

User Manual

ATS-03-S **WEBUI**



Designed and manufactured by Austin Hughes



REACH

Legal Information

First English printing, May 2023

Information in this document has been carefully checked for accuracy; however, no guarantee is given to the correctness of the contents. The information in this document is subject to change without notice. We are not liable for any injury or loss that results from the use of this equipment.

Safety Instructions

Please read all of these instructions carefully before you use the device. Save this manual for future reference.

- Unplug equipment before cleaning. Don't use liquid or spray detergent; use a moist cloth.
- Keep equipment away from excessive humidity and heat. Preferably, keep it in an air-conditioned environment with temperatures not exceeding 40° Celsius (104° Fahrenheit).
- When installing, place the equipment on a sturdy, level surface to prevent it from accidentally falling and causing damage to other equipment or injury to persons nearby.
- When the equipment is in an open position, do not cover, block or in any way obstruct the gap between it and the power supply. Proper air convection is necessary to keep it from overheating.
- Arrange the equipment's power cord in such a way that others won't trip or fall over it.
- If you are using a power cord that didn't ship with the equipment, ensure that it is rated for the voltage and current labelled on the equipment's electrical ratings label. The voltage rating on the cord should be higher than the one listed on the equipment's ratings label.
- Observe all precautions and warnings attached to the equipment.
- If you don't intend on using the equipment for a long time, disconnect it from the power outlet to prevent being damaged by transient over-voltage.
- Keep all liquids away from the equipment to minimize the risk of accidental spillage. Liquid spilled on to the power supply or on other hardware may cause damage, fire or electrical shock.
- Only qualified service personnel should open the chassis. Opening it yourself could damage the equipment and invalidate its warranty.
- If any part of the equipment becomes damaged or stops functioning, have it checked by qualified service personnel.

What the warranty does not cover

- Any product, on which the serial number has been defaced, modified or removed.
- Damage, deterioration or malfunction resulting from:
 - ☐ Accident, misuse, neglect, fire, water, lightning, or other acts of nature, unauthorized product modification, or failure to follow instructions supplied with the product.
 - ☐ Repair or attempted repair by anyone not authorized by us.
 - ☐ Any damage of the product due to shipment.
 - ☐ Removal or installation of the product.
 - ☐ Causes external to the product, such as electric power fluctuation or failure.
 - ☐ Use of supplies or parts not meeting our specifications.
 - ☐ Normal wear and tear.
 - ☐ Any other causes which does not relate to a product defect.
- Removal, installation, and set-up service charges.

Regulatory Notices Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

Any changes or modifications made to this equipment may void the user's authority to operate this equipment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

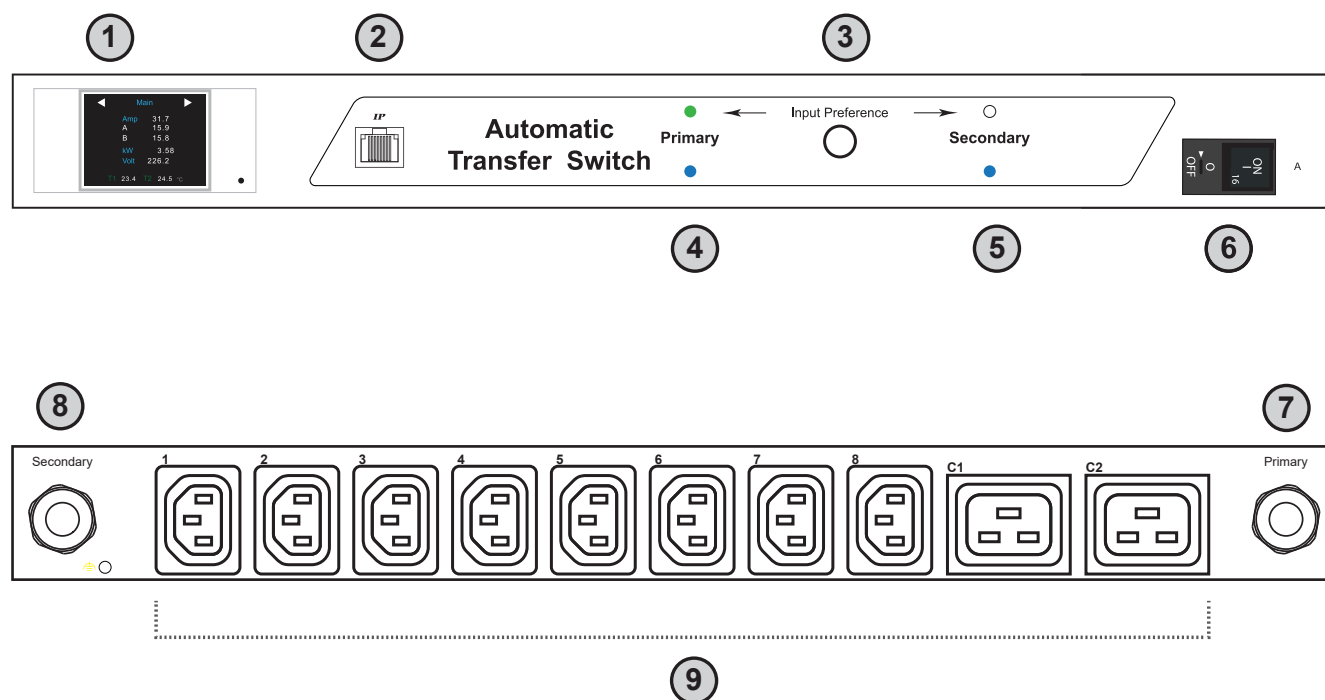
However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Re-position or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Contents

< 1.1 >	ATS Key Features	P.1
< 1.2 >	How to switch power input	P.2
< 1.3 >	Meter Reading & Setting	P.3
< 1.4 >	Hardware Specification	P.5
< 1.5 >	ATS GUI ATS-03-S Key Features	P.8
< 1.6 >	IP Configuration	P.9
< 1.7 >	ATS-03-S GUI	P.10
< 1.8 >	System	P.13
< 1.9 >	Network	P.14
< 1.10 >	DHCP Setting	P.15
< 1.11 >	Login	P.17
< 1.12 >	SNMP Setup	P.21
< 1.13 >	Notification	P.25
< 1.14 >	Syslog	P.26
< 1.15 >	ATS Firmware Upgrade	P.27
< 1.16 >	Bulk Firmware Upgrade	P.29
< 1.17 >	802.1X authentication	P.41
< 1.18 >	Command Line Interface (CLI) Access	P.44

< 1.1 > ATS Key Features



- ➊ 2.0" color LCD (feature w/ Touchscreen)
- ➋ IP Port
- ➌ Input Preference Switch
- ➍ Power LED - primary input
- ➎ Power LED - secondary input
- ➏ Circuit Breaker
- ➐ Primary Input attached with 3M cord & inlet plug
- ➑ Secondard Input attached with 3M cord & inlet plug
- ➒ Outlets

< 1.2 > How to switch power input

1. By Manual

- Press the local input switch button on the front panel
- Set the input preference via WEBUI / SNMP remotely

2. By Auto

- Switch automatically when the preferred input source is powered off



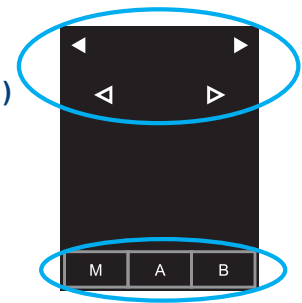
Once ATS current loading is over the rated input current, input switching is not allowed either by local or remote. However, automatic switching is NOT affected.

< 1.3 > Meter Reading & Setting

Reading

- Amp, Voltage & Power Factor
- kWh Energy Consumption
- Active & Apparent Power
- Temp. & Humidity

Touch Button
(Single & Dual Circuit)



Single Circuit

1 - 3

◀ Main ▶

Amp 15.9

kW 1.80

Volt 226.2

T1 23.4 T2 24.5 °C

M

4 - 7

◀ Power ▶

Factor 0.50

Active 1.80 kW

Apparent 3.60 kVA

299,678.56 kWh

1 Jan 15 / 23 : 59 : 40

M

◀ PDU ID ▶

Group : 050

Level : 16

M

◀ TH ▶

T1 23.4 °C

T2 24.5 °C

H1 63.4 %

H2 56.5 %

M

◀ Circuit A ▶

15.9 Amp

Peak Load Amp 16.2

1 Jan 15 / 23 : 59 : 40

M

◀ System ▶

Time 23 : 59 : 40

Date 15 Jan 15

F/W WSi-1B-V7

Serial no. 20315150589-1120-P001

Model no. V24C13/12C19 -16A-WSI/CR_EN/3B-1

M

◀ Outlet ▶

◀ 01 ▶

Amp 10.9

kW 1.23

Page no.5
Touch °C / °F to change temp. unit
* ATS does not support any sensor

Page no.7
Wi / WSi outlet measurement PDU only

Dual Circuit

1 - 4

◀ Main ▶

Amp 31.7

A 15.9

B 15.8

kW 3.58

Volt 226.2

T1 23.4 T2 24.5 °C

M A B

5 - 8

◀ Power ▶

Factor 0.50

Active 03.58 kW

Apparent 07.16 kVA

299,678.56 kWh

1 Jan 15 / 23 : 59 : 40

M A B

◀ PDU ID ▶

Group : 050

Level : 16

M A B

◀ TH ▶

T1 23.4 °C

T2 24.5 °C

H1 63.4 %

H2 56.5 %

M A B

◀ Circuit A ▶

15.9 Amp

Peak Load Amp 16.2

1 Jan 15 / 23 : 59 : 40

M A B

◀ System ▶

Time 23 : 59 : 40

Date 15 Jan 15

F/W WSi-2B-V7

Serial no. 20315150589-1120-P001

Model no. V24C13/12C19 -32A-WSI/CR_EN/3B-1

M A B

◀ Circuit B ▶

15.8 Amp

Peak Load Amp 16.2

1 Jan 15 / 23 : 59 : 40

M A B

◀ Outlet ▶

Cir. A

◀ 01 ▶

Amp 10.9

kW 1.23

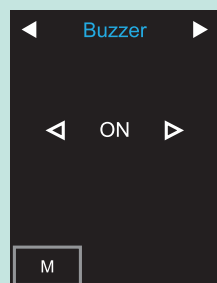
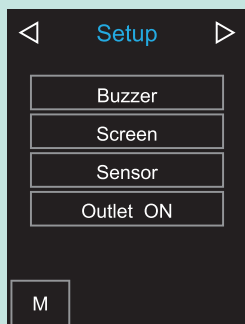
A B

Page no.6
Touch °C / °F to change temp. unit
* ATS does not support any sensor

Page no.8
Wi / WSi outlet measurement PDU only

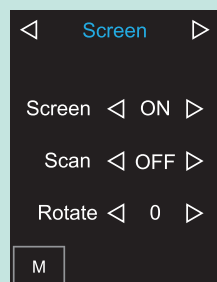
< 1.3 > Meter Reading & Setting

Setting



Buzzer ON / OFF

Default : ON



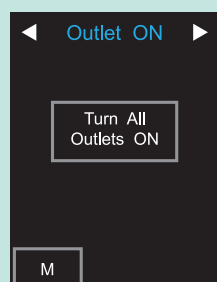
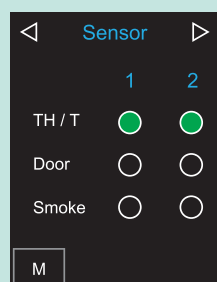
Default : Screen < ON > Scan < OFF >

* OFF Screen :

- Screen OFF in 30 seconds
- If want to turn on the screen just touch it
- OFF in 30 seconds if no any further touch

* ON Scan :

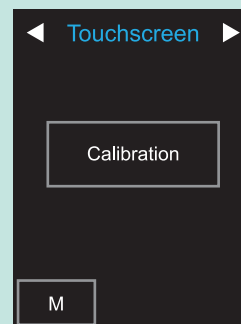
- Scanning starts in 30 seconds
- Then scan each page per 3 seconds



Outlet ON / OFF

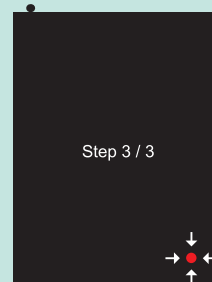
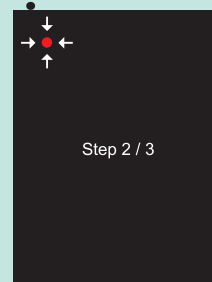
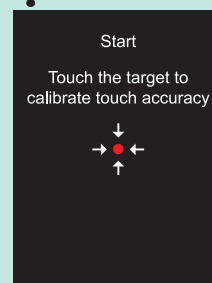
Default : ON

WS / WSi Switched PDU only



Touchscreen Calibration

If no any calibrate touch in 30 seconds, it will return to Touchscreen page



< 1.4 > Hardware Specification

230V

Electrical	Nominal input voltage	200 ~ 230V
	Acceptable input voltage	±10% nominal
	Input frequency	50 / 60Hz
	Inlet plug & cord	2 x C14 / C20 / EN 60309 / BS1363 / CEE7 plug w/ 3M cord
	Outlet connectors	C13 / C13+C19 / C19 / IEC309 / UK / Schuko / FR
	Local meter	2.0" color LCD (feature w/ Touchscreen)
	Overload protection	1 x 10-amp circuit breaker for C14 inlet 1 x 13-amp circuit breaker for BS1363 inlet 1 x 16-amp circuit breaker for C20 / EN16 60309 / CEE7 inlet 1 x 20-amp circuit breaker for Open-end 2 x 16-amp circuit breaker for EN32 60309 inlet
	Transfer time	10 - 16ms typical
	Electrical endurance	1 x 10 ⁵ operations
	Power consumption	Approx. 8VA
Physical	Product dimensions (1U)	442 x 270 x 43.5 mm (W x D x H)
	Packing dimensions (1U)	540 x 540 x 150 mm (W x D x H)
	Net weight	4.7 kg / 10.3 lb
	Gross weight	5.2 kg / 11.4 lb
	Product dimensions (2U)	442 x 270 x 87.5 mm (W x D x H)
	Packing dimensions (2U)	540 x 540 x 150 mm (W x D x H)
	Net weight	6.6 kg / 14.5 lb
	Gross weight	7.1 kg / 15.6 lb
	Chassis color / materials	Dark / Steel
Environmental	Operating temperature	-5 to 60°C degree (23 to 140°F)
	Storage temperature	-25 to 65°C degree (13 to 149°F)
	Operating humidity	0~95%, non-condensing
	Storage humidity	0~95%, non-condensing
Compliance	EMC	FCC & CE
	Safety	CUL, LVD
	Environment	RoHS3 & REACH compliant

< 1.4 > Hardware Specification

208V

Electrical	Nominal input voltage	208V
	Acceptable input voltage	±10% nominal
	Input frequency	50 / 60Hz
	Inlet plug & cord	2 x L620 / L630 plug w/ 3M cord
	Outlet connectors	C13 / C13+C19 / C19 / IEC309
	Local meter	2.0" color LCD (feature w/ Touchscreen)
	Overload protection	1 x 20-amp circuit breaker for L6-20P inlet 1 x 30-amp circuit breaker for L6-30P inlet
	Transfer time	10 - 16ms typical
	Electrical endurance	1 x 10 ⁵ operations
	Power consumption	Approx. 8VA
Physical	Product dimensions (1U)	4.7 kg / 10.3 lb
	Packing dimensions (1U)	5.2 kg / 11.4 lb
	Net weight	442 x 270 x 87.5 mm (W x D x H)
	Gross weight	540 x 540 x 150 mm (W x D x H)
	Product dimensions (2U)	6.6 kg / 14.5 lb
	Packing dimensions (2U)	7.1 kg / 15.6 lb
	Net weight	5.5 kg / 12.1 lb
	Gross weight	6.8 kg / 15 lb
	Chassis color / materials	Dark / Steel
Environmental	Operating temperature	-5 to 60°C degree (23 to 140°F)
	Storage temperature	-25 to 65°C degree (13 to 149°F)
	Operating humidity	0~95%, non-condensing
	Storage humidity	0~95%, non-condensing
Compliance	EMC	FCC & CE
	Safety	CUL, LVD
	Environment	RoHS3 & REACH compliant

< 1.4 > Hardware Specification

110V

Electrical	Nominal input voltage	110V
	Acceptable input voltage	±10% nominal
	Input frequency	50 / 60Hz
	Inlet plug & cord	2 x 515 / L520 / L530 plug w/ 3M cord
	Outlet connectors	NEMA 5-20R
	Local meter	2.0" color LCD (feature w/ Touchscreen)
	Overload protection	1 x 15-amp circuit breaker for NEMA 5-15P inlet 1 x 20-amp circuit breaker for NEMA L5-20P inlet 1 x 30-amp circuit breaker for NEMA L5-30P inlet
	Transfer time	10 - 16ms typical
	Electrical endurance	1 x 10 ⁵ operations
	Power consumption	Approx. 8VA
Physical	Product dimensions (1U)	442 x 270 x 43.5 mm (W x D x H)
	Packing dimensions (1U)	540 x 540 x 150 mm (W x D x H)
	Net weight	4.7 kg / 10.3 lb
	Gross weight	5.2 kg / 11.4 lb
	Product dimensions (2U)	442 x 270 x 87.5 mm (W x D x H)
	Packing dimensions (2U)	540 x 540 x 150 mm (W x D x H)
	Net weight	6.6 kg / 14.5 lb
	Gross weight	7.1 kg / 15.6 lb
	Chassis color / materials	Dark / Steel
Environmental	Operating temperature	-5 to 60°C degree (23 to 140°F)
	Storage temperature	-25 to 65°C degree (13 to 149°F)
	Operating humidity	0~95%, non-condensing
	Storage humidity	0~95%, non-condensing
Compliance	EMC	FCC & CE
	Safety	CUL, LVD
	Environment	RoHS3 & REACH compliant

< 1.5 > ATS GUI ATS-03-S Key Features

InfraPower Manager ATS-03-S is a FREE built-in GUI of each intelligent ATS which allows remotely monitoring over IP.

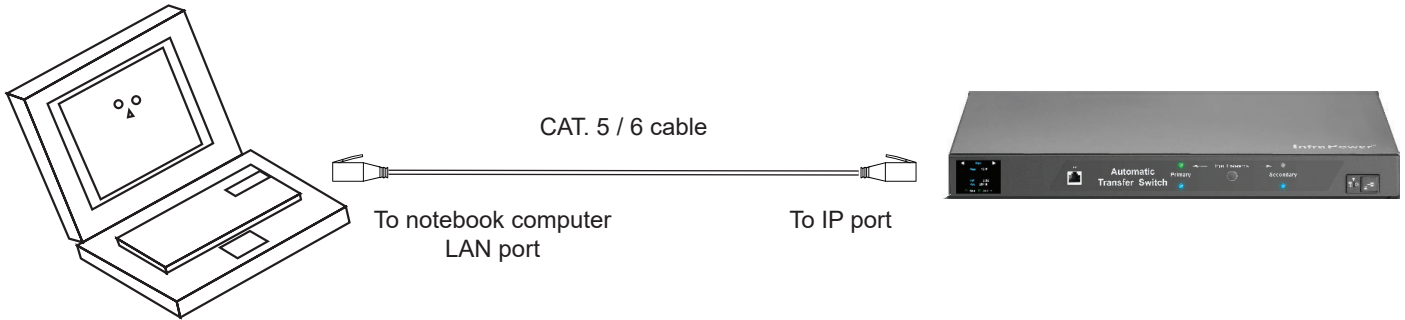
InfraPower ATS-03-S


Features		
Capacity	IP Dongle Group	1
	ATS Number	1
	Concurrent User	1
Features	Input Source Selection	✓
	Input Source Status Monitoring	✓
	Individual Outlet Switch ON/OFF	✓
	Outlet Level kWh & Amp Measurement	✓
	Energy Consumption (kWh) Monitoring	✓
	Apparent Power (kVA) Monitoring	✓
	Active Power (kW) Monitoring	✓
	Power Factor Measurement	✓
	Voltage (Volt) Monitoring	✓
	Circuit Amp. Monitoring	✓
	Circuit Breaker Monitoring	✓
	Amp. Alarm / R. Alert / L. Alert Setting	✓

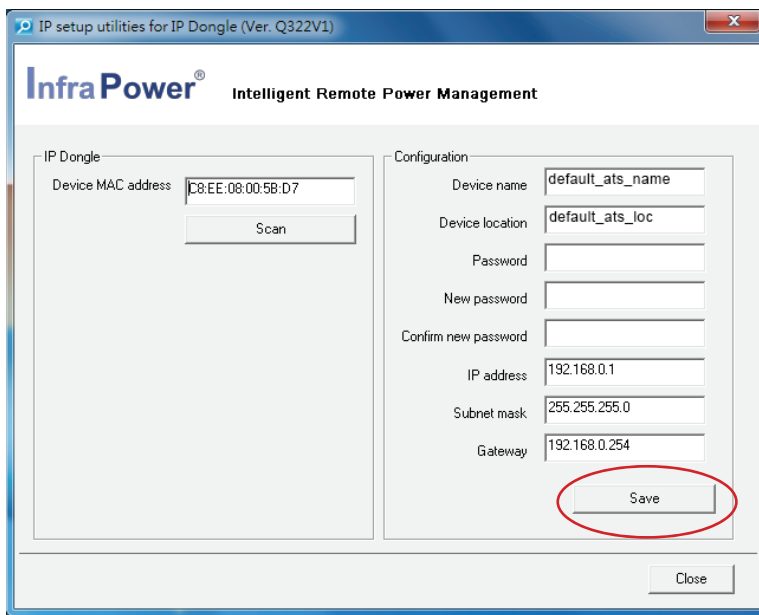
< 1.6 > IP Configuration

 The following steps show the static IP setting only. For DHCP setting, please refer to < 1.10 > DHCP Setting

- Step 1.** Prepare a notebook computer to download the IP setup utilities from the link : <http://www.austin-hughes.com/support/utilities/infrapower/IPdongleSetup.msi>
- Step 2.** Double Click the IPDongleSetup.msi and follow the instruction to complete the installation
- Step 3.** Connect the ATS with the notebook computer using a piece of Cat. 5 / 6 cable to configure the IP setting by IP setup utilities as below. Please take the procedure for all ATS **ONE BY ONE**



 Reconnect the ATS with the network device (router or hub), after finish IP configuration.



The screenshot shows the 'IP setup utilities for IP Dongle (Ver. Q322V1)' window. The window has a title bar and a menu bar. The main area is divided into two sections: 'IP Dongle' and 'Configuration'. The 'IP Dongle' section contains a 'Device MAC address' field with the value 'C8:EE:08:00:5B:D7' and a 'Scan' button. The 'Configuration' section contains several fields: 'Device name' (default: 'default_ats_name'), 'Device location' (default: 'default_ats_loc'), 'Password' (empty), 'New password' (empty), 'Confirm new password' (empty), 'IP address' (default: '192.168.0.1'), 'Subnet mask' (default: '255.255.255.0'), and 'Gateway' (default: '192.168.0.254'). A 'Save' button is located at the bottom right of the 'Configuration' section and is highlighted with a red circle. A 'Close' button is at the bottom right of the window.




1. If the ATS (IPD-03-S built-in) is in factory default setting or the password is " 00000000 ", you **MUST** change the password for security purpose.
2. The password **MUST** contain at least three of the following four character groups :
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Numerals (0 through 9)
 - Non-alphabetic characters (` , \$, " , \ are NOT supported)
3. Device name **NOT EQUAL** to the Login name of ATS WEBUI (ATS-03-S). To change Login name, please refer to 1.11 < Login > for details.

- Step 4.** Click " **Scan** " to search the connected ATS
- Step 5.** Enter device name in " **Device name** " (min. 4 char. / max. 16 char.). Default is " **default_ats_name** "
- Step 6.** Enter device location in " **Device location** " (min. 4 char. / max. 16 char.). Default is " **default_ats_loc** "
- Step 7.** Enter password in " **Password** " for authentication (min. 8 char. / max. 16 char.). Default is " **00000000** "
- Step 8.** Enter new password in " **New password** " (min. 8 char. / max. 16 char.)
- Step 9.** Re-enter new password in " **Confirm new password** "
- Step 10.** Change the desired " **IP address** " / " **Subnet mask** " / " **Gateway** ", then Click " **Save** " to confirm the changes
The default IP setting is as below:
IP address : 192.168.0.1
Subnet mask : 255.255.255.0
Gateway : 192.168.0.254

< 1.7 > ATS-03-S GUI

Each ATS provides a FREE built-in GUI, ATS-03-S, which allows user, via a web browser, to monitor the ATS status over a TCP / IP Ethernet network remotely.

 Each web browser window supports only one ATS. If you install more ATS, multi windows will be required.


Please follow the steps below to login the ATS GUI (ATS-03-S).

Step 1. Open Internet Explorer (I.E.), version 11.0

Step 2. Enter the configured ATS's IP address into the address bar
(Please refer to < 1.6 > IP configuration)


Device	ATS-03-S
Login name	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/> <input type="button" value="Cancel"/>	

Device	ATS-03-S
You are required to change the default password.	
Login name	<input type="text"/>
Default Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

 If the Intelligent ATS is in factory default setting or the password is “00000000”, this window will be shown and you **MUST** change the “**Password**” before you can login the Intelligent ATS WEBUI

Step 3. Enter “**Login name**”, “**Password**” & Click “**Login**”

Device	ATS-03-S
Login name	<input type="text" value="00000000"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Login"/> <input type="button" value="Cancel"/>	

 Default Login name : 00000000
Password : the one you set in Step 7 of < 1.6 > IP Configuration.
The login account will be LOCKED for 5 mins if three unsuccessful login attempts to the ATS GUI

< 1.7 > ATS-03-S GUI

In < **Status** > ,

- View the installed ATS status
- View aggregate current & energy consumption of the ATS
- Select the preferred “ **Input Switch** ”
- Change “ **Name** ” & “ **Location** ” of ATS & Click “ **Apply** ”
- Change “ **Alarm amp** ” , “ **Rising alert amp.** ” & “ **Low alert amp.** ” of the ATS circuit & Click “ **Apply** ”
Default alarm amp. = 80% of circuit's max. amp.
Default rising alert amp. & low alert amp. = 0.0 (disabled)
- Click “ **Reset** ” to reset peak amp. or kWh of ATS's circuit
- Click “ **Time Sync** ” to update ATS's real time clock from the computer logged in the ATS.
- View latest loading & energy consumption of each outlet (Outlet Measurement PDU only)
- View latest voltage of each circuit
- Click " ON / OFF " to switch ON / OFF outlet (Outlet Switched PDU only)

Status

Model : ATS-H16C13-32A-WSi Name : Default_ATS_name
Status : Connected Location : Default_ATS_loc.

Input Switch :

Primary Online

Secondary Online

kWh : 0.00 Power factor : 0.00
Load amp : 0.0 kVA : 0.00

A

Voltage :	215.7	Alarm amp :	<input type="text" value="12.8"/>
Max. amp :	16.0	Rising alert amp :	<input type="text" value="0.0"/>
Load amp :	0.0	Low alert amp :	<input type="text" value="0.0"/>
Peak amp :	0.0	2015/01/01 00:00:00	<input type="button" value="Reset"/>
kWh :	0.00	2015/01/01 00:00:00	<input type="button" value="Reset"/>

B

Voltage :	215.7	Alarm amp :	<input type="text" value="12.8"/>
Max. amp :	16.0	Rising alert amp :	<input type="text" value="0.0"/>
Load amp :	0.0	Low alert amp :	<input type="text" value="0.0"/>
Peak amp :	0.0	2015/01/01 00:00:00	<input type="button" value="Reset"/>
kWh :	0.00	2015/01/01 00:00:00	<input type="button" value="Reset"/>

Outlet	Name	Amp	kWh	kVA	Status	Switch
01	outlet_name_01	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
03	outlet_name_03	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
05	outlet_name_05	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
07	outlet_name_07	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
09	outlet_name_09	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
11	outlet_name_11	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
13	outlet_name_13	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
15	outlet_name_15	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>

Click outlet icon for setting

Outlet	Name	Amp	kWh	kVA	Status	Switch
02	outlet_name_02	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
04	outlet_name_04	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
06	outlet_name_06	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
08	outlet_name_08	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
10	outlet_name_10	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
12	outlet_name_12	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
14	outlet_name_14	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>
16	outlet_name_16	0.0	0.00	0.00	ON	<input type="button" value="OFF"/>

Click outlet icon for setting

* Press F11 to enlarge or diminish the screen

☒ Auto data refresh : ☐ Untick during data input.

Save new data input Synchronize this device time with computer
 Discard new data input



Once ATS current loading is over the rated input current, input switching is NOT allowed either by local or remote

< 1.7 > **ATS-03-S GUI**

In < **Outlet details** > ,

- Change PDU outlet name
 - Change " Power up sequence delay " (Outlet Switched PDU only)
 - Change " Alarm amp. " , " Rising alert amp. " & " Low alert amp. " (Outlet Measurement PDU only)
- Click " Apply " to finish the above settings
- Click " Reset " to reset peak amp. or kWh (Outlet Measurement PDU only)

Outlet details

Model :

ATS-H16C13-32A-WSi

Status :

Connected

Name :



Default_ATS_name

Location :

Default_ATS_loc.

A

Outlet :

01  

Name :

outlet_name_01

Status :

ON

Power up sequence delay :

1

Load amp :

0.0

Alarm amp :

5.0

R. alert amp :

0.0

L. alert amp :

0.0

Peak amp :

0.0

2015/01/01 00:00:00

Reset

kWh :

0.00

2015/01/01 00:00:00

Reset

Apply

Save new data input

Exit

Return to previous page

Cancel

Discard new data input

< 1.8 > System

In < **System** > ,

- Change the built-in IPD-03-S name & location
- Change temperature unit displayed in GUI
- Set “ **Date & Time** ” of the ATS (by “ **Manually** ” or “ **NTP server** ”). Default is “ **Manually** ”
- Click “ **Apply** ” to finish the above settings

Device

Status

Setting

System

Network

Login

Local User

Domain/LDAP

SNMP

SNMP Traps

Notification

Syslog

Firmware

System

Name : default_ats_name

Location : default_ats_loc.

Temperature unit : ☒ °C ☐ °F

Date & Time 2023-02-21 15:45:35

Time zone : GMT+08:00 ▼

Time setting : Manually ▼

Date (YYYY-MM-DD) : 2023-02-21

Time : 15 ▼ : 45 ▼ : 35 ▼

Web Access

Protocol : HTTPS ▼

Port : 443 (Default: 443)

SSL Certificate : ☒ Use default certificate ☐ Use custom certificate

Apply Cancel Reset to Factory Default Reboot System

System

Name : default_ats_name

Location : default_ats_loc.

Temperature unit : ☒ °C ☐ °F

Date & Time 2007-01-01 20:16:34

Time zone : GMT+08:00 ▼

Time setting : Synchronize with NTP server ▼

NTP server : time.google.com Sync Now

Web Access

Protocol : HTTPS ▼

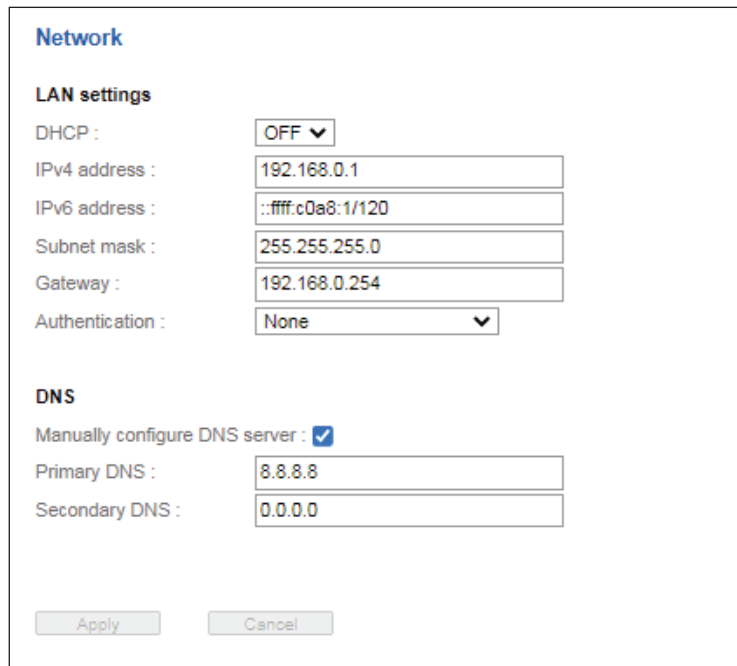
Port : 443 (Default: 443)

SSL Certificate : ☒ Use default certificate ☐ Use custom certificate

Apply Cancel Reset to Factory Default Reboot System

< 1.9 > Network

- Change the “ **IPv4 address** ”, “ **IPv6 address** ”, “ **Subnet mask** ” & “ **Gateway** ”
(For static IP setting only)
- Select “ **ON** ” in “ **DHCP** ” to enable DHCP setting. Default is OFF
(For DHCP setting, please refer to < 1.10 > DHCP Setting.)
- Enter the IP address of “ **Primary DNS** ”. Default is 8.8.8.8
- Enter the IP address of “ **Secondary DNS** ”. Default is 0.0.0.0
- Click “ **Apply** ” to finish the above settings.



The image shows a 'Network' settings window. It has a title bar 'Network' in blue. Below it is a section 'LAN settings'. Under 'LAN settings', there are several fields: 'DHCP' with a dropdown menu set to 'OFF', 'IPv4 address' with the value '192.168.0.1', 'IPv6 address' with the value '::ffff:c0a8:1/120', 'Subnet mask' with the value '255.255.255.0', 'Gateway' with the value '192.168.0.254', and 'Authentication' with a dropdown menu set to 'None'. Below the 'LAN settings' section is a 'DNS' section. It contains a checkbox 'Manually configure DNS server' which is checked, and two text input fields: 'Primary DNS' with the value '8.8.8.8' and 'Secondary DNS' with the value '0.0.0.0'. At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

Network

LAN settings

DHCP : OFF ▼

IPv4 address : 192.168.0.1

IPv6 address : ::ffff:c0a8:1/120

Subnet mask : 255.255.255.0

Gateway : 192.168.0.254

Authentication : None ▼

DNS

Manually configure DNS server : ☒

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Apply Cancel

< 1.10 > DHCP Setting

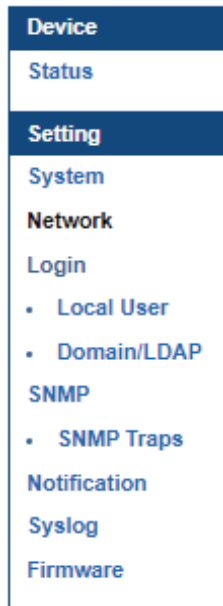
Step 1. Connect the Intelligent ATS to the computer (Please refer to < 1.6 > IP Configuration)

Step 2. Open Internet Explorer (I.E.), version 11.0

Step 3. Enter the configured ATS's IP address into the address bar
(Please refer to < 1.6 > IP configuration)

Step 4. Enter the “ **Login name** ” & “ **Password** ”.
Default login name : 00000000
Password : the one you set in Step 7 of < 1.6 > IP Configuration

Step 5. Select “ **Network** ” from the left navigation pane

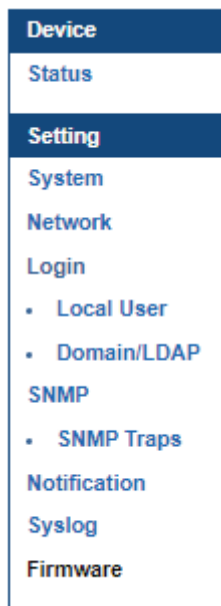


Step 6. Select “ ON ” from “ **DHCP** ” & Click “ **Apply** ” to save the settings.

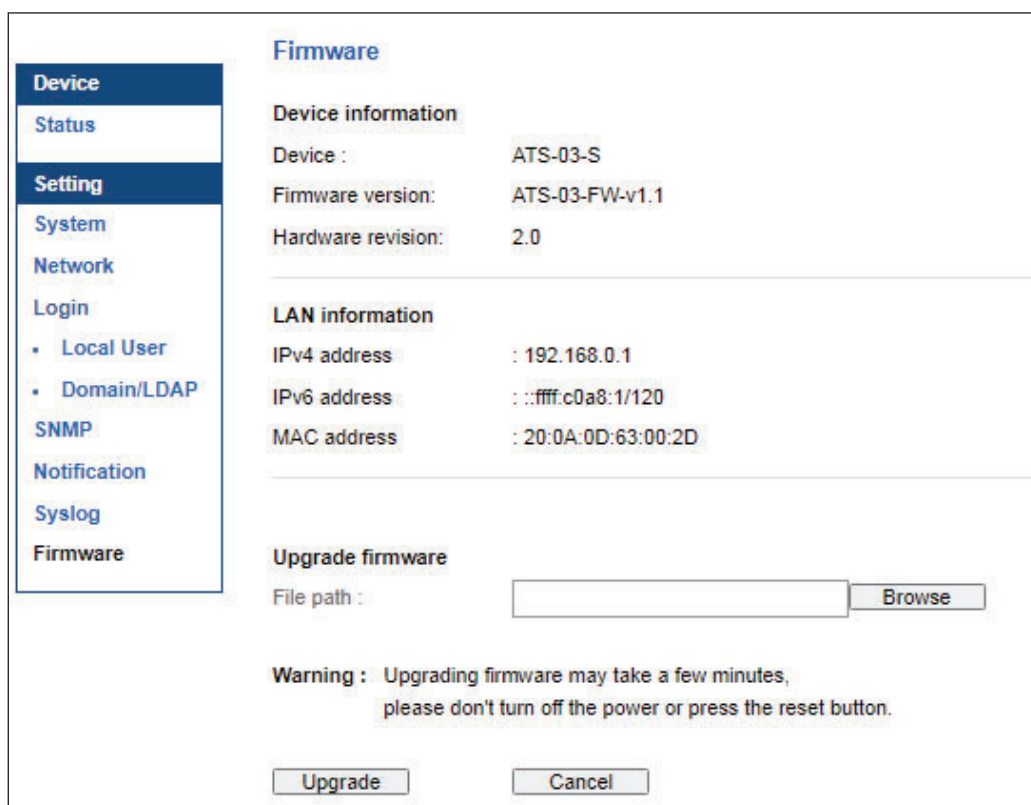
The image shows the 'Network' configuration page. At the top is the title 'Network'. Under 'LAN settings', there is a 'DHCP' dropdown menu set to 'ON'. Below this are fields for 'IPv4 address' (192.168.0.1), 'IPv6 address' (::ffff:c0a8:1/120), 'Subnet mask' (255.255.255.0), 'Gateway' (192.168.0.254), and 'Authentication' (set to 'None'). Under the 'DNS' section, there is a checkbox for 'Manually configure DNS server' which is checked. Below this are input fields for 'Primary DNS' (8.8.8.8) and 'Secondary DNS' (0.0.0.0). At the bottom of the form are 'Apply' and 'Cancel' buttons.

< 1.10 > DHCP Setting

Step 7. Select “ **Firmware** ” from the left navigation pane



Step 8. Record the “ **Device MAC address** ”



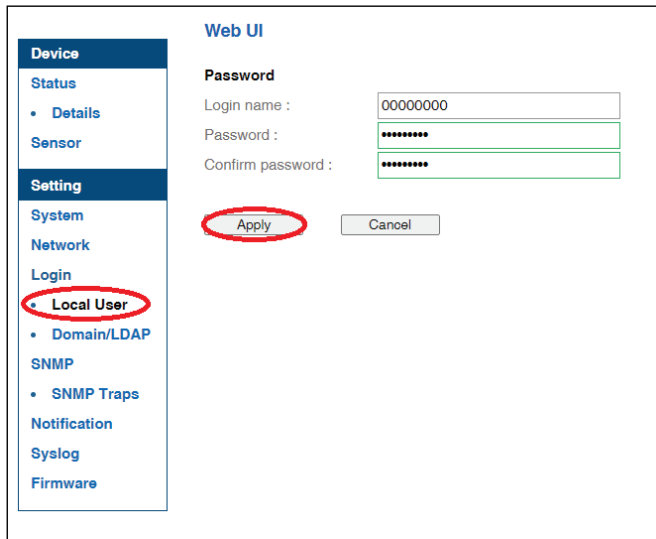
Step 9. Assign an IP address to the Intelligent ATS from your DHCP server.

< 1.11 > Login

In < **Login** >, you can login the ATS WEBUI by “ **Local User** ” or “ **Domain/LDAP** ” login.
(Default login : “ **Local User** ”)

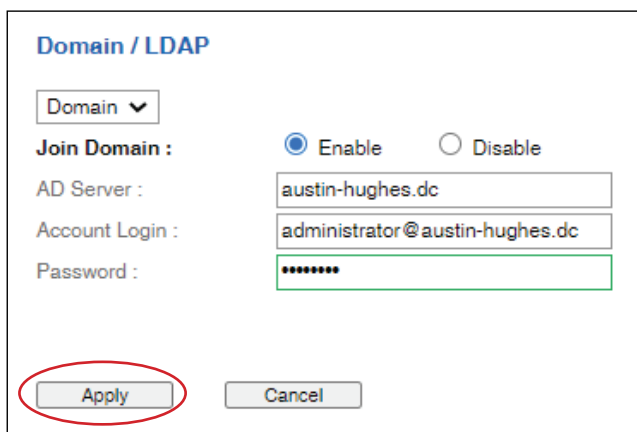
Local User :

- Change “ **Login name** ” OR “ **Password** ”
- Re-enter password in “ **Confirm password** ”
- Click “ **Apply** ” and “ **OK** ” on the pop up window to make changes effective



Domain/LDAP :

- Default Join Domain is “ **Disable** ”
- Enable “ **Join Domain** ” only when you want to login the ATS WEBUI by AD server
- Enter “ **AD Server** ”, “ **Account Login** ” & “ **Password** ”
- Click “ **Apply** ” and “ **OK** ” on the pop up window to make changes effective
- You can now go to “ **Domain Users** ” to assign access right to the “ **Domain Users** ” or the “ **Domain Group** ”



< 1.11 > Login

In “ **Domain Users Setting** ”,

- Click “ **Update domain data** ” to update domain user list.
- Assign access right (No access / Allow / Deny) to “ **Domain Users** ” and click “ **Apply** ” .
- The Domain User assigned “ **Allow** ” access right can login the ATS WEBUI.

Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password :

Update user list

Domain User ▼

No.	Domain User	No access	Allow	Deny
1.	Administrator	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2.	DefaultAccount	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.	Guest	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
4.	databaseadmin	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Apply Cancel

In “ **Domain Users Setting** ”,

- Click “ **Update domain data** ” to update domain group list.
- Assign access right (No access / Allow) to “ **Domain Group** ” and click “ **Apply** ” .
- The Users of the Domain Group assigned “ **Allow** ” access right can login the ATS WEBUI.

Domain Users Setting

Account Login : administrator@austin-hughes.dc

Password :

Update user list

Domain Group ▼

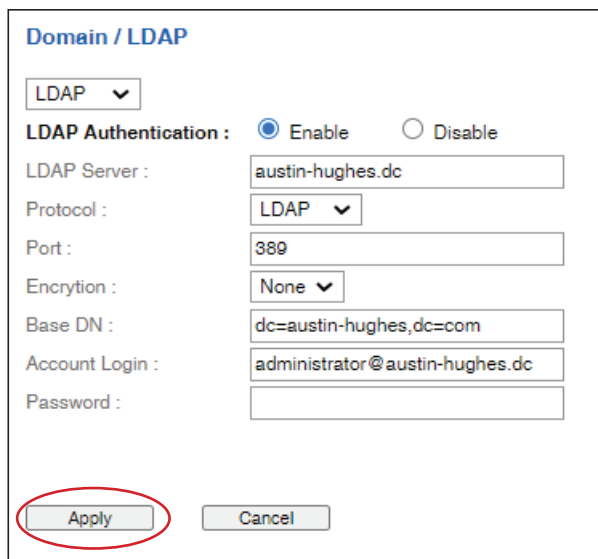
No.	Domain Group	No access	Allow
1.	Access Control Assistance Operators	<input checked="" type="radio"/>	<input type="radio"/>
2.	Account Operators	<input type="radio"/>	<input checked="" type="radio"/>
3.	Administrators	<input checked="" type="radio"/>	<input type="radio"/>
4.	Allowed RODC Password Replication Group	<input checked="" type="radio"/>	<input type="radio"/>
5.	Backup Operators	<input checked="" type="radio"/>	<input type="radio"/>

Apply Cancel

< 1.11 > Login

Domain/LDAP :

- Default LDAP Authentication is “ **Disable** ”
- Enable “ **LDAP Authentication** ” only when you want to login the ATS WEBUI by LDAP server
- Enter “ **LDAP Server** ”,
- Select “ **Protocol** ”(LDAP / LDAPS). Default is “ **LDAP** ”
- Enter “ **Port** “. Default is “ **389** ”
- Select “ **Encryption** ”(None / SSL). Default is “ **None** ”
- Enter “ **Base DN** ”.
- Enter “ **Account Login** ” & “ **Password** ”.
- Click “ **Apply** ” and “ **OK** ” on the pop up window to make changes effective
- You can now go to “ **LDAP Users** ” to assign access right to the “ **LDAP User** ” or the “ **LDAP Group** ”



Domain / LDAP

LDAP ▾

LDAP Authentication : ☒ Enable ☐ Disable

LDAP Server : austin-hughes.dc

Protocol : LDAP ▾

Port : 389

Encryption : None ▾

Base DN : dc=austin-hughes,dc=com

Account Login : administrator@austin-hughes.dc

Password :

Apply Cancel

< 1.11 > Login

In “ **LDAP Access Setting** ”,

- Click “ **Update domain data** ” to update domain user list.
- Assign access right (No access / Allow / Deny) to “ **LDAP User** ” and click “ **Apply** ” .
- The LDAP User assigned “ **Allow** ” access right can login the ATS WEBUI.

LDAP Access Setting

Account Login : administrator@austin-hughes.dc

Password :

LDAP User ▼

No.	LDAP User	No access	Allow	Deny
1.	Administrator	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
2.	DefaultAccount	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
3.	Guest	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
4.	databaseadmin	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

In “ **LDAP Access Setting** ”,

- Click “ **Update domain data** ” to update domain user list.
- Assign access right (No access / Allow / Deny) to “ **LDAP Group** ” and click “ **Apply** ” .
- The LDAP Group assigned “ **Allow** ” access right can login the ATS WEBUI.

LDAP Access Setting

Account Login : administrator@austin-hughes.dc

Password :

LDAP Group ▼

No.	LDAP Group	No access	Allow
1.	Access Control Assistance Operators	<input checked="" type="radio"/>	<input type="radio"/>
2.	Account Operators	<input type="radio"/>	<input checked="" type="radio"/>
3.	Administrators	<input checked="" type="radio"/>	<input type="radio"/>
4.	Allowed RODC Password Replication Group	<input checked="" type="radio"/>	<input type="radio"/>
5.	Backup Operators	<input checked="" type="radio"/>	<input type="radio"/>

< 1.12 > SNMP Setup

The intelligent ATS has SNMP (v1/v2 or v3) function which is capable of integration of 3rd party DCIM to achieve centralized monitoring for power, cooling and environment factors across facilities and IT systems.

(I). Accessing MIB Files

Step 1. Click the following link to go to the mangement software download page :
<http://www.austin-hughes.com/resources/software/infrapower>

Step 2. Select the MIB file of the intelligent ATS

(II). Enabling SNMP Support

i. The following steps summarize how to enable the ATS for SNMP v1 / v2 support.

Step 1. Connect the ATS to a computer. (Please refer to < 1.6 > IP configuration)

Step 2. Open the Internet Explorer (I.E.) version 11.0

Step 3. Enter the configured ATS's address into the address bar
(Please refer to < 1.6 > IP configuration)

Step 4. Enter the “ **Login name** “ , “ **Password** “

Default Login name : 00000000

Password: the one you set in Step 7 of < 1.6 > IP Configuration.

Step 5. Select the SNMP from the left navigation pane



< 1.12 > SNMP Setup

Step 6. The SNMP settings window appears as below :

The image shows a web-based configuration window titled "SNMP". It contains several sections for setting up the SNMP service and traps.

SNMP agent : ☒ Enable ☐ Disable

SNMP version :

SNMP port :

sysContact :

sysLocation :

sysName :

SNMP configuration

Read community :

Write community :

Station 1 : ☐ Deactivate ☒ Activate

Trap Station IP :

Trap port :

Trap community :

Station 2 : ☒ Deactivate ☐ Activate

Trap Station IP :

Trap port :

Trap community :

Station 3 : ☒ Deactivate ☐ Activate

Trap Station IP :

Trap port :

Trap community :

At the bottom, there are "Apply" and "Cancel" buttons.

Step 7. Click “ **Enable** “ in “ **SNMP agent** “ to start the SNMP agent service

Step 8. Select “ **v1/v2** “ in “ **SNMP version** “

Step 9. Input “ **SNMP port** “. Default is 161.

Step 10. Input “ **sysContact** “. Default is human.being<nobody@but.you>

Step 11. Input “ **sysLocation** “. Default is Earth

Step 12. Input “ **sysName** “. Default is ATS-03-S

Step 13. Input “ **Read Community** “. Default is public

Step 14. Input “ **Write Community** “. Default is private

Step 15. Click “ **Activate** “ in Station 1 to enable the trap service

Step 16. Input “ **Trap Station IP** “ , “ **Trap Port** “ & “ **Trap Community** “ of Station 1

Step 17. Repeat Step 15 & 16 for Station 2 & 3

Step 18. Click “ **Apply** “ to finish the SNMP v1 / v2 settings

< 1.12 > SNMP Setup

ii. The following steps summarize how to enable the ATS for SNMP v3 support.

Step 1. Connect the ATS to a computer. (Please refer to < 1.6 > IP configuration)

Step 2. Open the Internet Explorer (I.E.) version 11.0

Step 3. Enter the configured ATS's address into the address bar
(Please refer to < 1.6 > IP configuration)

Step 4. Enter “ **Login name** “ , “ **Password** “

Default Login name : 00000000

Password: the one you set in Step 7 of < 1.6 > IP Configuration.

Step 5. Select SNMP from the left navigation pane



Step 6. The **SNMP** Settings window appears as below:

A screenshot of the 'SNMP' configuration window. At the top left is the title 'SNMP'. Below it, the 'SNMP agent' section has radio buttons for 'Enable' and 'Disable', with 'Disable' selected. Below this are input fields for 'SNMP version' (set to 'v1/v2'), 'SNMP port' (set to '161'), 'sysContact' (set to 'human.being<nobody@but.you>'), 'sysLocation' (set to 'Earth'), and 'sysName' (set to 'ATS-03-S'). The 'SNMP configuration' section has input fields for 'Read community' (set to 'public') and 'Write community' (set to 'private'). At the bottom, there are three columns for 'Station 1', 'Station 2', and 'Station 3'. Each column has radio buttons for 'Deactivate' and 'Activate', and input fields for 'Trap Station IP', 'Trap port', and 'Trap community'. For Station 1, 'Activate' is selected and IP is '192.168.1.113'. For Station 2, 'Deactivate' is selected and IP is '192.168.0.254'. For Station 3, 'Deactivate' is selected and IP is '192.168.0.254'. All 'Trap port' fields are set to '162' and all 'Trap community' fields are set to 'private'. At the bottom left are 'Apply' and 'Cancel' buttons.

< 1.12 > SNMP Setup

Step 7. Click “ **Enable** ” in “ **SNMP agent** ” to start the SNMP agent service

Step 8. Select “ **v3** ” in “ **SNMP version** ” & the SNMP v3 settings window appears as below :

SNMP

SNMP agent : ☒ Enable ☐ Disable

SNMP version : **v3**

SNMP port : 161

sysContact : human.being<nobody@but.you>

sysLocation : Earth

sysName : ATS-03-S

SNMP configuration

User 1 :	User 2 :	User 3 :
<input type="radio"/> Deactivate <input checked="" type="radio"/> Activate	<input checked="" type="radio"/> Deactivate <input type="radio"/> Activate	<input checked="" type="radio"/> Deactivate <input type="radio"/> Activate
User role : read only	User role : read only	User role : read only
USM user : usm_user1	USM user : usm_user2	USM user : usm_user3
Auth algorithm : None	Auth algorithm : None	Auth algorithm : None
Auth password : *****	Auth password : *****	Auth password : *****
Privacy algorithm : None	Privacy algorithm : None	Privacy algorithm : None
Privacy password : *****	Privacy password : *****	Privacy password : *****
SNMP trap : Disabled	SNMP trap : Disabled	SNMP trap : Disabled
Trap Station IP : 192.168.0.100	Trap Station IP : 192.168.0.254	Trap Station IP : 192.168.0.254
Trap port : 162	Trap port : 162	Trap port : 162

Apply Cancel

Step 9. Input “ **SNMP port** “. Default is 161.

Step 10. Input “ **sysContact** “. Default is human.being<nobody@but.you>

Step 11. Input “ **sysLocation** “. Default is Earth

Step 12. Input “ **sysName** “. Default is ATS-03-S

Step 13. Click “ **Activate** ” in User 1

Step 14. Select “ **Read Only** ” or “ **Read & Write** ” in User role :

Step 15. Input the name of “ **USM user** ” . Default is usm_user1

Step 16. Select “ **None / MD5 / SHA** ” in “ **Auth algorithm** ”.
If you select “ **Read & Write** ” in “ **User role** ” ,
you **MUST** select “ **MD5 / SHA** ” in “ **Auth algorithm** ”

Step 17. Input the “ **Auth password** ” Default is “ 00000000 ”

Step 18. Select “ **None / DES / AES / AES192 / AES256** ” in “ **Privacy algorithm** ” .
If the Auth algorithm is “ **NONE** ” , NO privacy algorithm can be selected.

Step 19. Input the “ **Privacy password** ”

Step 20. If you want to receive trap message, select “ **Enable** ” in SNMP trap

Step 21. Input the “ **Trap Station IP** ” & “ **Trap port** ”

Step 22. Repeat step 13 to 21 for User 2 & 3

Step 23. Click “ **Apply** ” to finish the SNMP v3 settings.

< 1.13 > Notification

In < **Notification** > , you can configure the alarm email server & max. 5 email recipients to receive alarm notifications from the IP dongle.

Default is “ **Disable** ”.

Step 1. “ **Enable** ” alarm email

Step 2. Enter “ **SMTP server** ” and “ **SMTP port** ”. Default is “ **Port 25** ”

Step 3. “ **Enable** ” or “ **Disable** ” the “ **SMTP authentication** “. Default is “ **Disable** ”

Step 4. Enter “ **User name** ” and “ **Password** ” when SMTP authentication is enabled

Step 5. Select the “ **secure connection** ” (None, SSL / TLS & STARTTLS). Default is “ **None** ”

Step 6. Enter the “ **Sender Name** ” and “ **Sender Email** ”

Step 7. Enter the “ **Alarm Interval** ”. (Min. 10, Max. 60 mins)

Step 8. Enter the alarm recipient email account in “ **Recipient 01** ”

Step 9. Repeat step 8 for other recipients

Step 10. Click “ **Apply** ” to finish the alarm email server setting

Email Notification

Alarm email : ☒ Enable ☐ Disable

SMTP server : smtp.austin-hughes.com

SMTP port : 25 (Default: 25)

Authentication : Enable ▼

User name : sender@mail.com

Password : *****

Secure connection : None ▼

Sender name : Email alarm

Sender email : sender@mail.com

Interval (minutes) : 10 (Min. 10, Max. 60)

Recipient 01 : recipient-01@mail.com

Recipient 02 :

Recipient 03 :

Recipient 04 :

Recipient 05 :

Apply Cancel

< 1.14 > Syslog

In < **Syslog** > , you can view the latest 2000 device and system log

Syslog <input type="button" value="Clear"/>			
#	Type	Date & Time	Event
1	System	2023-02-21 15:55:11	Change SNMP Settings
2	Device	2023-02-21 15:54:36	Input switch - Primary
3	System	2023-02-21 15:53:53	Change SNMP Settings
4	Device	2023-02-21 09:13:39	Switch outlet power ON(1) - Circuit A - Outlet 4 (04 , outlet_name_04)
5	Device	2023-02-21 09:13:02	Switch outlet power OFF(0) - Circuit A - Outlet 4 (04 , outlet_name_04)
6	Device	2023-02-20 18:09:59	Input switch - Secondary
7	Device	2023-02-20 18:08:03	Switch outlet power ON(1) - Circuit A - Outlet 4 (04 , outlet_name_04)
8	System	2023-02-20 18:07:42	2023-02-20,18:07:42.1,+0800 : User(00000000) from IP 192.168.0.100 login successfully.
9	System	2023-02-20 18:06:58	Change location to (default_ats_loc.)
10	System	2023-02-20 18:06:57	Change name to (default_ats_name)
11	Device	2023-02-20 18:06:32	ATS reconnection
12	System	2023-02-20 18:06:24	Start monitoring service
13	System	2023-02-20 18:06:17	ATS-03-S is started.
14	System	2023-02-20 18:05:34	Rebooting...
15	System	2023-02-20 18:05:10	2023-02-20,18:05:10.1,+0800 : User(00000000) from IP 192.168.0.100 login successfully.
16	System	2023-02-20 18:04:00	Change location to (default_ats_loc.)
17	System	2023-02-20 18:03:58	Change name to (default_ats_name)
18	Device	2023-02-20 18:01:55	Input switch - Primary
19	Device	2023-02-20 17:08:14	Switch outlet power OFF(0) - Circuit A - Outlet 4 (04 , outlet_name_04)
20	Device	2023-02-20 14:20:08	Change outlet alarm amp.(045) - Circuit A - Outlet 2 (02 , outlet_name_02)
21	Device	2023-02-20 14:19:32	Change outlet rising alert amp.(025) - Circuit A - Outlet 2 (02 , outlet_name_02)

< 1.15 > ATS Firmware Upgrade

For function enhancement of the intelligent ATS WEBUI , please take the following steps to remotely update the ATS firmware :

Step 1. Click the following link to go to the mangement software download page :

<http://www.austin-hughes.com/downloads/IPDL/IPDfirmware.html>

Step 2. Select the appropriate firmware file for intelligent ATS (IPD-03-S built-in)

Step 3. Connect the intelligent ATS to the computer. (Please refer to < 1.6 > IP configuration)

Step 4. Open the Internet Explorer (I.E.) version 11.0

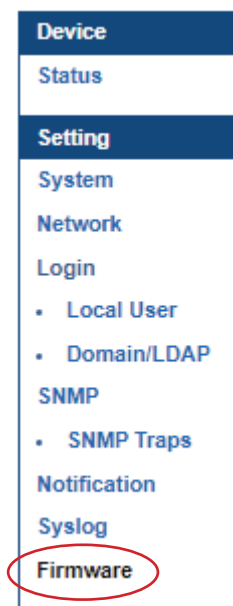
Step 5. Enter the configured ATS's IP address into the address bar
(Please refer to < 1.6 > IP configuration)

Step 6. Enter “ **Login name** ” & “ **Password** ”.

Default Login name : 00000000

Password: the one you set in Step 7 of < 1.6 > IP Configuration.

Step 7. Select the Firmware from the left navigation pane



< 1.15 > ATS Firmware Upgrade

Step 8. The firmware upgrade window appears as below :

Firmware

Device information

Device : ATS-03-S

Firmware version: ATS-03-FW-v1.1

Hardware revision: 2.0

LAN information

IPv4 address : 192.168.0.1

IPv6 address : ::ffff:c0a8:1/120

MAC address : 20:0A:0D:63:00:2D

Upgrade firmware

File path :

Warning : Upgrading firmware may take a few minutes,
please don't turn off the power or press the reset button.

Step 9. Click “ **Browse** ” and select the firmware file (xxx.enc) from the specific path in the pop up window and Click “ **Open** ”


Step 10. Click “ **Upgrade** ” to start the upgrade process. It takes a few minutes to complete.
(DO NOT close the web browser or refresh the web page during the upgrade process.)

Step 11. Once complete, the login page will display again. (If the login page does not display, open a new tab and try to access the login page.)

< 1.16 > Bulk Firmware Upgrade

< Bulk Firmware Upgrade via DHCP/TFTP >

If a TFTP server is available, you can use it to perform firmware upgrade for a huge number of intelligent ATS (IPD-03-S built-in) in the same network.

-  • The feature of bulk firmware upgrade via DHCP/TFTP only works on intelligent ATS (IPD-03-S built-in) directly connected to the network.
- The bulk firmware upgrade can ONLY be performed via IPv4 network.

< Procedure for Bulk Firmware Upgrade >

The bulk firmware upgrade feature only available for intelligent ATS (IPD-03-S built-in) firmware version v1.1 or above. Ensure the intelligent ATS (IPD-03-S built-in) firmware is v1.1 or above before you want to perform the upgrade.

Steps of using DHCP/TFTP for bulk firmware upgrade

Step 1. Change IP dongle firmware file in .enc format to ATS firmware file in .enc format

Step 2. Configure your TFTP server properly. See ***TFTP Requirements***

Step 3. Put ALL required files into a folder and COPY the folder to the TFTP root directory

Step 4. Properly configure your DHCP server so that it refers to the file “ **fwupdate.cfg** ” on the TFTP server for your intelligent ATS. See ***DHCP IPv4 Configuration in Windows***

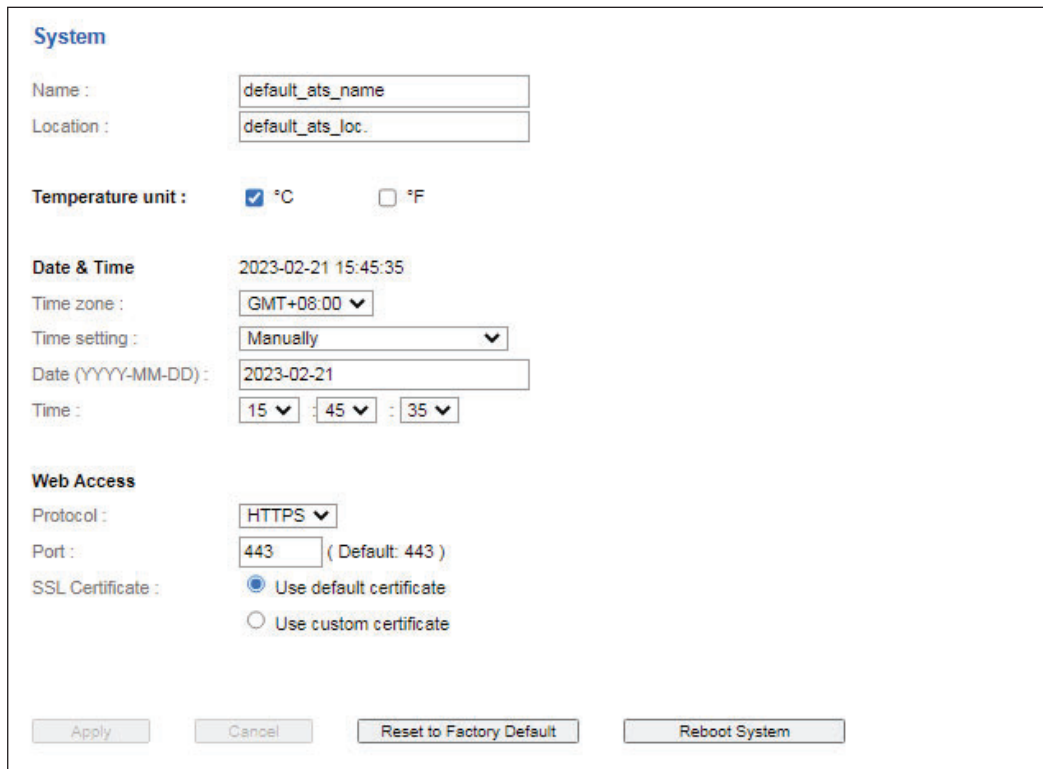
Step 5. Make sure all of the intelligent ATS use DHCP as the IP configuration method and have been directly connected to the network.



The default IP configuration of intelligent ATS is “ **STATIC** ”

< 1.16 > Bulk Firmware Upgrade

Step 6. Reboot the Intelligent ATS. The DHCP server will execute the commands in the “**fwupdate.cfg**” file on the TFTP server to upgrade those intelligent ATS supporting DHCP in the same network. You can Click “**Reboot System**” in “**System**” of intelligent ATS GUI.



The screenshot shows the 'System' configuration page of the Intelligent ATS GUI. It contains several sections: 'Name' and 'Location' fields with default values; 'Temperature unit' with radio buttons for °C (selected) and °F; 'Date & Time' section with a timestamp, time zone dropdown (GMT+08:00), time setting dropdown (Manually), and date/time input fields; 'Web Access' section with protocol dropdown (HTTPS), port input (443), and SSL certificate options (Use default certificate selected, Use custom certificate). At the bottom are four buttons: Apply, Cancel, Reset to Factory Default, and Reboot System.



You must enable firmware upgrade via DHCP in SSH (default is ENABLED) and input the username and password for bulk firmware upgrade in the “**fwupdate.cfg**” file. You can change the username and password for bulk firmware upgrade via SSH. **See *Configuration of username / password for bulk firmware upgrade.***

< 1.16 > Bulk Firmware Upgrade

Configuration of username / password for bulk firmware upgrade

Step 1. Access the SSH using putty

Step 2. Input the login name and password to login the CLI.

```
login as: 00000000
00000000@192.168.01.64's password:

*****
*                               *
*          System Status        *
*                               *
*****
* Firmware                      *
*   -FirmwareID   : ATS-03-FW-v1.1 *
*   -Build_info   : 20230222      *
*                               *
* Device                      *
*   -Model        : ATS-03-S      *
*   -Name         : default_ats_name *
*   -Location     : default_ats_loc. *
*   -Temp. unit   : C             *
*                               *
* Network settings             *
*   -Auto failover: Disable      *
*   [ LAN 1 (1000) ]           *
*   -LAN 1 link   : up (100)     *
*   -DHCP         : Disable      *
*   -MAC address  : 20:0A:0D:63:00:27 *
*   -IPv6 address : ::ffff:192.168.0.1/120 *
*****
```

Step 3. Select “ (U) Firmware upgrade ” and “ Enter ”

```
*   -IPM-04 support : Yes          *
*   -SNMP agent     : Enable        *
*   -WebUI HTTPS    : Enable TLSv1/1.2/1.3 *
*   -FTP server     : Disable       *
*   -UDP discovery  : Enable        *
*   -Telnet         : Disable       *
*   -SSH console    : Enable        *
*   -Service account : Enable       *
*   -Firmware upgrade: Disable      *
*****
*****
*                               *
*          Menu (Ver. 20.06.19) *
*                               *
*****
* (0) Show system status      *
* (1) Change System settings  *
* (2) Change Login settings   *
* (5) Reboot                  *
* (U) Firmware upgrade        *
* (F) Reset to factory default and reboot *
* (?) This menu               *
* (Q) Exit                    *
*****
Input menu item number(? for help):U
```

< 1.16 > Bulk Firmware Upgrade

Step 4. Select “ (5) Change firmware upgrade authentication ” and “ Enter ”

```
*****
* (0) Show system status *
* (1) Change System settings *
* (2) Change Login settings *
* (5) Reboot *
* (U) Firmware upgrade *
* (F) Reset to factory default and reboot *
* (?) This menu *
* (Q) Exit *
*****
Input menu item number(? for help):u
Input menu item number(? for help):U

*****
* Menu (Ver. 20.06.19) *
*****
* (0) Show system status *
* (1) Enable/Disable firmware upgrade via DHCP *
* (5) Change firmware upgrade authentication *
* (R) Reboot *
* (?) This menu *
* (Q) Exit *
*****
Input menu item number(? for help):5
```

Step 5. Select “ (1) Change authentication name ” or “ (2) Change authentication password ” to change the username or password for bulk firmware upgrade purpose.

```
Input menu item number(? for help):U

*****
* Menu (Ver. 20.06.19) *
*****
* (0) Show system status *
* (1) Enable/Disable firmware upgrade via DHCP *
* (5) Change firmware upgrade authentication *
* (R) Reboot *
* (?) This menu *
* (Q) Exit *
*****
Input menu item number(? for help):5

*****
* Firmware upgrade authentication *
*****
* (0) Show system status *
* (1) Change authentication name *
* (2) Change authentication password *
* (?) This menu *
* (Q) Exit *
*****
Input menu item number(? for help):
```

< 1.16 > Bulk Firmware Upgrade

< TFTP Requirements >

To perform bulk firmware upgrade successfully, your TFTP server must meet the following requirements :



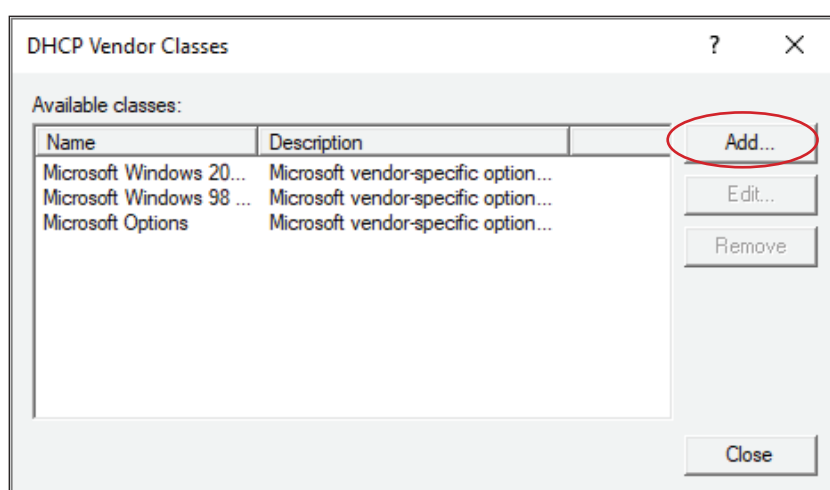
- Able to work with IPv4
- A folder containing all required files is available in the TFTP root directory. The folder name **MUST** be the same as the String value of the Magic code. Details please refer to DHCP IPv4 Configuration in Windows
- The TFTP server supports the write operation including file creation and upload.

< DHCP IPv4 Configuration in Windows >

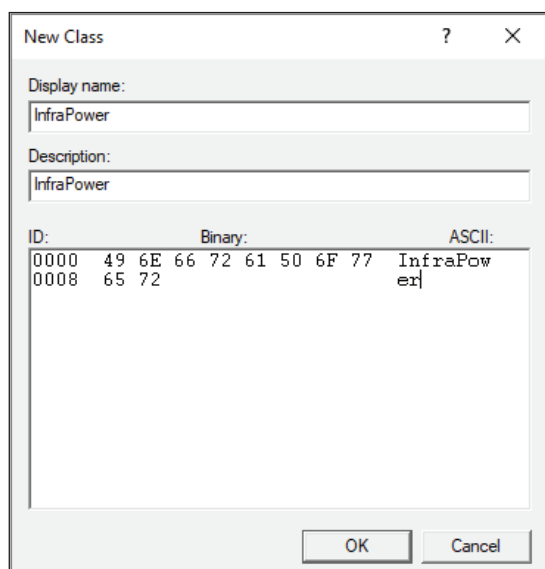
Please follow the procedures below to configure your DHCP server. The illustration below is based on Microsoft Windows Server 2019

Step 1. Add a new vendor class for Austin Hughes Intelligent ATS

- Right Click the IPv4 node in DHCP to select Define Vendor Classes (under server manager, select tools > DHCP
- Click “ **Add** ” to add a new vendor class.



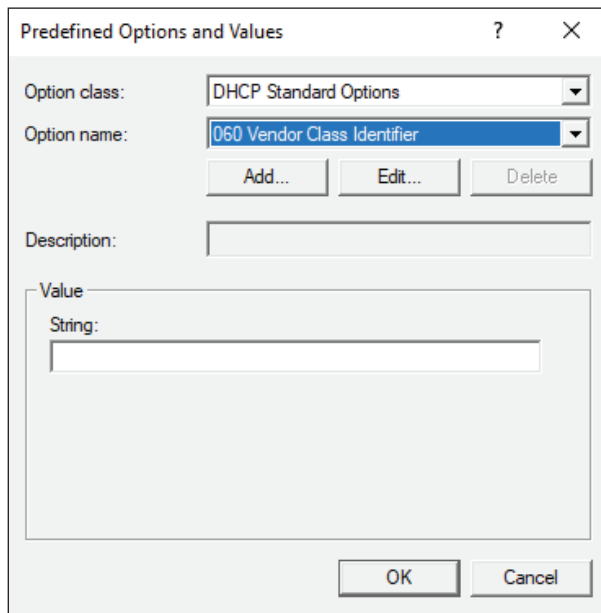
- Specify a unique name for this vendor class and type the binary codes of “ **InfraPower** ” in the New Class dialog. The vendor class is named “ **InfraPower** ” in this illustration.



< 1.16 > Bulk Firmware Upgrade

Step 2. Define one DHCP standard option – Vendor Class Identifier

- Right Click the IPv4 node in DHCP to select Set Predefined Options.
- Select “ **DHCP Standard Options** ” in the “ **Option class** ” field, and “ **Vendor Class Identifier** ” in the “ **Option name** ” field. Leave the String field blank.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 060 Vendor Class Identifier

Add... Edit... Delete

Description:

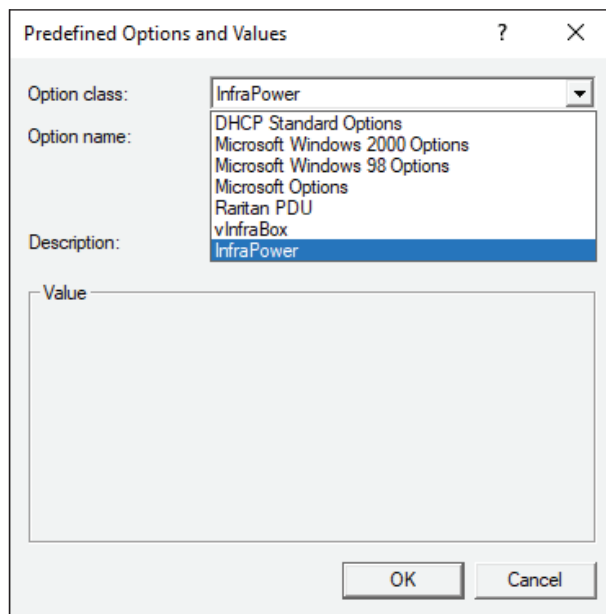
Value

String:

OK Cancel

Step 3. Add four options to the new vendor class “ **InfraPower** ” in the same dialog. The fourth option is an optional item if the UDP port you set for the TFTP server is NOT 69.

- Select “ **InfraPower** ” in the “ **Option class** ” field.



Predefined Options and Values

Option class: InfraPower

Option name: DHCP Standard Options
Microsoft Windows 2000 Options
Microsoft Windows 98 Options
Microsoft Options
Raritan PDU
vInfraBox
InfraPower

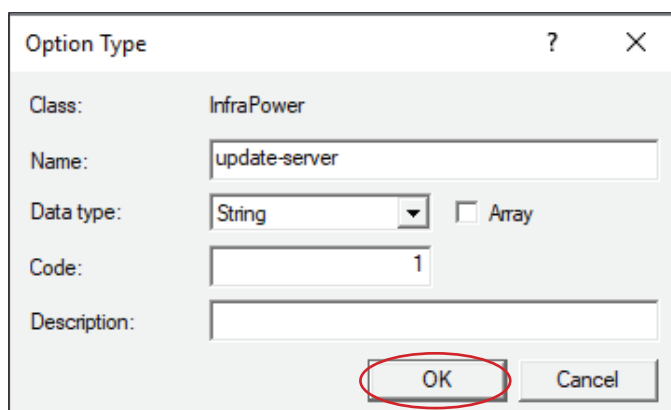
Description:

Value

OK Cancel

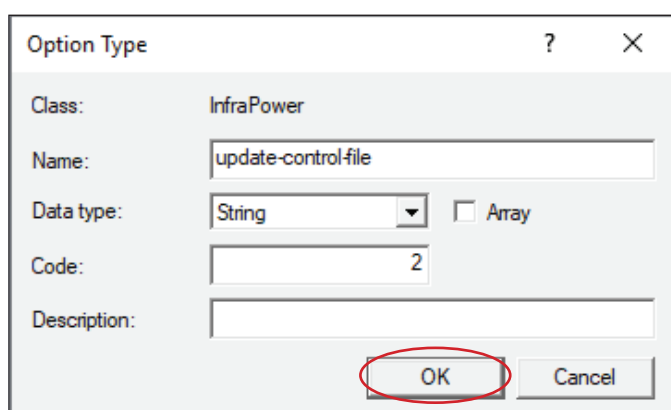
< 1.16 > Bulk Firmware Upgrade

- Click “ **Add** ” to add the first option. Type “ **update-server** ” in the Name field, select String as the data type, and type 1 in the Code field and Click “ **OK** ”.



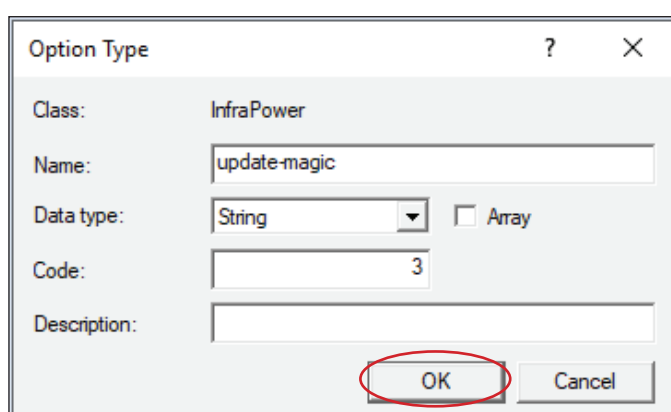
The dialog box titled "Option Type" has a Class field set to "InfraPower". The Name field contains "update-server". The Data type dropdown is set to "String", and the Array checkbox is unchecked. The Code field contains "1". The Description field is empty. The OK button is circled in red.

- Click “ **Add** ” to add the second option. Type “ **update-control-file** ” in the Name field, select String as the data type, and type 2 in the Code field and Click “ **OK** ”.



The dialog box titled "Option Type" has a Class field set to "InfraPower". The Name field contains "update-control-file". The Data type dropdown is set to "String", and the Array checkbox is unchecked. The Code field contains "2". The Description field is empty. The OK button is circled in red.

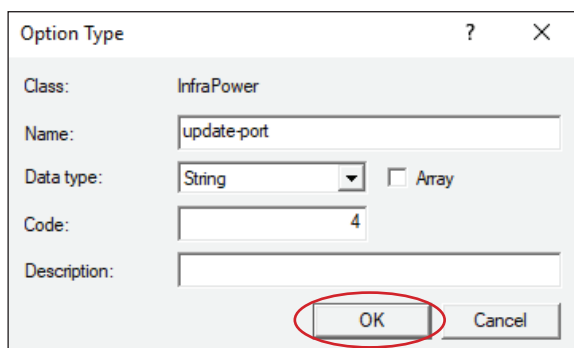
- Click “ **Add** ” to add the third option. Type “ **update-magic** ” in the Name field, select String as the data type, and type 3 in the Code field and Click “ **OK** ”.



The dialog box titled "Option Type" has a Class field set to "InfraPower". The Name field contains "update-magic". The Data type dropdown is set to "String", and the Array checkbox is unchecked. The Code field contains "3". The Description field is empty. The OK button is circled in red.

< 1.16 > Bulk Firmware Upgrade

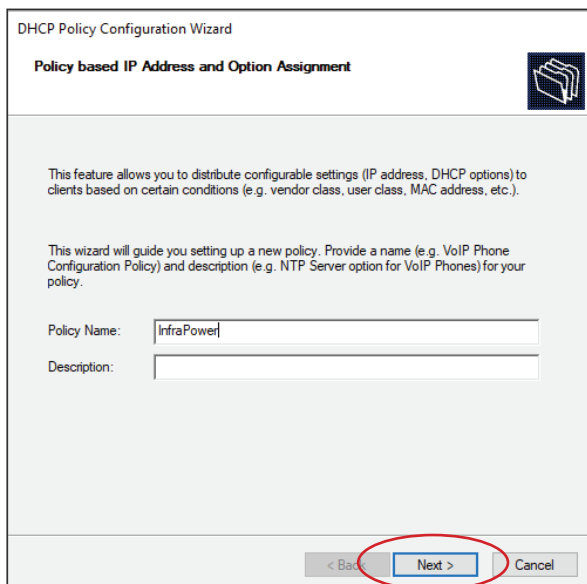
- Click “ **Add** ” to add the fourth option. Type “ **update-port** ” in the Name field, select String as the data type, and type 4 in the Code field and Click “ **OK** ”.



The 'Option Type' dialog box is shown. It has a title bar with a question mark and a close button. The 'Class' is set to 'InfraPower'. The 'Name' field contains 'update-port'. The 'Data type' is set to 'String' with a dropdown arrow, and there is an unchecked 'Array' checkbox. The 'Code' field contains '4'. The 'Description' field is empty. At the bottom, the 'OK' button is circled in red, next to a 'Cancel' button.

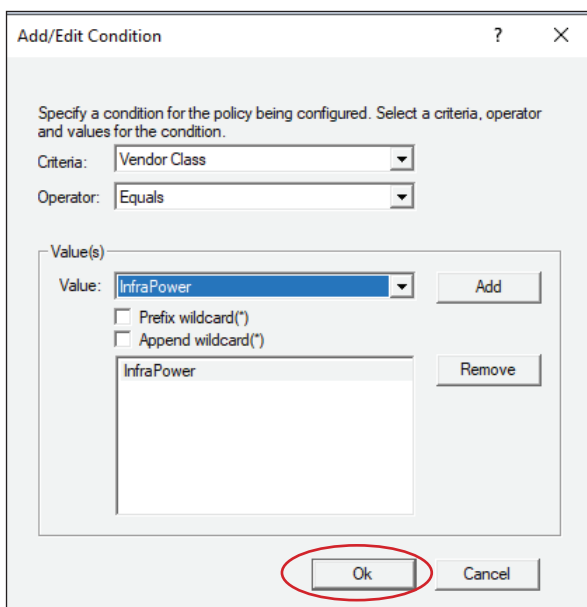
Step 4. Create a new policy associated with the “ **InfraPower** ” vendor class.

- Right Click the Policies node under IPv4 to select New Policy.
- Specify a policy name and click “ **Next** ”. The policy is named “ **InfraPower** ” in this illustration.



The 'DHCP Policy Configuration Wizard' is shown. The title bar says 'DHCP Policy Configuration Wizard'. The main title is 'Policy based IP Address and Option Assignment'. Below this, there is explanatory text: 'This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).' and 'This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.' There are two input fields: 'Policy Name' with 'InfraPower' entered, and 'Description' which is empty. At the bottom, the 'Next >' button is circled in red, next to '< Back' and 'Cancel' buttons.

- Click “ **Add** ” to add a new condition
- Select the vendor class “ **InfraPower** ” in the Value field, click “ **Add** ” and then “ **OK** ”.



The 'Add/Edit Condition' dialog box is shown. It has a title bar with a question mark and a close button. The text says 'Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.' There are two dropdown menus: 'Criteria' set to 'Vendor Class' and 'Operator' set to 'Equals'. Below these is a 'Value(s)' section. It has a 'Value:' dropdown set to 'InfraPower' with an 'Add' button next to it. There are two unchecked checkboxes: 'Prefix wildcard(*)' and 'Append wildcard(*)'. Below these is a list box containing 'InfraPower' with a 'Remove' button next to it. At the bottom, the 'Ok' button is circled in red, next to a 'Cancel' button.

< 1.16 > Bulk Firmware Upgrade

- Click “ **Next** ”.
- Select “ **DHCP Standard Options** ” in the “ **Vendor class** ” field, select “ **060 Vendor Class Identifier** ” from the Available Options list, and type “ **InfraPower** ” in the “ **String value** ” field.

DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: **DHCP Standard Options**

Available Options	Description
<input checked="" type="checkbox"/> 060 Vendor Class Identifier	
<input type="checkbox"/> 064 NIS+ Domain Name	The name of the client's NIS+
<input type="checkbox"/> 065 NIS+ Servers	A list of IP addresses indicatinc

Data entry

String value:
InfraPower

< Back Next > Cancel

- Select the “ **InfraPower** ” in the “ **Vendor class** ” field, select “ **001 update-server** ” from the Available Options list, and type your TFTP server's IPv4 address in the “ **String value** ” field.

DHCP Policy Configuration Wizard

Configure settings for the policy
If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: **InfraPower**

Available Options	Description
<input checked="" type="checkbox"/> 001 update-server	
<input type="checkbox"/> 002 update-control-file	
<input type="checkbox"/> 003 update-magic	
<input type="checkbox"/> 004 vendorclass	vendorclass

Data entry

String value:
192.168.0.1

< Back Next > Cancel

< 1.16 > Bulk Firmware Upgrade

- Select “ **002 update-control-file** ” from the Available Options list, and type the filename “ **fwupdate.cfg** ” in the “ **String value** ” field.

The screenshot shows the 'DHCP Policy Configuration Wizard' window. The title bar says 'DHCP Policy Configuration Wizard'. Below the title bar, there is a section 'Configure settings for the policy' with a sub-note: 'If the conditions specified in the policy match a client request, the settings will be applied.' To the right of this section is a folder icon. Below this, there is a 'Vendor class:' dropdown menu with 'InfraPower' selected. Underneath is a table with two columns: 'Available Options' and 'Description'. The table contains four rows: '001 update-server' (checked), '002 update-control-file' (checked), '003 update-magic' (unchecked), and '004 vendorclass' (unchecked) with 'vendorclass' in the description column. Below the table is a 'Data entry' section with a 'String value:' label and a text box containing 'fwupdate.cfg'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- Select “ **003 update-magic** ” from the Available Options list, and type folder name of the files you stored in the root directory of the TFTP server in the “ **String value** ” field. This String value is the magic code to prevent the fwupdate.cfg commands from being executed repeatedly.

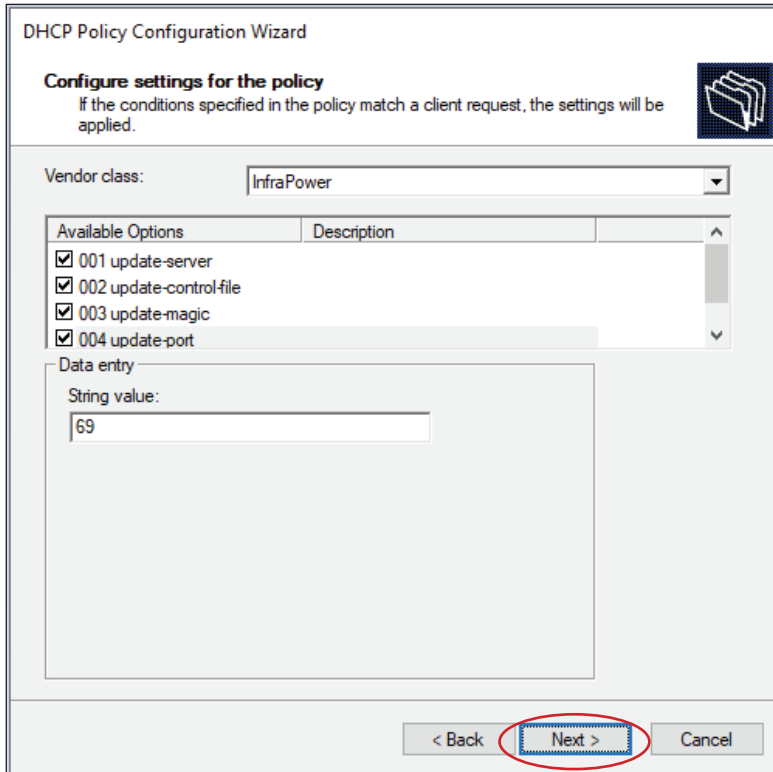
The screenshot shows the 'DHCP Policy Configuration Wizard' window. The title bar says 'DHCP Policy Configuration Wizard'. Below the title bar, there is a section 'Configure settings for the policy' with a sub-note: 'If the conditions specified in the policy match a client request, the settings will be applied.' To the right of this section is a folder icon. Below this, there is a 'Vendor class:' dropdown menu with 'InfraPower' selected. Underneath is a table with two columns: 'Available Options' and 'Description'. The table contains four rows: '001 update-server' (checked), '002 update-control-file' (checked), '003 update-magic' (checked), and '004 vendorclass' (unchecked) with 'vendorclass' in the description column. Below the table is a 'Data entry' section with a 'String value:' label and a text box containing 'ATS-03-FW-v1.1'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.



The magic code is transmitted to and stored in Intelligent ATS at the time of executing the “ **fwupdate.cfg** ” commands. The DHCP/TFTP operation is triggered ONLY when there is a mismatch between the magic code in DHCP and the one stored in the Intelligent ATS. Therefore, you must modify the magic code’s value in DHCP when intending to execute the “ **fwupdate.cfg** ” commands next time.

< 1.16 > Bulk Firmware Upgrade

- Select “ **004 update-port** ” from the Available Options list, and type UDP port number you set for the TFTP server in the “ **String value** ” field. Port number 69 is used in this illustration.



The screenshot shows the 'DHCP Policy Configuration Wizard' window. At the top, it says 'Configure settings for the policy' and 'If the conditions specified in the policy match a client request, the settings will be applied.' Below this, the 'Vendor class' is set to 'InfraPower'. A table lists 'Available Options' with their descriptions: '001 update-server', '002 update-control-file', '003 update-magic', and '004 update-port'. All four options are checked. Below the table, the 'Data entry' section has a 'String value:' field containing the number '69'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red oval.

Available Options	Description
<input checked="" type="checkbox"/> 001 update-server	
<input checked="" type="checkbox"/> 002 update-control-file	
<input checked="" type="checkbox"/> 003 update-magic	
<input checked="" type="checkbox"/> 004 update-port	

Data entry

String value:

69

< Back **Next >** Cancel

- Click “ **Next** ” and “ **Finish** ” to complete the setup.

< 1.16 > Bulk Firmware Upgrade

Description of Devices.csv

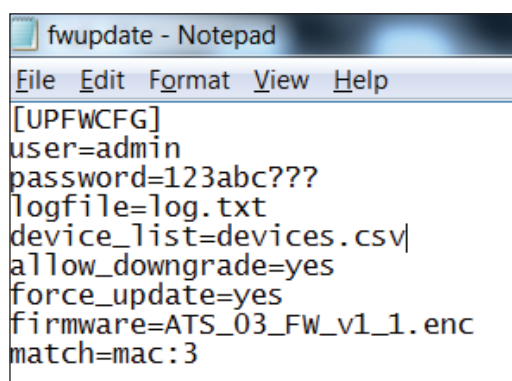
	A	B	C	D	E
1	1	1	20:0A:0D:FF:CA:BF	192.168.0.123	192.168.0.1
2	1	1	20:0A:0D:FF:3C:E6	192.168.0.122	192.168.0.1
3	#--keep this be the last line of this file--				
4					
5					

Column A & B is reserved for future use

Column C is the MAC address of the network interface of Intelligent ATS.

Column D & E is the IP address of the network interface of the Intelligent ATS and the TFTP server respectively.

Description of fwupdate.cfg



```
[UPFWCFG]
user=admin
password=123abc???
logfile=log.txt
device_list=devices.csv
allow_downgrade=yes
force_update=yes
firmware=ATS_03_FW_v1_1.enc
match=mac:3
```

First and second row is the user and password for authentication of bulk firmware upgrade which can be configured via SSH. Details refer to Section “**Configuration of username / password for bulk firmware upgrade**”.

Fourth row tells the TFTP server to generate a log file after bulk firmware upgrade is performed. It is stored at the same location of the fwupdate.cfg and the filename is the same as the MAC address of the Intelligent ATS.

Fifth row lets Intelligent ATS to check if its’ MAC address exists in the column 3 of devices.csv to execute the firmware upgrade.

Eighth row is the firmware version you want to upgrade, it MUST be the same as the filename of the firmware stored in the folder under the root directory of the TFTP server.

< 1.17 > 802.1X authentication

User Guide of 802.1X Authentication

802.1X is an authentication protocol which provides protected authentication for secure network access with the use of a Radius server. It opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.

802.1X authentication function ONLY available at Intelligent ATS (IPD-03-S built-in) firmware version v1.1 or above.

Before configure the 802.1X authentication, ensure the system clock of the Intelligent ATS is set up properly. Otherwise, the authentication will fail while the RADIUS server verifies the validity of the certificate. You can go the System page to set up the date and time of the Intelligent ATS.

The screenshot displays the 'System' configuration page of the Intelligent ATS. On the left is a navigation menu with categories: Device, Status, Setting, and sub-items under Setting including System, Network, Login, Local User, Domain/LDAP, SNMP, SNMP Traps, Notification, Syslog, and Firmware. The 'System' section is active. The main content area is titled 'System' and contains the following fields and options:

- Name :** default_ats_name
- Location :** default_ats_loc.
- Temperature unit :** ☒ °C ☐ °F
- Date & Time**
 - Date & Time**: 2023-02-21 15:45:35
 - Time zone :** GMT+08:00
 - Time setting :** Manually
 - Date (YYYY-MM-DD) :** 2023-02-21
 - Time :** 15 : 45 : 35
- Web Access**
 - Protocol :** HTTPS
 - Port :** 443 (Default: 443)
 - SSL Certificate :** ☒ Use default certificate ☐ Use custom certificate

At the bottom of the page are four buttons: Apply, Cancel, Reset to Factory Default, and Reboot System.

< 1.17 > 802.1X authentication

Please follow the procedures below to setup the 802.1X authentication in Intelligent ATS WEBUI.

Step 1. Login the Intelligent ATS's WEBUI and go the Network.

Network

LAN settings

DHCP : OFF ▾

IPv4 address : 192.168.0.1

IPv6 address : ::ffff:c0a8:1/120

Subnet mask : 255.255.255.0

Gateway : 192.168.0.254

Authentication : None ▾

DNS

Manually configure DNS server : ☒

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Apply Cancel

Step 2. Click the Authentication pull down menu and you will see the authentication method.

Network

LAN settings

DHCP : ON ▾

IPv4 address : 192.168.0.1

IPv6 address : ::ffff:c0a8:1/120

Subnet mask : 255.255.255.0

Gateway : 192.168.0.254

Authentication :

None ▾
None
PEAP
TLS

DNS

Manually configure DNS server : ☒

Primary DNS : 8.8.8.8

Secondary DNS : 0.0.0.0

Apply Cancel

< 1.17 > 802.1X authentication

Step 3. To use PEAP as authentication method, select PEAP. Then input the “ **Identity** ”, “ **Password** ” and “ **CA certificate** ” in PEM format. You can uncheck “ **Enable CA certificate** ” to bypass the authentication using CA certificate.

Click “ **Apply** ” to save the configuration.

The screenshot shows the 'Network' configuration window. Under 'LAN settings', the 'Authentication' dropdown is set to 'PEAP'. The 'Identity' field contains 'administrator', the 'Password' field is masked with dots, and the 'CA certificate' field is empty with a 'Browse' button next to it. The 'Enable CA certificate' checkbox is unchecked. Under 'DNS', 'Manually configure DNS server' is checked, 'Primary DNS' is '8.8.8.8', and 'Secondary DNS' is '0.0.0.0'. At the bottom, the 'Apply' button is circled in red.

Step 4. To use TLS as authentication method, select TLS. Then input the “ **Identity** ”, “ **Certificate** ”, “ **Private key** ”, “ **Private key password** ” and “ **CA certificate** ”. (Certificate, private key and CA certificate are in PEM format)

Click “ **Apply** ” to save the configuration.

The screenshot shows the 'Network' configuration window with 'Authentication' set to 'TLS'. The 'Identity' field contains 'administrator'. The 'Certificate', 'Private key', and 'CA certificate' fields are empty, each with a 'Browse' button. Red error messages 'Certificate is required.' and 'Private key is required.' are displayed below their respective fields. The 'Private key password' field is masked with dots. The 'Enable CA certificate' checkbox is unchecked. Under 'DNS', 'Manually configure DNS server' is checked, 'Primary DNS' is '8.8.8.8', and 'Secondary DNS' is '0.0.0.0'. At the bottom, the 'Apply' button is circled in red.

< 1.18 > Command Line Interface (CLI) Access

Command Line Interface (CLI) allows you access the ATS via Telnet or Secure Shell (SSH) to configure the system settings and login settings.

By default, CLI access via SSH is enabled and Telnet is disabled whereas Telnet can be enabled.

Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption.

If you want high security access, you can use SSH for access to the command line interface. SSH encrypts user name, password and transmitted data.

If you use SSH to access the command line interface, DISABLE Telnet.

CLI and ATS WEBUI shares the same login name & password

Default login name : 00000000

Password : the one you set in Step 7 of < 1.6 > IP Configuration

You can change the following settings via CLI access :

- i. System settings
 - Change temperature display unit : change the temp unit to be displayed in the WEBUI
 - Change the system RTC date time : set the system time of the ATS
 - Change network settings : change the IP settings of the ATS
 - Change features & services
 - a. Enable / disable management software support. Default is Enabled.
 - b. Enable / disable SNMP agent. Default is Disabled.
 - c. Enable / disable WEBUI. Default is Enabled.
 - d. Enable / disable FTP server. Default is Disabled.
 - e. Enable / disable UDP (When disabled, ATS CANNOT be found by IP setup utilities). Default is Enabled.
 - f. Enable / disable Telnet. Default is Disabled.
 - g. Enable / disable maintenance (service) account. Default is Disabled.
 - h. Enable / disable HTTPS. Default is Enabled.
- ii. Login settings
 - Change login name
 - Change login password
 - Reset to default login name & password
- iii. Firmware upgrade
 - Enable / disable firmware upgrade via DHCP (For bulk firmware upgrade). Default is Enabled.
 - Change firmware upgrade authentication (change username and password for bulk firmware upgrade authentication).

The company reserves the right to modify product specifications without prior notice and assumes no responsibility for any error which may appear in this publication.

All brand names, logo and registered trademarks are properties of their respective owners.

Copyright 2023 Austin Hughes Electronics Ltd. All rights reserved.