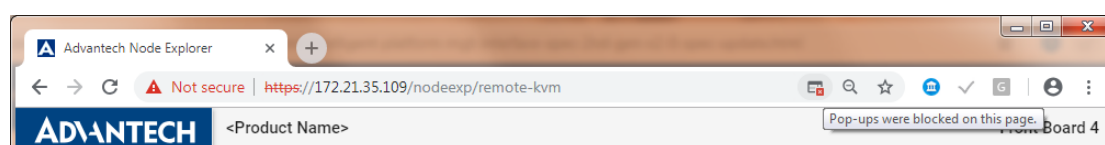
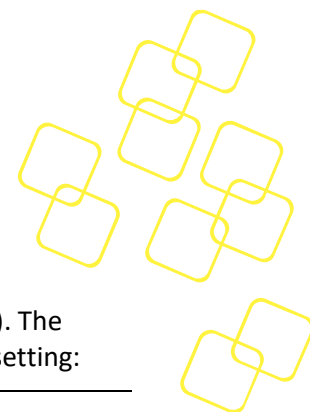


Figure 87: Pop-ups Were Blocked On This Page.



Figure 88: iKVM Screenshot Example: Graphic UI



3.5.3.1 iKVM functionality

iKVM settings menu is located at the bottom-left corner on iKVM screen (Figure 89). The tooltip for each setting will be displayed when the mouse cursor hovers over each setting:

 Close iKVM	Close iKVM connection. "Disconnected" will be shown on the screen in disabled mode as Figure 90
 Image Quality (%)	Lowering the Jpeg quality improves performance, whereas higher quality setting means more bandwidth and computing power are required, which can reduce performance.
 Key Press Mode	Enable/disable key-press mode. Enable this when network conditions are slow in order to enhance keyboard usability. This feature is designed to help you to manually set the bandwidth in situations where network connection performance is limited or when BMC performance is poor.
 Keyboard	Show/hide soft keyboard. Currently, US and DE keyboards are supported. You can switch to a different keyboard by right-clicking on the soft keyboard. 
 Frame Rate	Choose the frame rate. Users can increase the frame rate to get better frame frequency or decrease the frame rate to get better data transfer performance.
 Full-screen	Enter full-screen mode
 Capture keyboard input	Keyboard input is redirected to the x86 host when the icon shows.

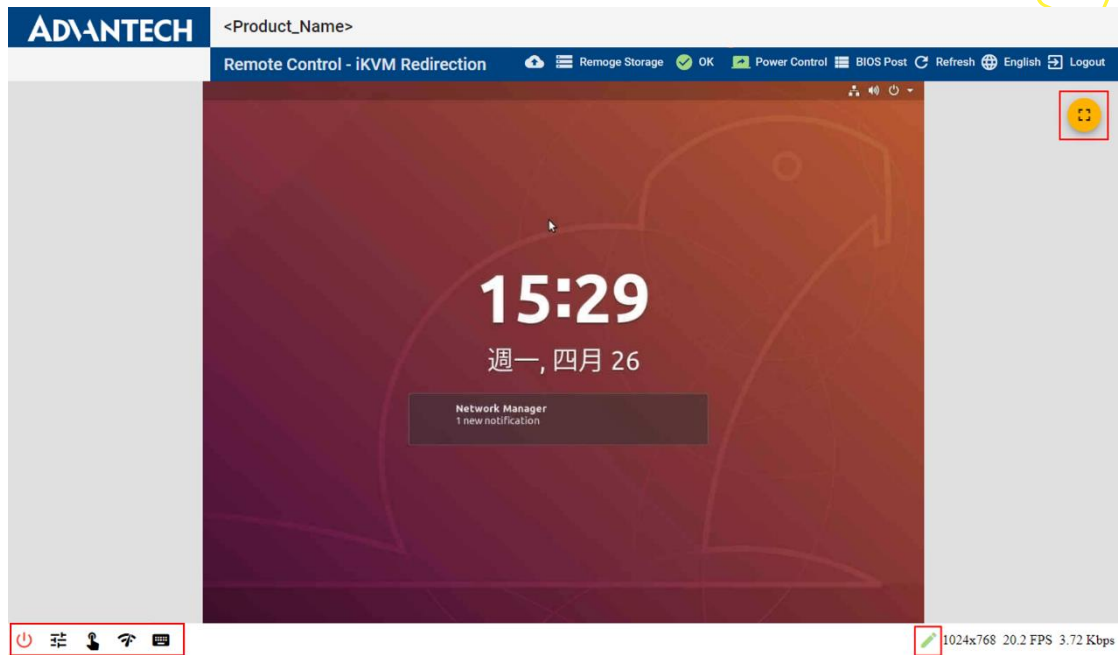


Figure 89: iKVM Redirection Settings Buttons



Note: If you get the message on the screen below, it means iKVM has timed out. Just click the undo icon to re-open iKVM.

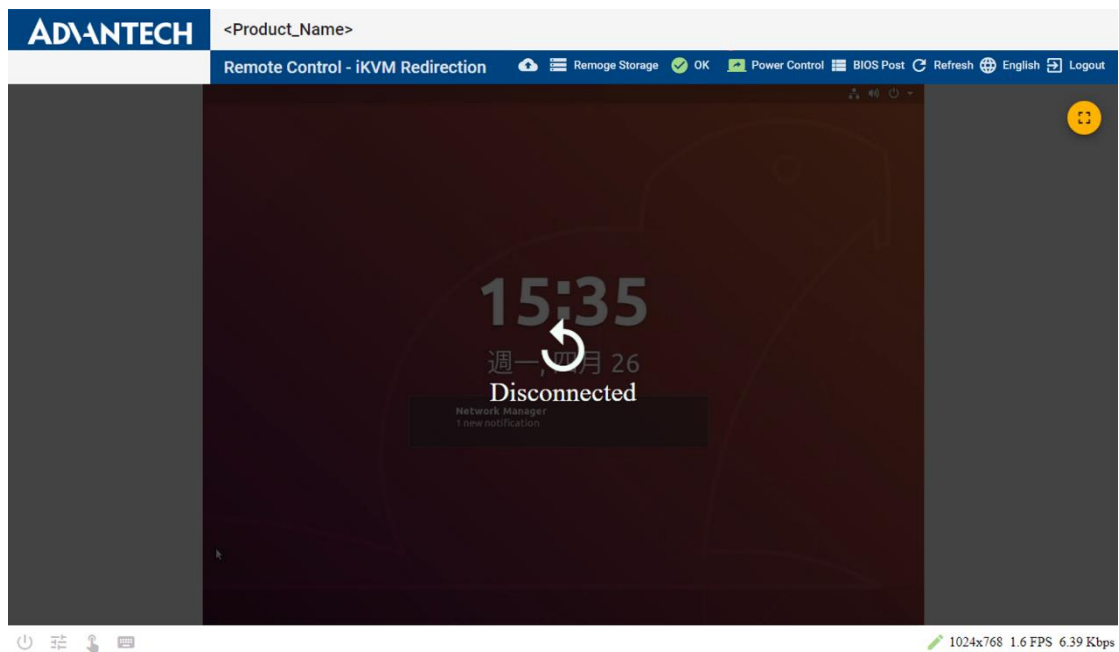
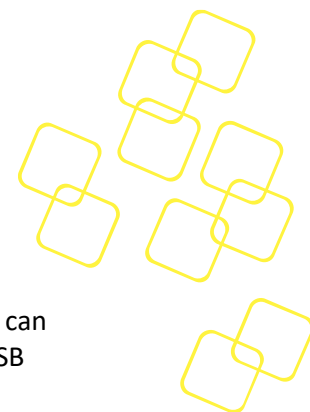


Figure 90: iKVM is Disconnected Because of Timeout or Shutdown



3.5.3.2 Remote Storage

The Remote Storage page allow you to mount remote storage as CD-ROM (i.e., you can mount remote ISO as a boot device for payload OS.) After connecting, the virtual USB storage device is shown in remote devices via 3.5.3 iKVM Redirection.

Note: the maximum capacity of remote storage is 8GB.

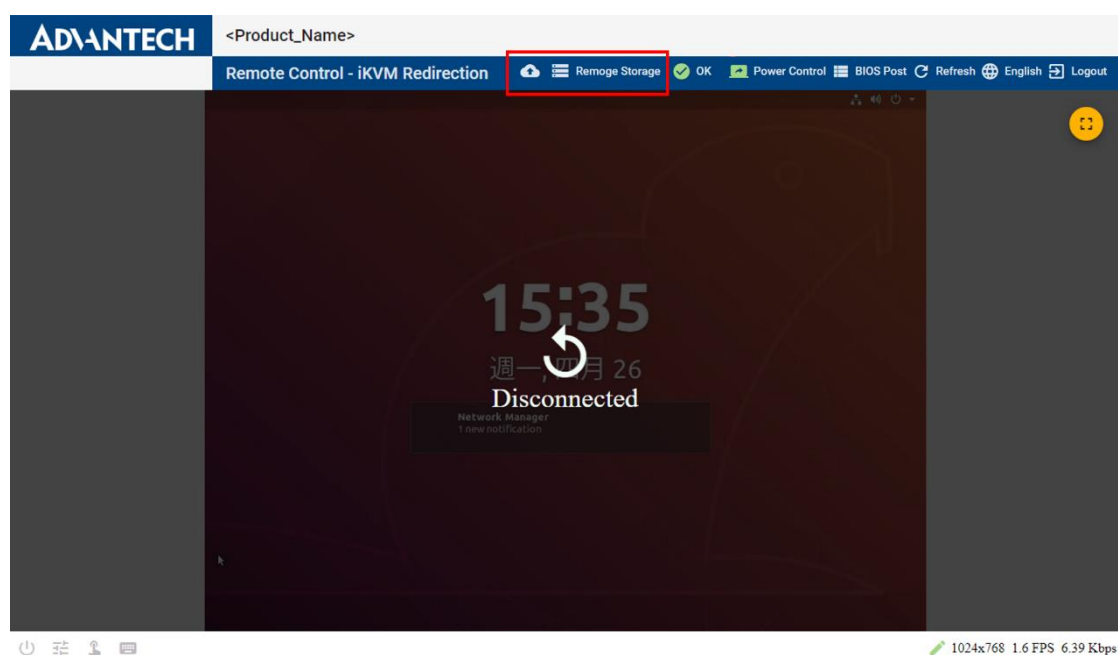


Figure 91: Remote Storage functionality

Via Windows File Share (SMB)

The Server Message Block (SMB) protocol is a network file-sharing protocol as implemented in Microsoft Windows, it is known as the Microsoft SMB Protocol.

After you have filled in the necessary information for the SMB server, including the share IP address, image file, domain name, user name, and password, and you have pressed **Insert** (see Figure 92), Advantech BMC will connect the SMB server and mount the image file to the payload automatically.

The format of remote storage configuration should follow the rule below.

- SMB share address: //<Host Address>/<Share Name>
- Path to image file: relative to the shared folder, path/to/image.file
- Domain: If it is left empty, "WORKGROUP" will be used.

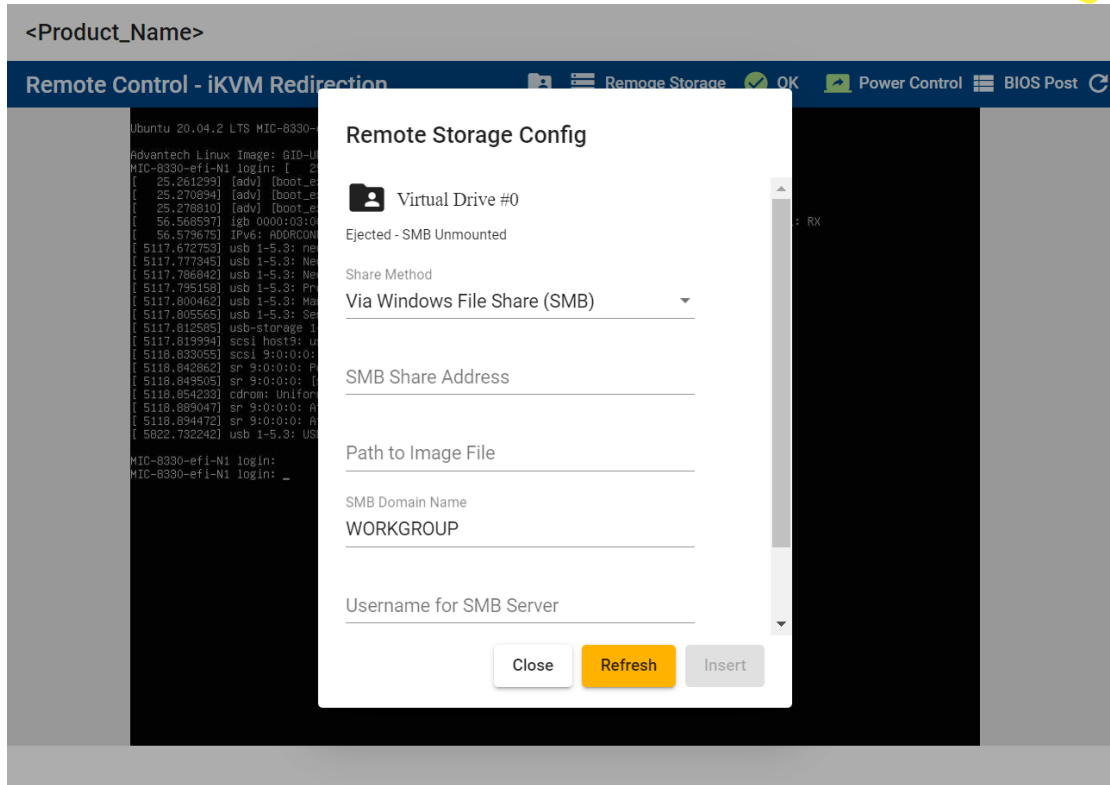
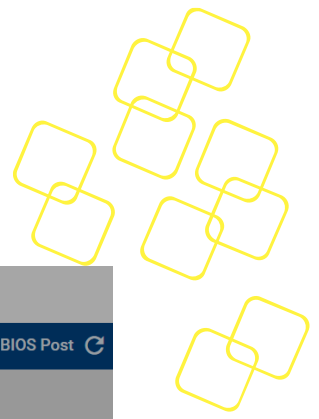
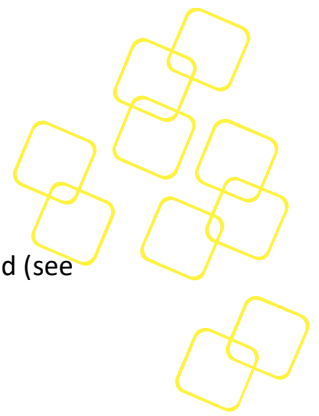


Figure 92: Remote Storage Connected via SMB

Once the virtual device has been mounted successfully, the status icon  beside Virtual Drive #0 will become green icon .

	SMB is unmounted / ejected. The icon is status bar will be white icon. 
	Mounting SMB
	SMB is mounted to the x86 payload.



You will be notified whether it is successful (see Figure 93) or if an error has occurred (see Figure 94).

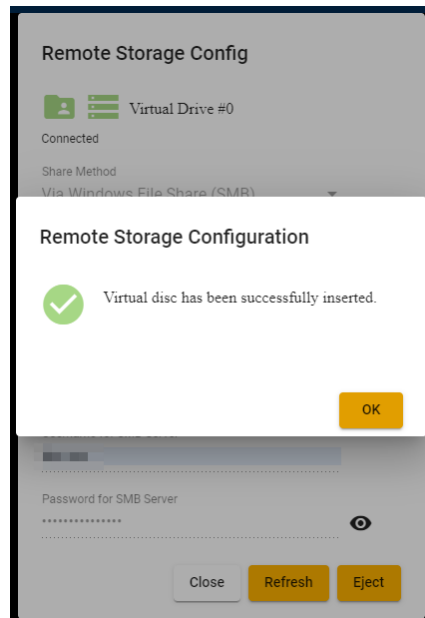


Figure 93: Remote Storage (SMB) Successfully Mounted

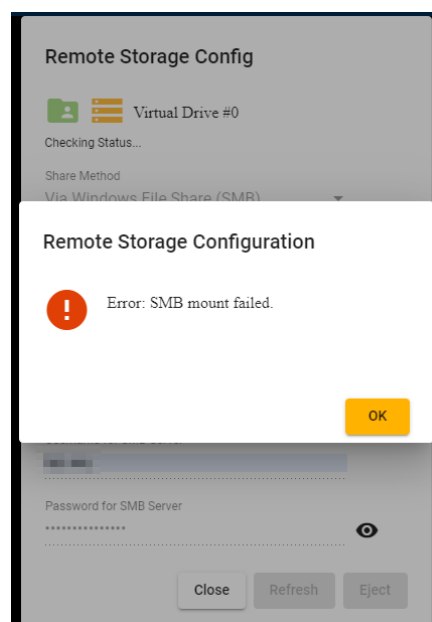


Figure 94: Remote Storage (SMB) Mount Failed

If you press **Eject**, the virtual device will be disconnected and dialog with, “Virtual disc has been successfully ejected” will be shown as Figure 95.

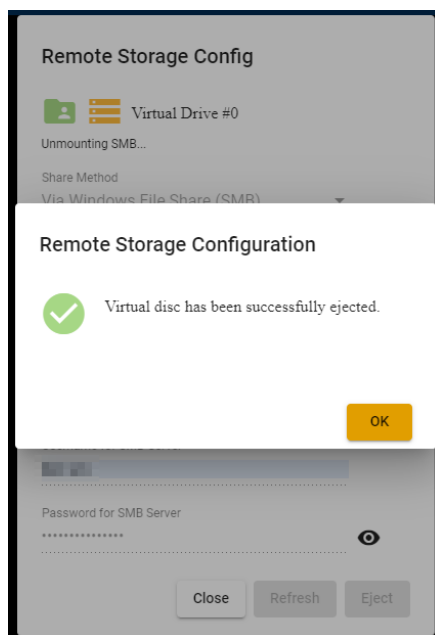
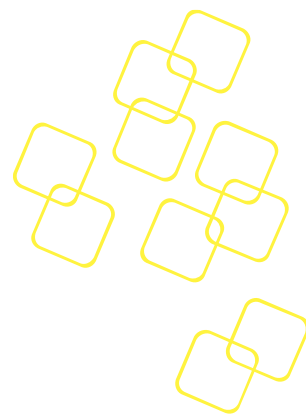


Figure 95: Remote Storage (SMB) Disconnected

Note: Only one administrator can insert a remote image at the same time.

The other administrator will see the message as Figure 96: The Remote Image (SMB) is Connected. To unblock the upload functionality, you need to click the **Eject** button.

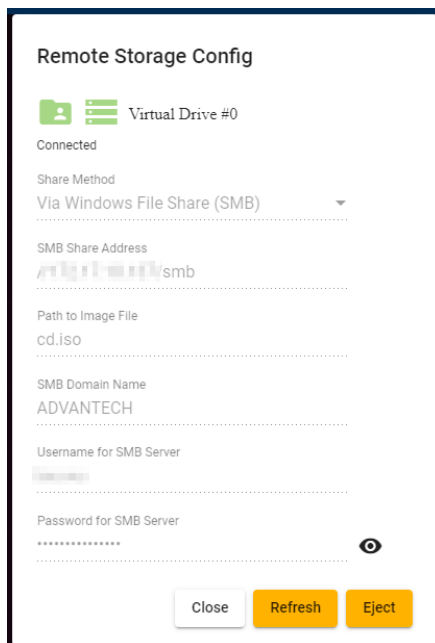
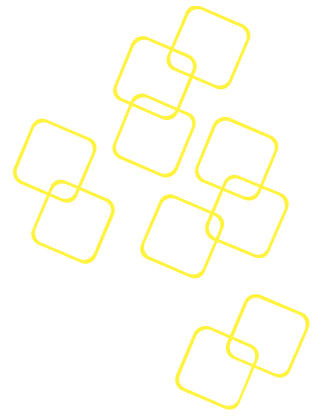


Figure 96: The Remote Image (SMB) is Connected



Via Web

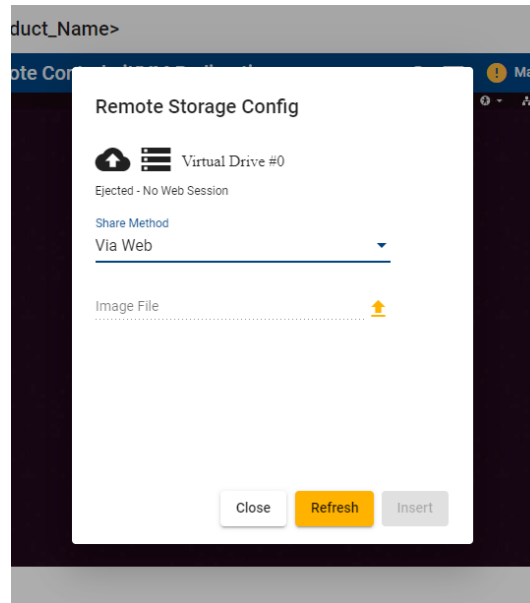


Figure 97: Remote Storage (Web)

To mount the remote storage via the web, there are two separate steps:

1. Press  to specify an image file from local storage (as shown in Figure 98) and press **Insert** to establish a connection between the web session, Advantech BMC, and the x86 payload, then mount the image file to load the payload as a virtual device.

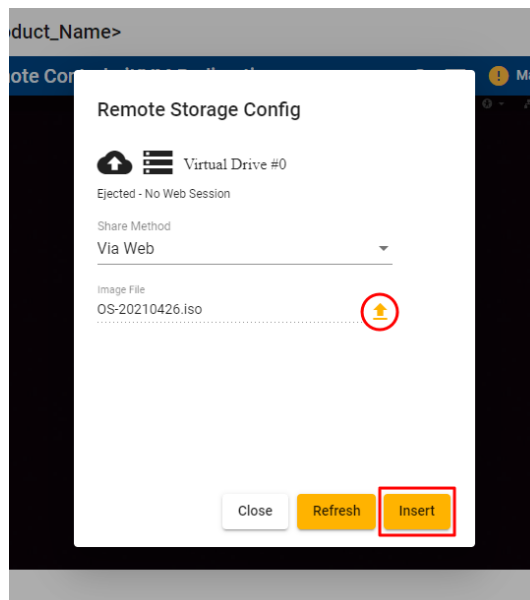
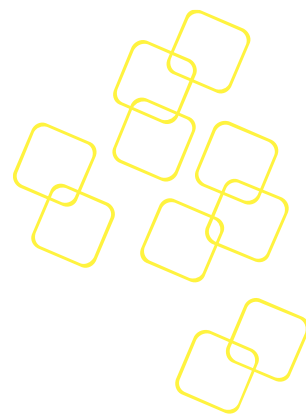


Figure 98: Selecting an Image File for Remote Storage (Web)

2. Once the virtual device has been mounted successfully, the Status icon  beside Virtual Drive #0 will turn green, the dialog box "Virtual disc has been successfully inserted" will appear and the image shown in web session dialog will be uploaded as in Figure 99. The



web session dialog can be closed but will stay connected when you click **Close**.

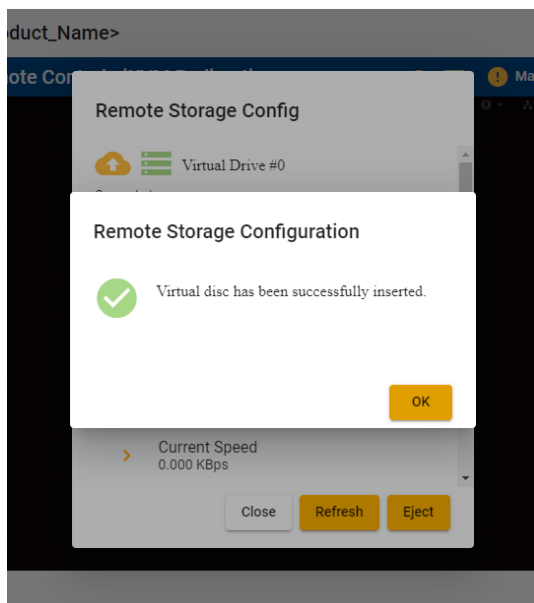


Figure 99: Virtual Drive Successfully Mounted via Remote Storage (Web)

Note: Only one administrator can insert a remote image.

The other administrator will see the status as in Figure 100: The Remote Image (Web) is provided by another Client. To insert a new image, you need to disconnect the current image by clicking **Eject**.

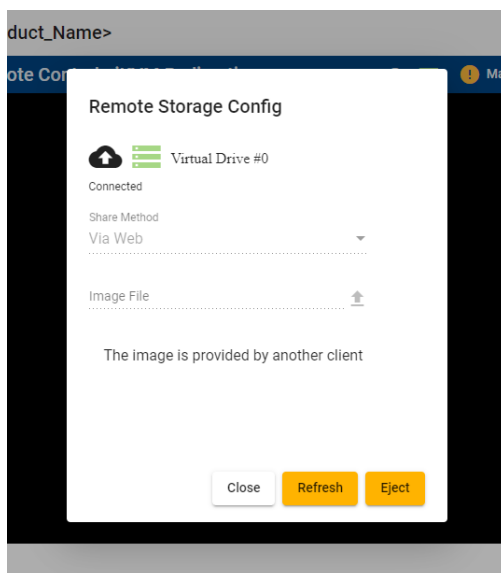
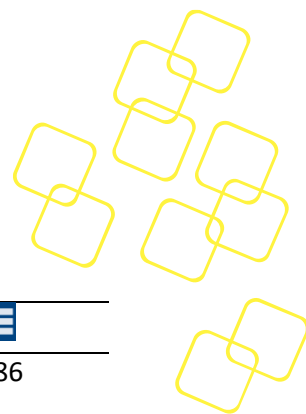


Figure 100: The Remote Image (Web) is provided by another Client



These icons beside the Virtual Drive # show different connectivity status.

	There is no web session. The icon on the status bar will be a white icon. 
	Connecting web session, Advantech BMC, and inserting the disc into the x86 payload
	Web session is connected to the x86 payload.

The icon shows different colors according to the web client usage and speed.

	There is no web session. The icon status bar will be a white icon. 
	The disc is inserted into the x86 host but not used.
	x86 host is reading the file in disc with smooth web client speed.
	x86 host is reading the file in disc with slow web client speed.

To end the remote storage connection, complete the following steps:

1. Press **Eject** on the main page to disconnect Advantech BMC, x86 payload, and the web session completely.
2. These icons  will become black. Close the pop up window as shown in Figure 101 after disconnection.

*Note: After the remote storage is connected, you can disconnect the storage by clicking the **Eject** button in remote storage dialog or eject it in the x86 host OS.*

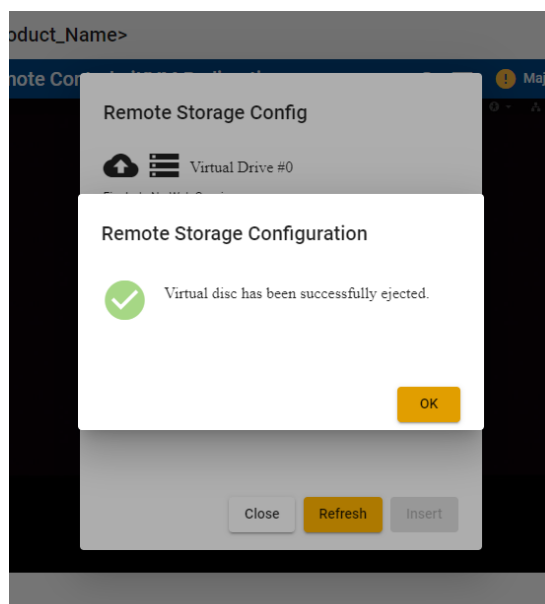
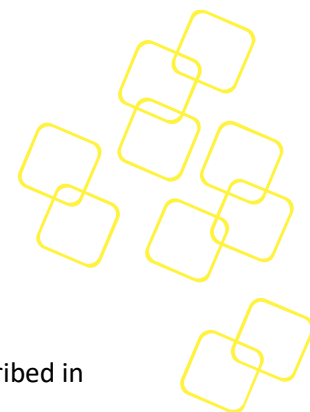


Figure 101: Virtual Drive Disconnected



After Mounting Remote Storage

To use remote storage, follow these steps:

1. Mount a remote storage such as USB storage and upload the image file as described in 3.5.3.2 Remote Storage.
2. Mount Remote Storage Via Windows File Share (SMB) or Via Web
3. Select **BIOS Boot Options** and reset x86 system as in 3.5.1 **System Power Control** page as Figure 102 or the power icon  in Tool bar at the right-topside of the web interface as in Figure 103. **Remote Boot** will boot from remote storage.

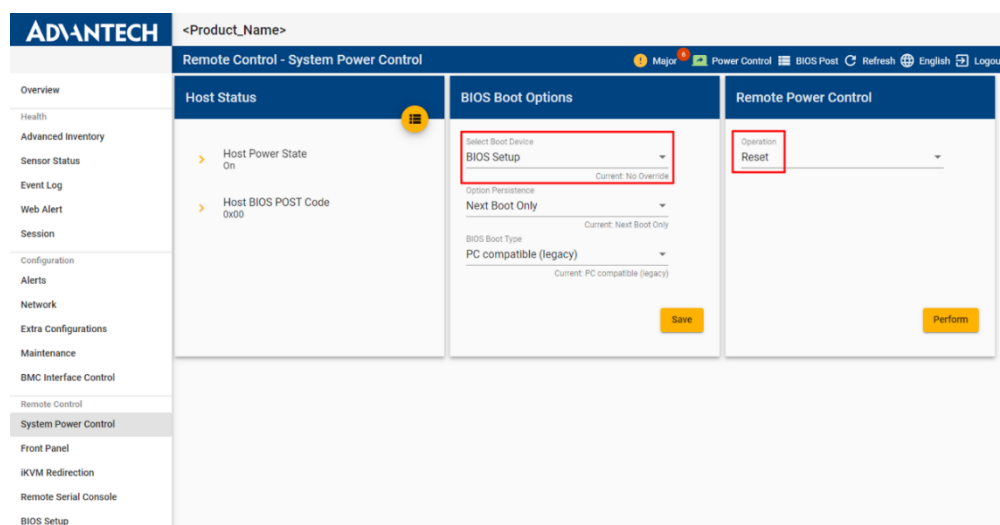


Figure 102: Restarting x86 Payload and Entering BIOS Setup Menu

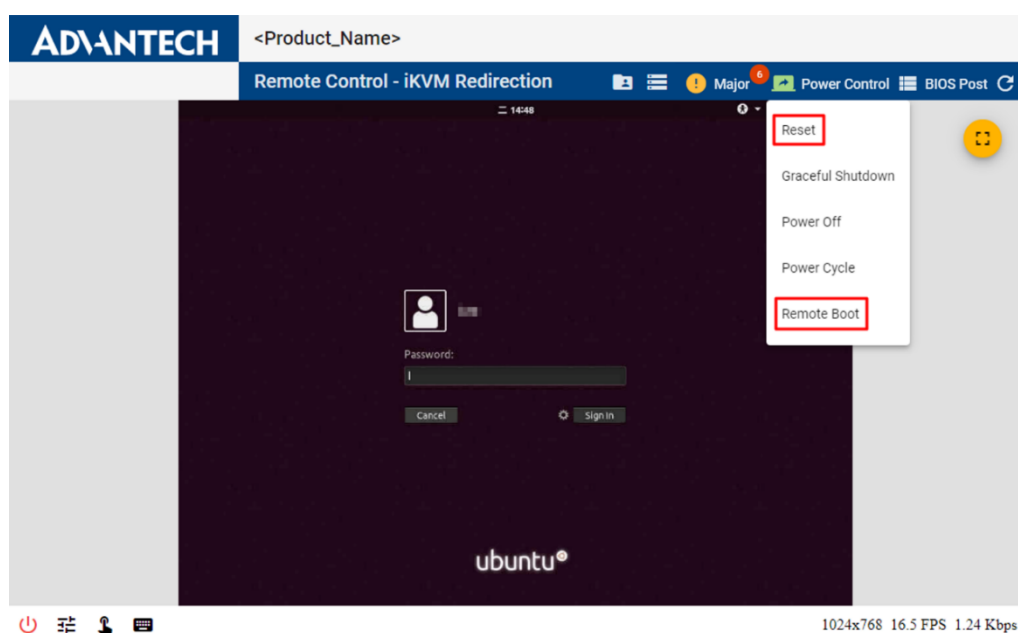


Figure 103: Restarting x86 Payload from Tool Bar and Entering BIOS Setup Menu

- Switch back to the screen on x86 payload as in 3.5.3 iKVM Redirection and you will see BIOS setup menu after the system reset. Choose rightmost **Save & Exit** tab, select the remote storage device in Boot override called **UEFI : Linux File-Stor Gadget 0414**, and then you can enter the installation page of the OS.

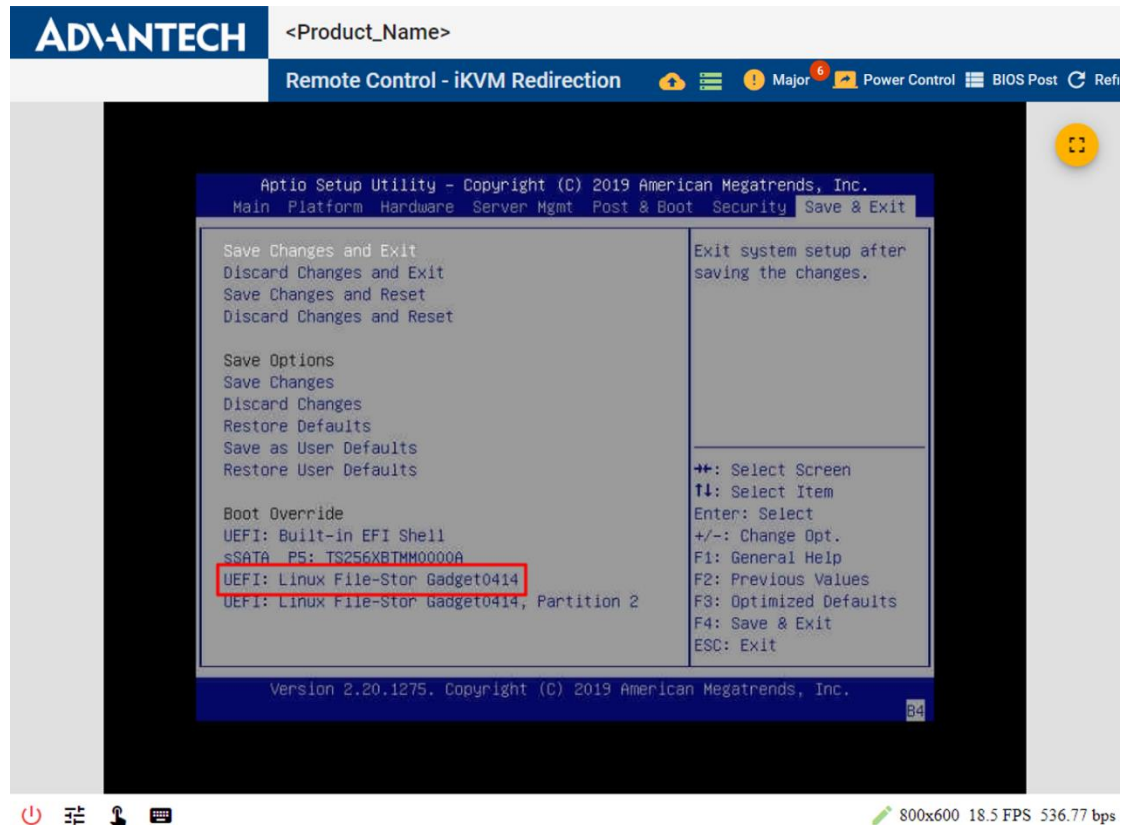
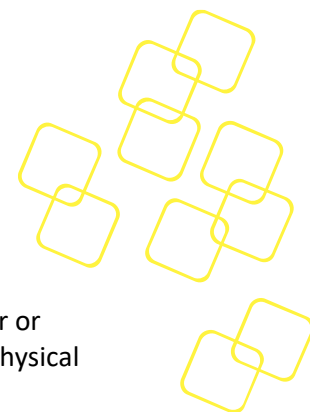


Figure 104: Select Remote Storage in BIOS Setup Menu



3.5.4 Remote Serial Console

The remote serial console is a connection that allows a person access to a computer or network device console over the web interface remotely instead of the RS-232 or physical serial port connection. The feature is available after nodeexp-1.19.0.

To access the console, follow the steps below:

1. Set up configuration in the OS. For example, you can refer to the setting on Internet. https://wiki.archlinux.org/index.php/working_with_the_serial_console
2. Make sure serial console in BIOS setup is enabled. Users can also configure it through iKVM remotely (refer to section 3.5.1 System Power Control).

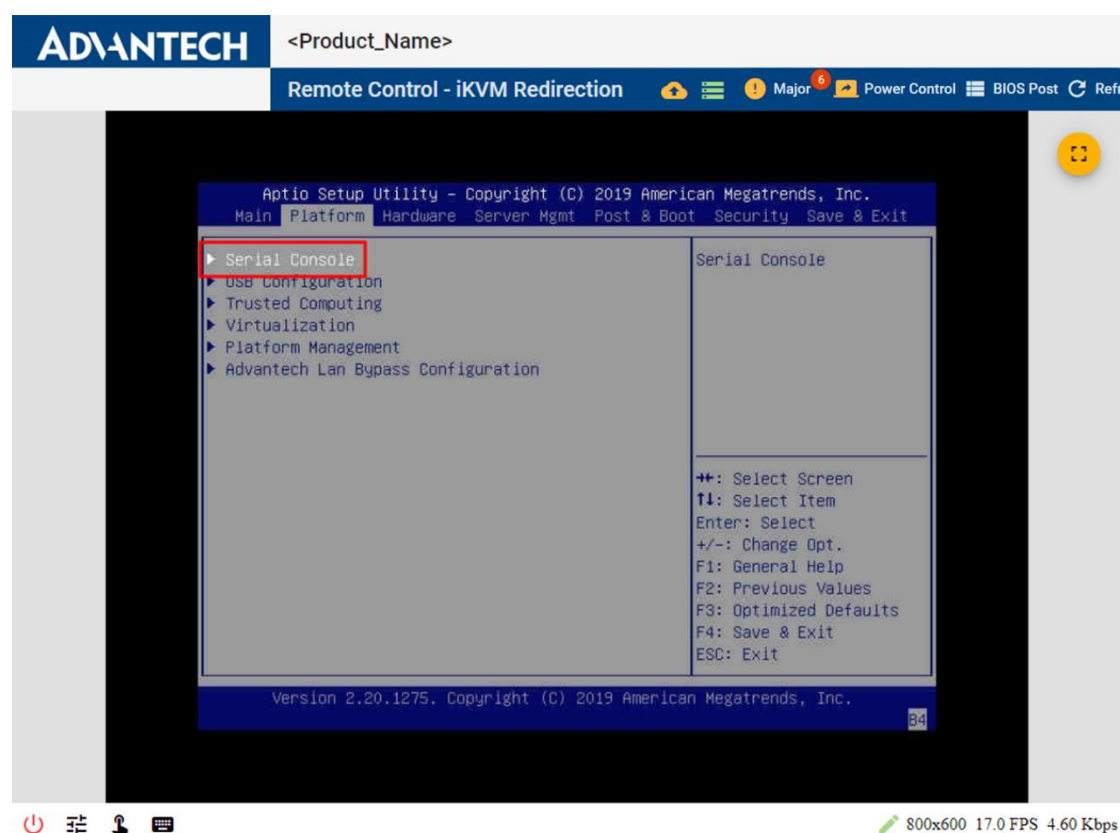


Figure 105: Serial Console in BIOS Setup Menu

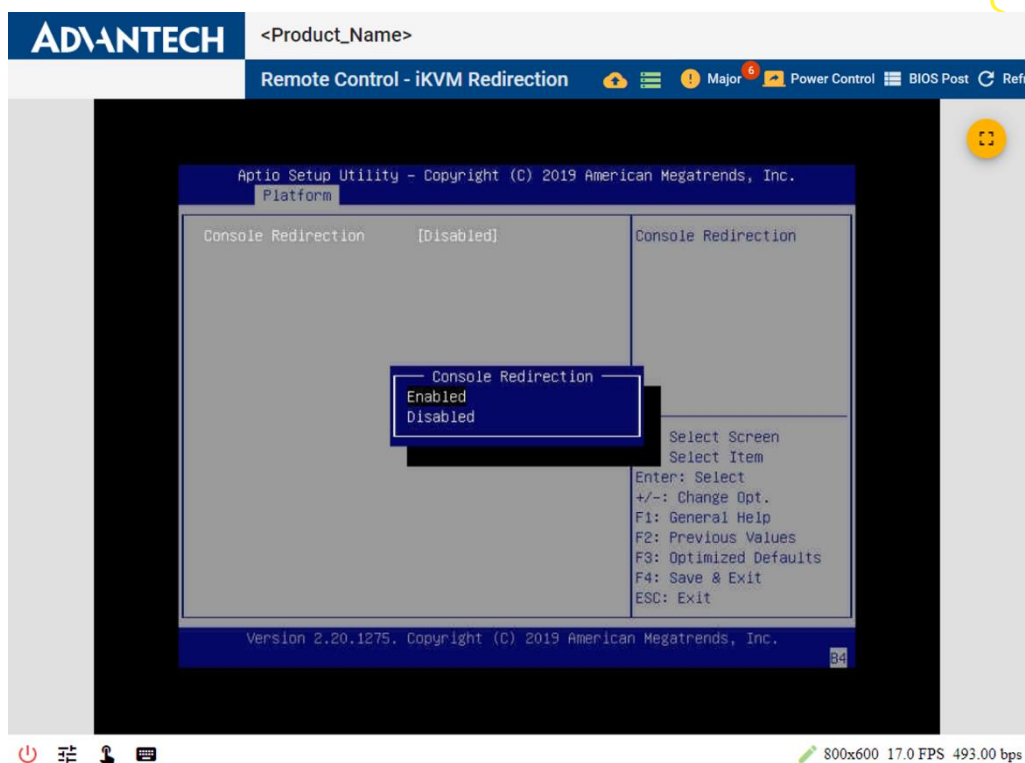


Figure 106: Enable Serial Console in BIOS Setup Menu

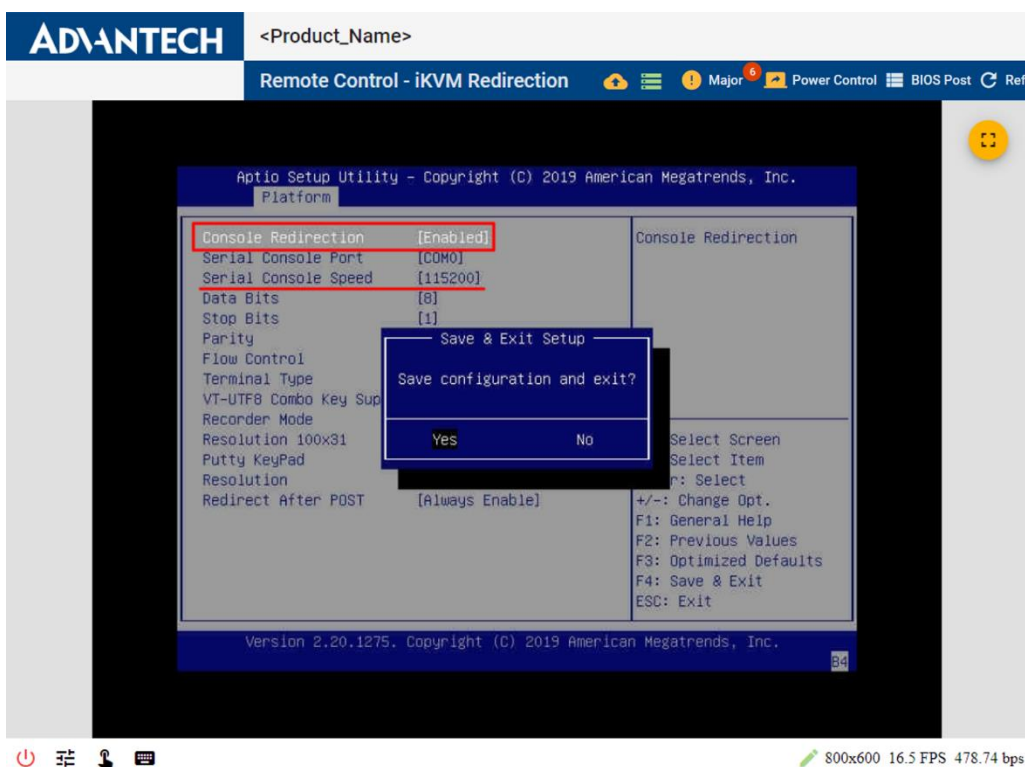


Figure 107: Save Serial Console Configuration in the BIOS Setup Menu



Open serial console session by clicking the **Remote Control** page in the left-side menu. To avoid timeouts, you can increase the **Inactive Timeout** referred to 3.4.3.9 The Session Timeout Tab.

Note: The baud rate in OS configuration, BIOS setup menu, and web interface should be aligned.

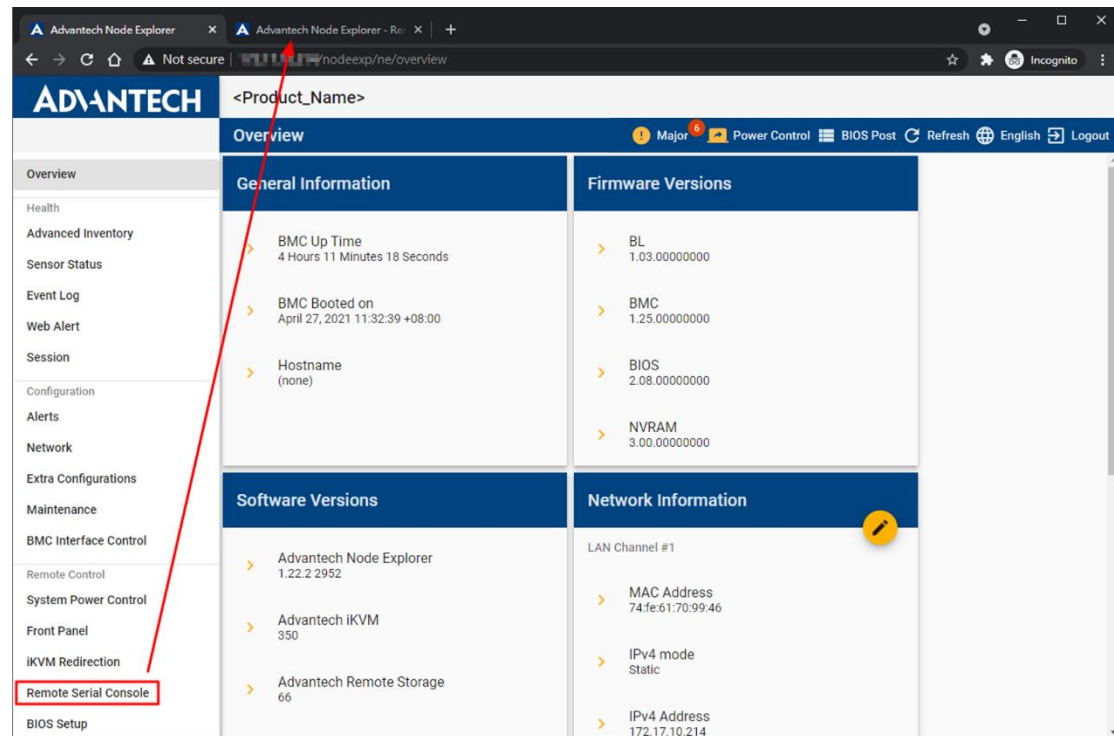


Figure 108: Open Serial Console in Remote Serial Console Page

Then the session page will be pop out in new tab in the browser directly.

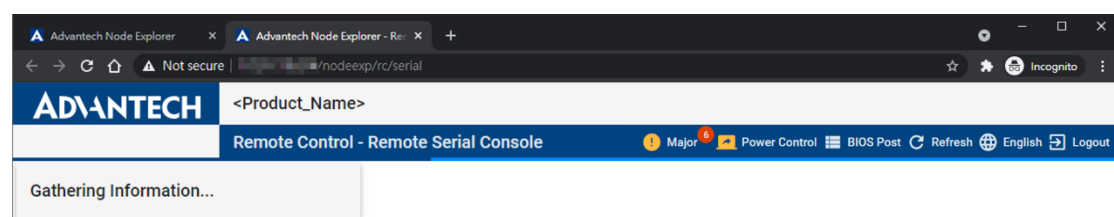


Figure 109: Redirecting

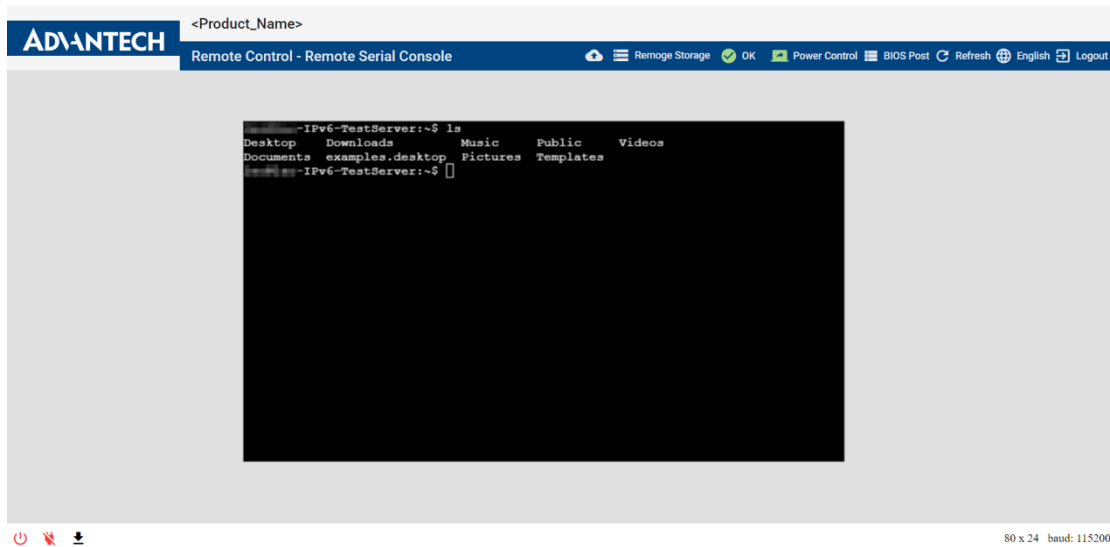
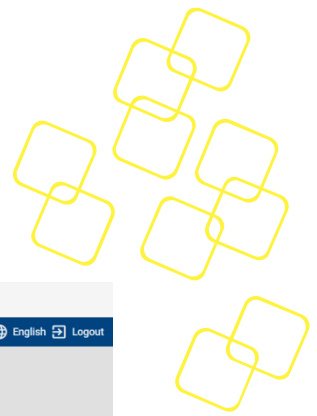


Figure 110: Remote Serial Console Page

When you open the serial console, the physical serial console connection will be disconnected. To return control access, press the button, **Disable UART Redirection** to stop the remote serial console session.

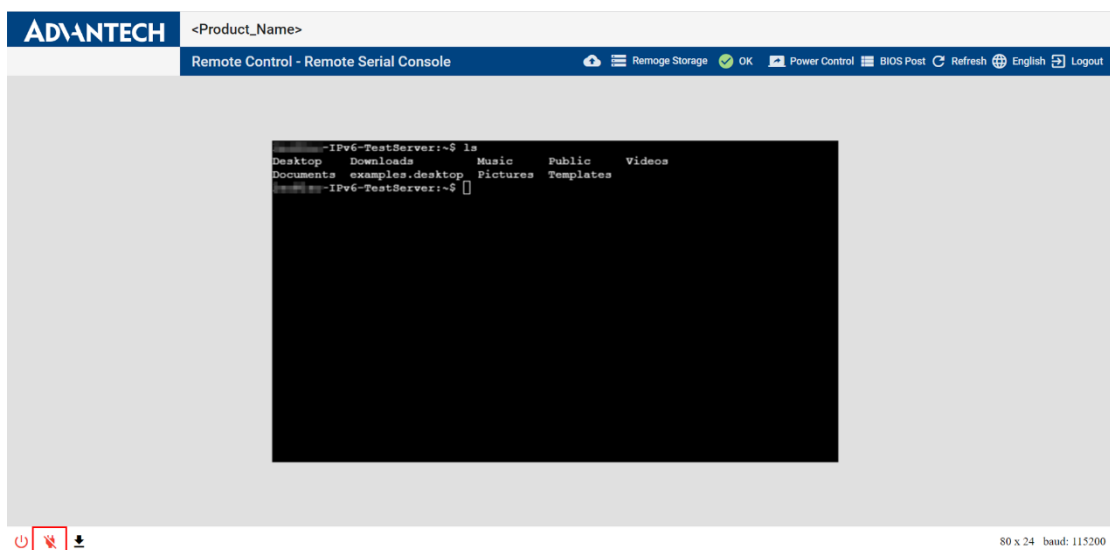


Figure 111: Disable UART Redirection



When another serial console session exists, the serial console page will show a dialog as Figure 112 for the user to decide whether to close the session or not.

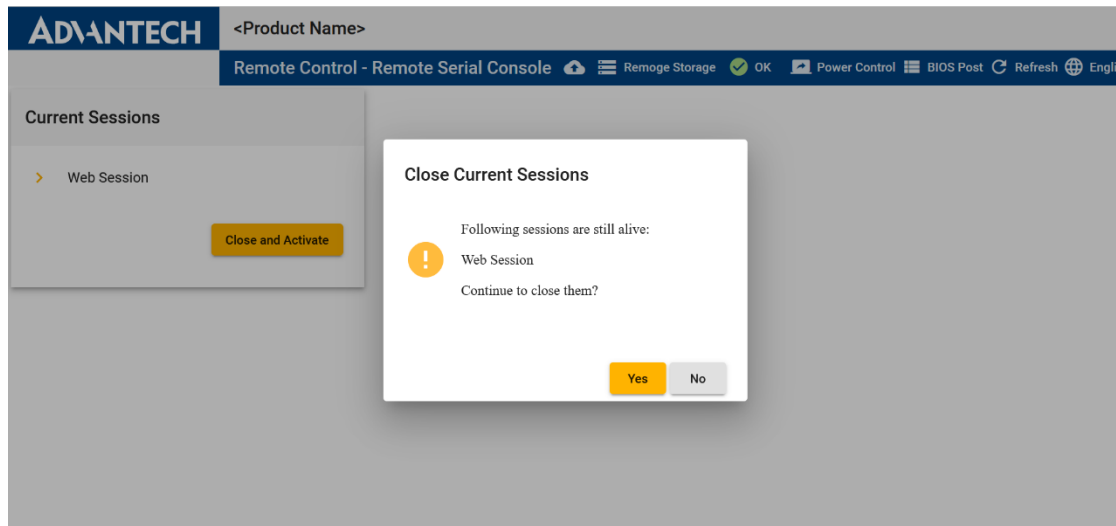
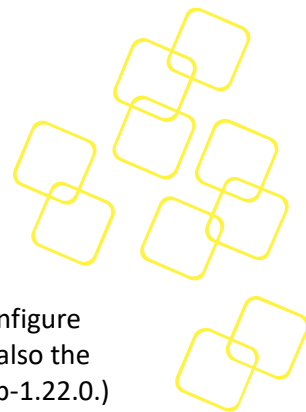


Figure 112: Close Current Sessions



3.5.5 BIOS Setup

The BIOS Setup provides a simulation of BIOS setup menu and allows the user to configure BIOS settings via Node Explorer. This functionality is based on Redfish features and also the Redfish modules supported on the BIOS side. (This feature is available after nodeexp-1.22.0.)

To configure BIOS settings, follow the steps below:

1. Click **BIOS Setup** on the left toolbar, the BIOS setup page will be shown in a new tab of the browser (see Figure 113).

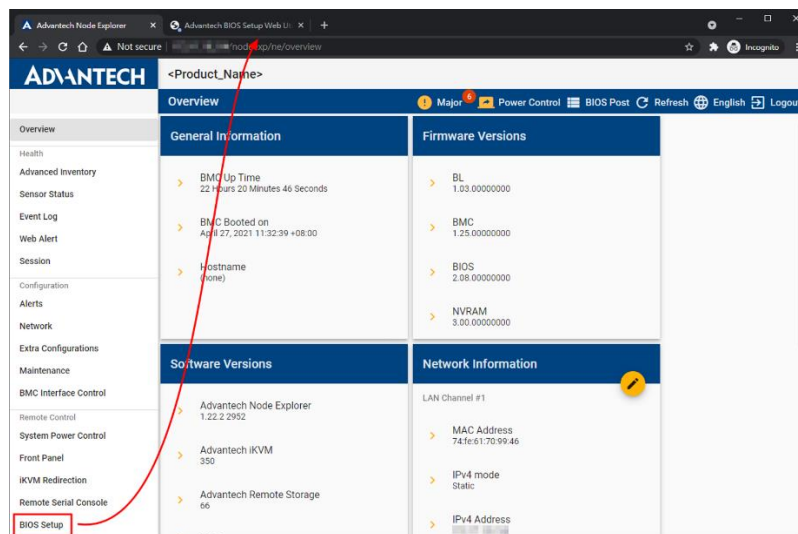


Figure 113: Open BIOS Setup Page

2. BIOS Setup page will ask the user to enter the username and password. The user credential will be used to access Redfish service for BIOS configurations.

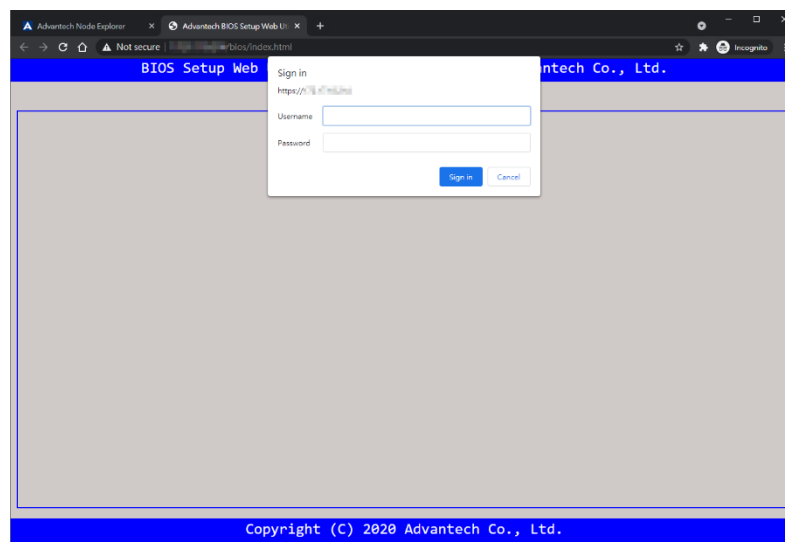


Figure 114: Asked for Username and Password in BIOS Setup Page



3. The BIOS Setup Web Utility page is almost the same as the original BIOS setup menu, but can only be controlled via mouse. The support of properties of BIOS configurations is dependent on the BIOS resource node of the Redfish service.

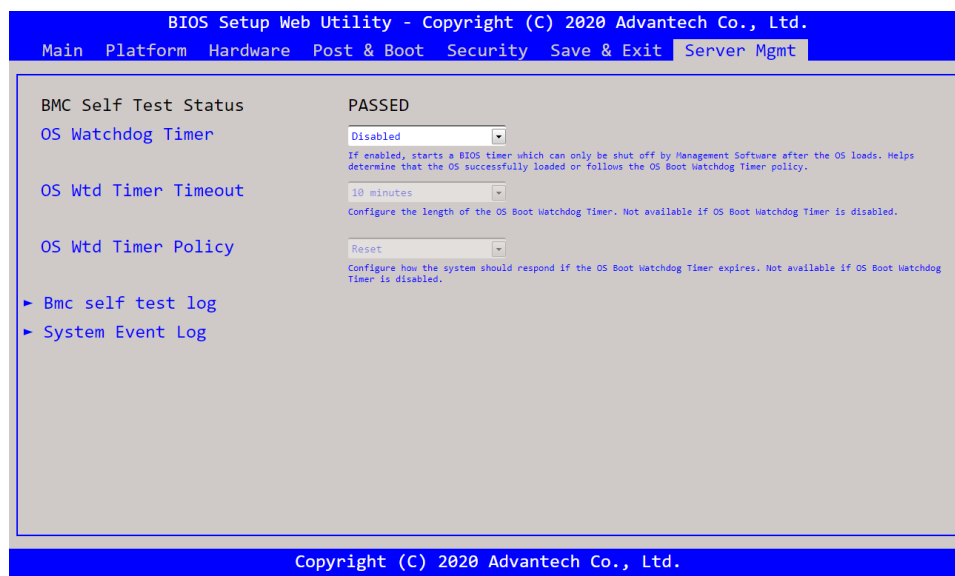
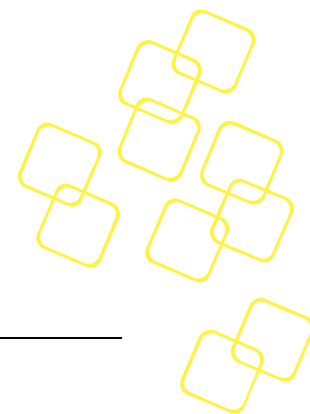


Figure 115: BIOS Setup Page (BIOS Setup Web Utility)

4. All the changes for BIOS configuration will take effect after the x86 system reset.



4. TIPS AND TROUBLESHOOTING

4.1 Web Page Timeout

The default web page (session) timeout setting is 1 week. The timer will be reset under the following conditions:

- Switching between the pages
- Clicking on any button on any page

4.2 Session Limitations

A login session is identified using cookies and addresses. Thus, if you open multiple tabs in the same browser and log them all into Node Explorer using the same account, all of them will be seen as the same session. Multiple concurrent sessions per user via different browsers or different IP addresses are also allowed.

However, a single iKVM session is only allowed by a single user. The new redirection will disconnect the previous redirection.

4.3 Security Warning Message

When you invoke Node Explorer or iKVM Redirection, the web browser may show a warning message (Figure 116: Security Warning MessageError! Reference source not found.) due to a self-signed certificate being integrated into Node Explorer by default. You can simply ignore the warning then trust the connection:

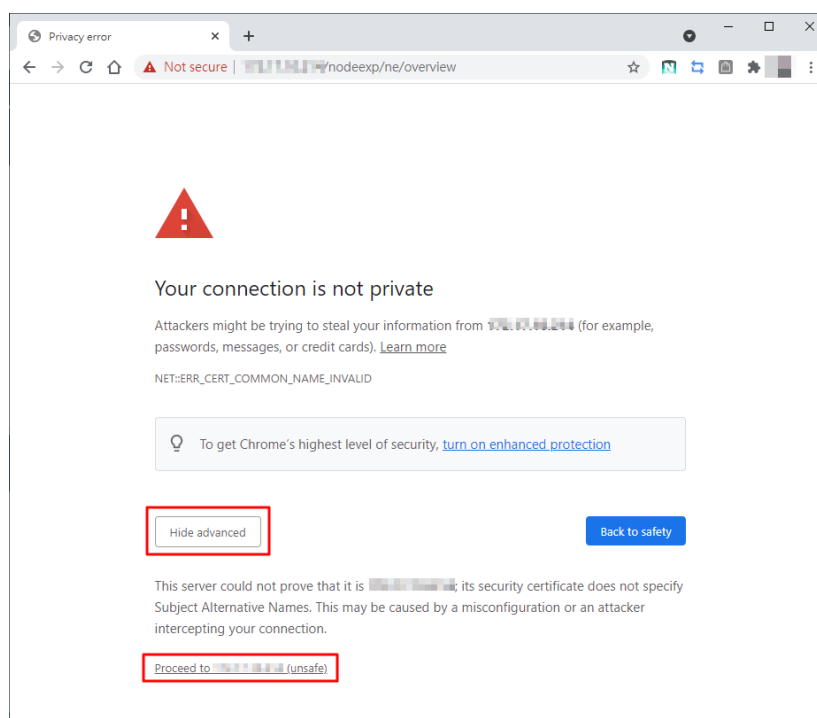
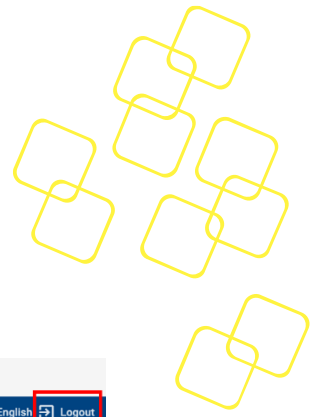


Figure 116: Security Warning Message



4.4 Log Out

Click **Logout**  on the top-right corner to log out from Node Explorer:

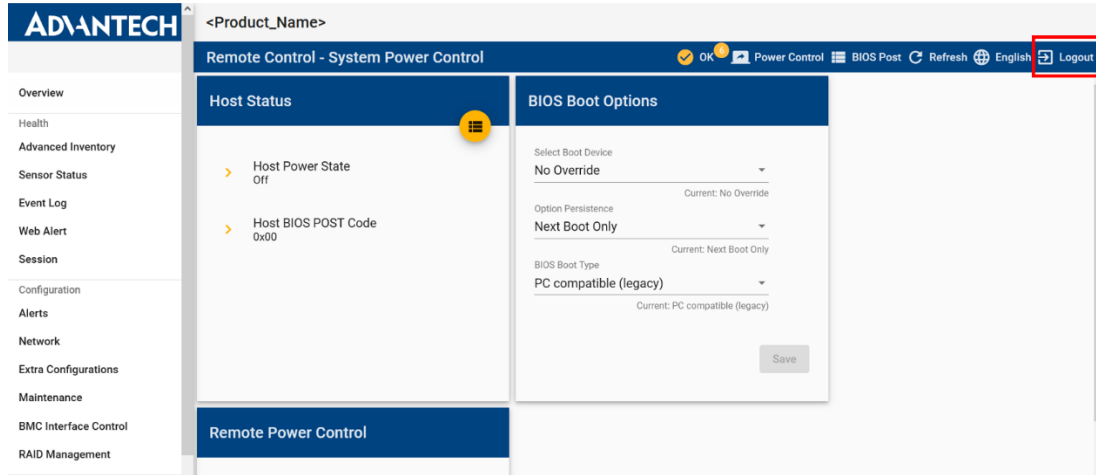


Figure 117: Log Out