InfraPower®

Inspired by Your Data Center

User Manual

ATS-03-S **WEBUI**

Designed and manufactured by Austin Hughes

FC CE RoHS REACH

Legal Information

First English printing, August 2023

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 40º Celsius (104º 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 dam aged 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 business, industrial and commercial environments.

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.

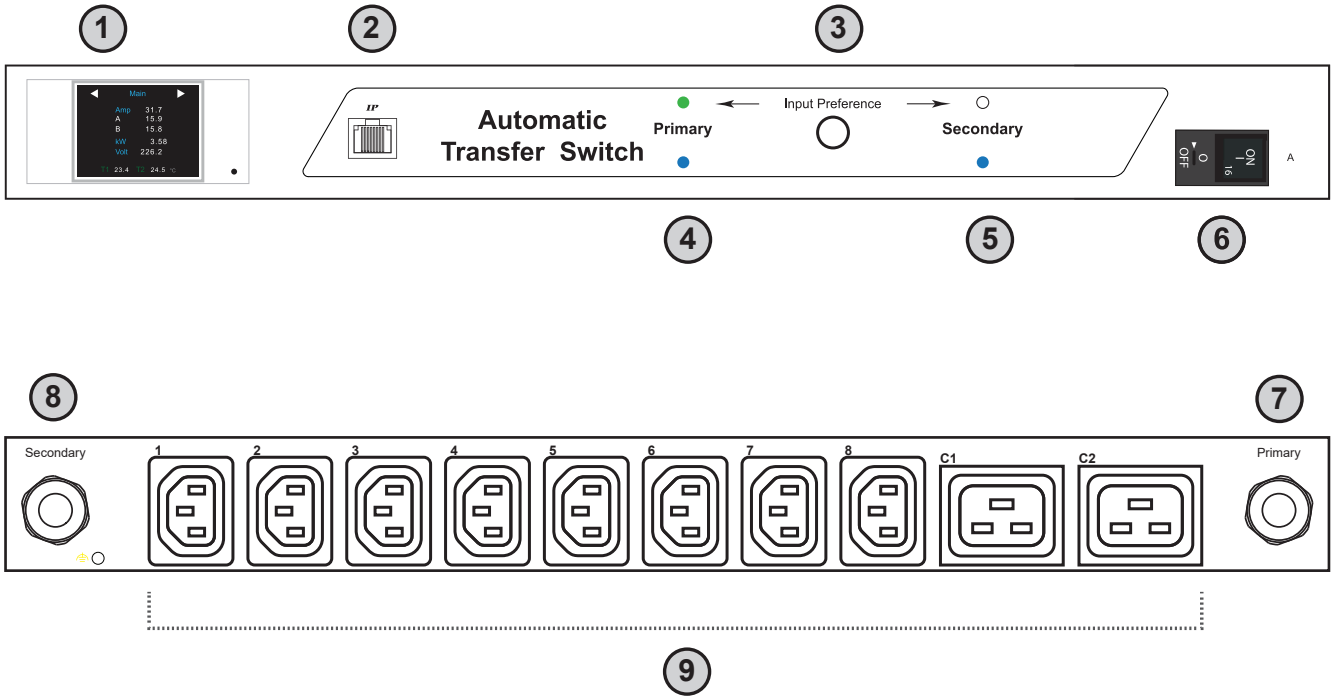
However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one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



1. 2.0" color LCD (feature w/ Touchscreen)
2. IP Port
3. Input Preference Switch
4. Power LED - primary input
5. Power LED - secondary input
6. Circuit Breaker
7. Primary Input attached with 3M cord & inlet plug
8. Secondard Input attached with 3M cord & inlet plug
9. 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

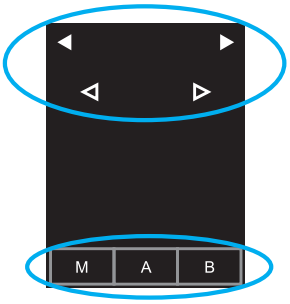
Once ATS current loading is over the rated input current, input switching is not allowed either by local or remote. However, automatic switching is NOT affected.

< 1.3 > Meter Reading & Setting

Reading

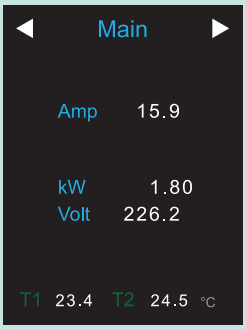
- Amp, Voltage & Power Factor
- kWh Energy Consumption
- Active & Apparent Power
- Temp. & Humidity

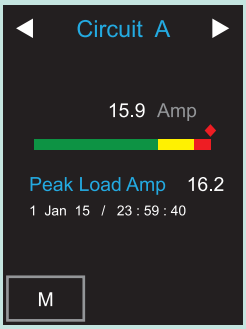
Touch Button
(Single & Dual Circuit)



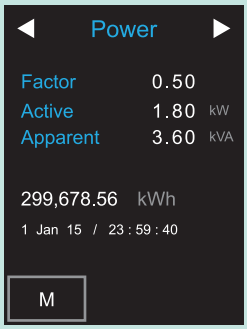
Single Circuit

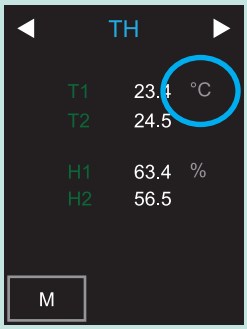
1 - 3

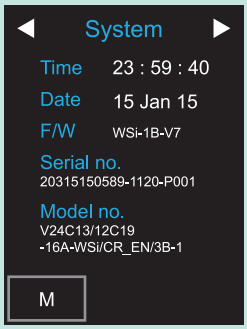


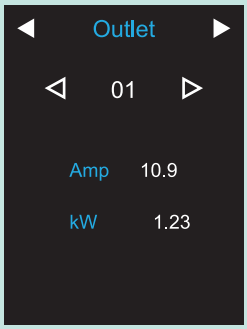


4 - 7







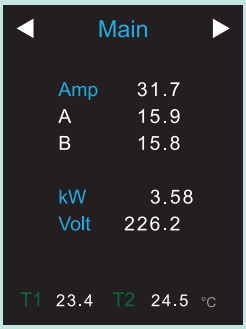


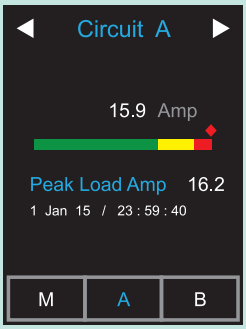
Page no.5
Touch °C / °F to change temp. unit
* ATS does not support any sensor

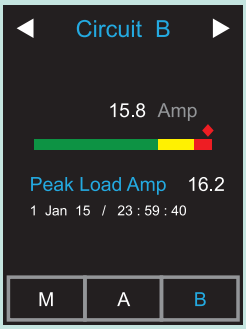
Page no.7
Wi / WSi outlet measurement PDU only

Dual Circuit

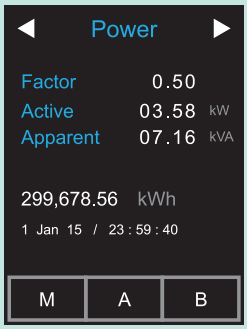
1 - 4

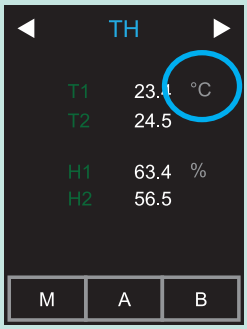


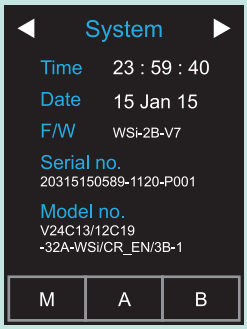


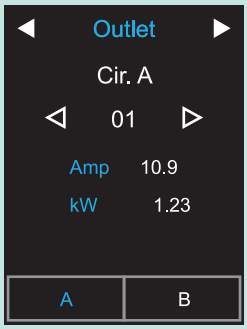


5 - 8







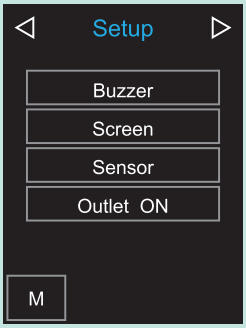


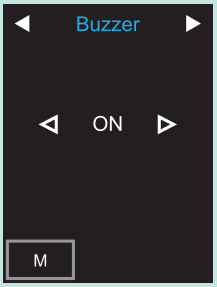
Page no.6
Touch °C / °F to change temp. unit
* ATS does not support any sensor

Page no.8
Wi / WSi outlet measurement PDU only

< 1.3 > Meter Reading & Setting

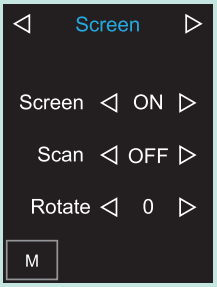
Setting





Buzzer ON / OFF

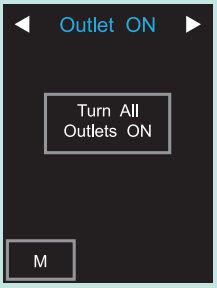
Default : ON



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

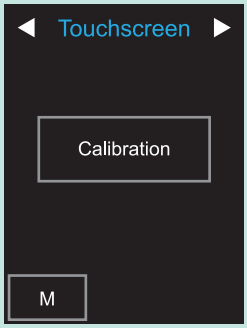
* **ON Scan :**
- Scanning starts in 30 seconds
- Then scan each page per 3 seconds



Outlet ON / OFF

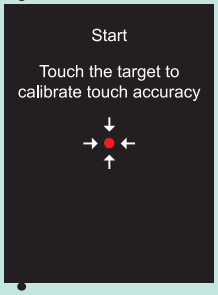
Default : ON

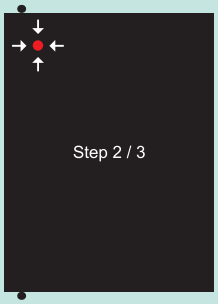
WS / WSi Switched PDU only

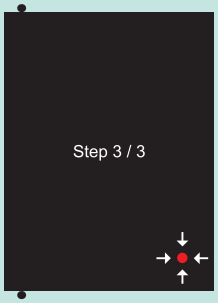


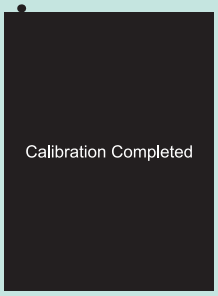
Touchscreen Calibration

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	✔

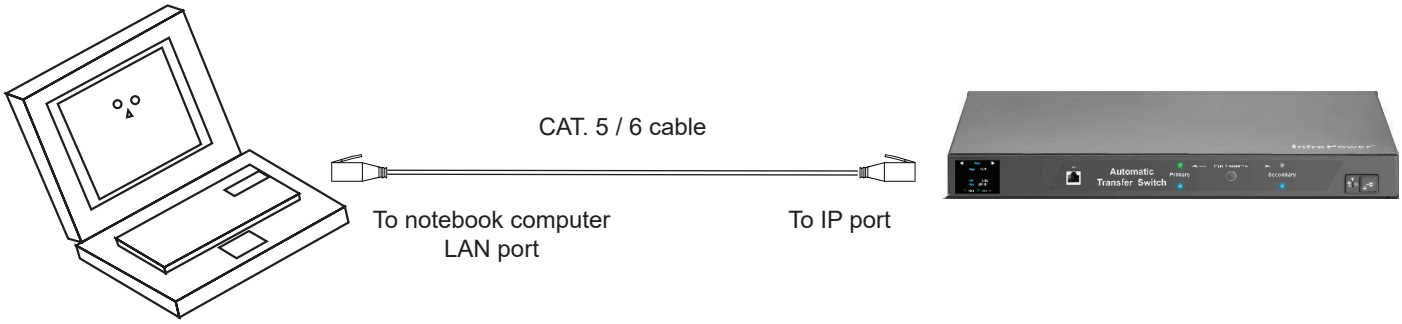
< 1.6 > IP Configuration

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

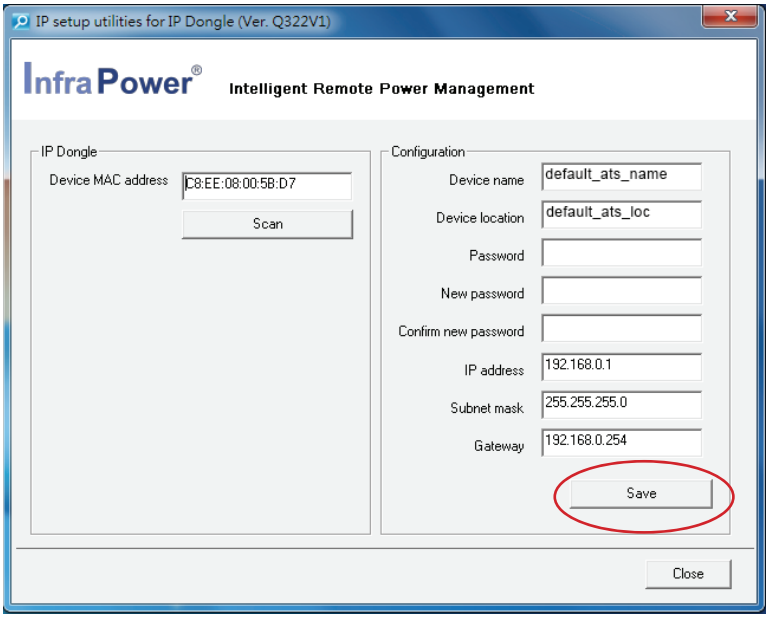
Step 1. Prepare a notebook computer to download the IP setup utilities from the link : http://www.austin-hughes.com/support/utilities/infrapower/IPdongleSetup.msi

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.



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

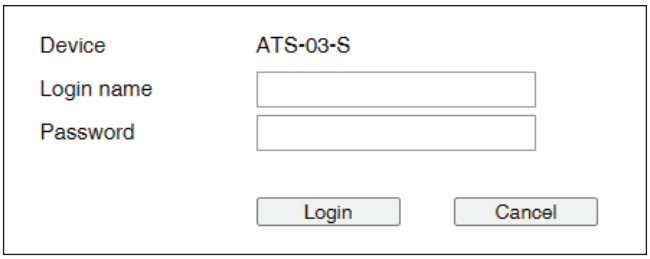
Each ATS provides a FREE built-in GUI, ATS-03-S, which allows user, via a web browser, to monitor the ATS status over a TCP / IP Ethernet network remotely.

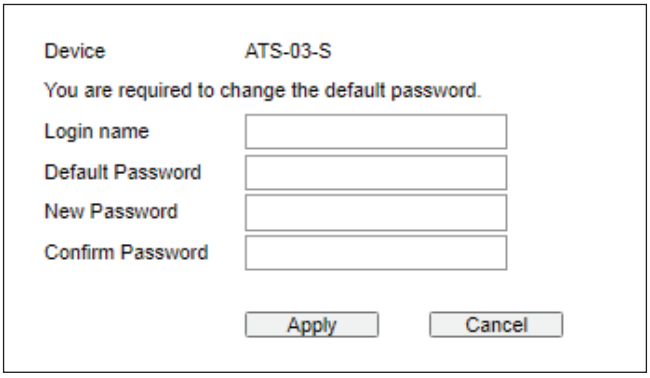
Each web browser window supports only one ATS. If you install more ATS, multi windows will be required.

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

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

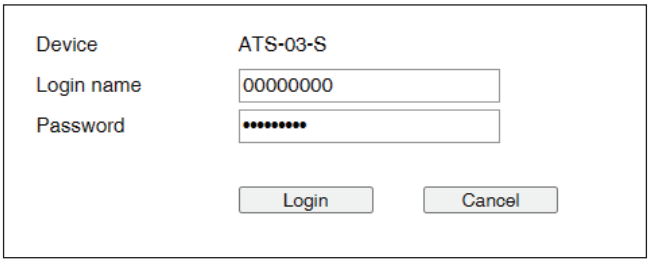
Step 2. Enter the configured ATS's IP address into the address bar
(Please refer to < 1.6 > IP configuration)





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** "

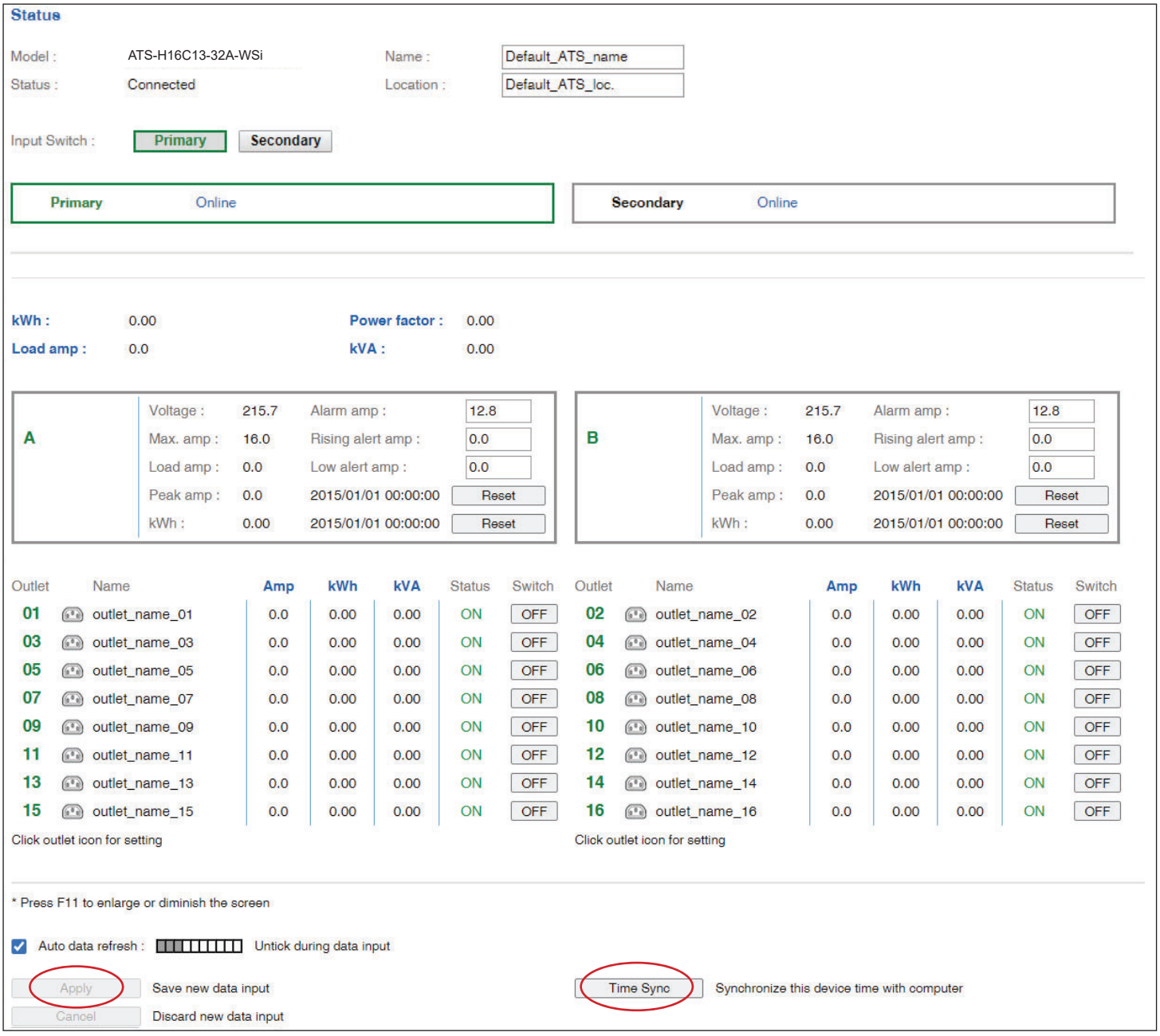


Default Login name : 00000000
Password : the one you set in Step 7 of < 1.6 > IP Configuration.
The login account will be LOCKED for 5 mins if three unsuccessful login attempts to the ATS GUI

< 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)

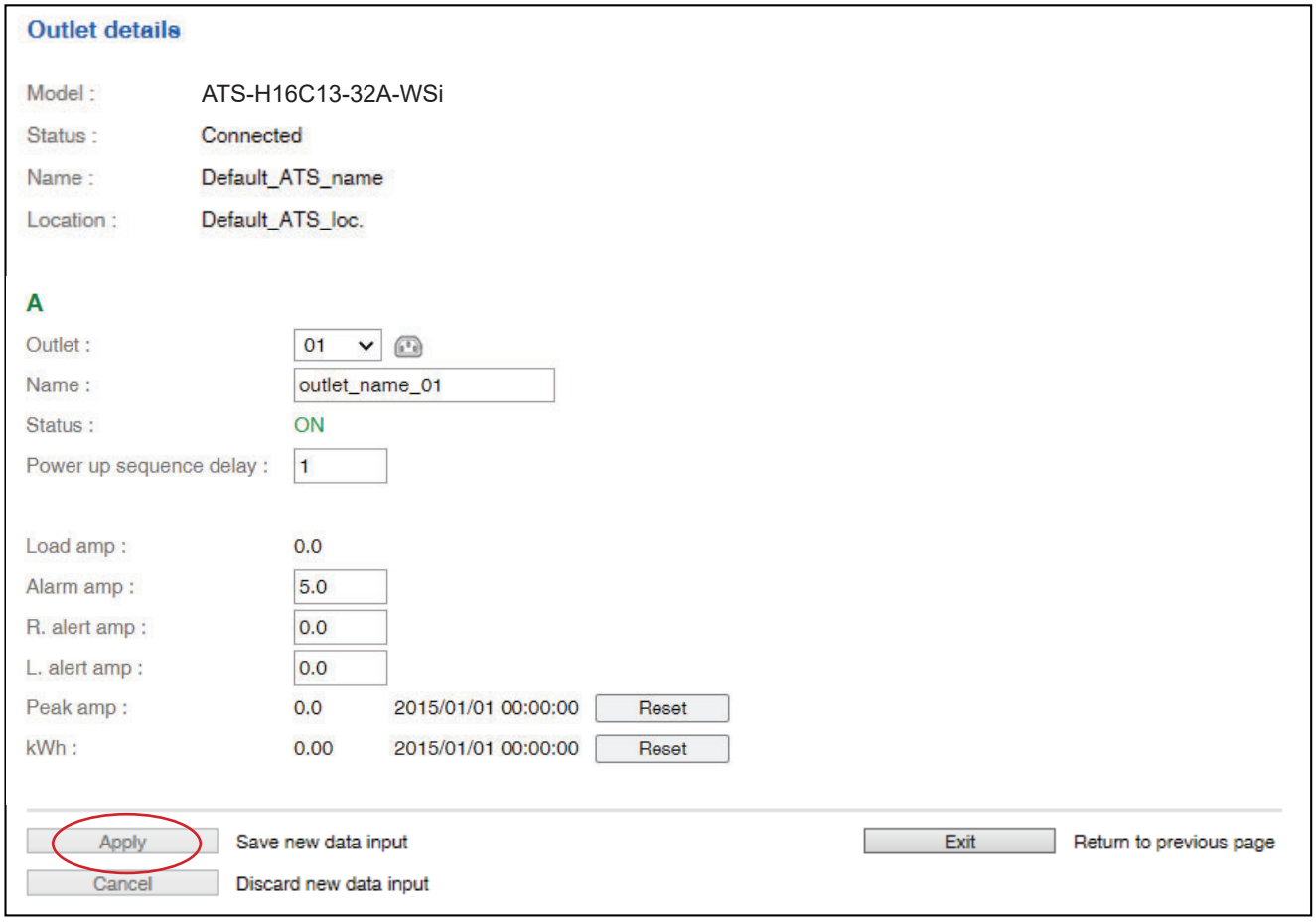


Once ATS current loading is over the rated input current, input switching is NOT allowed either by local or remote

< 1.7 > ATS-03-S GUI

In < **Outlet details** >,

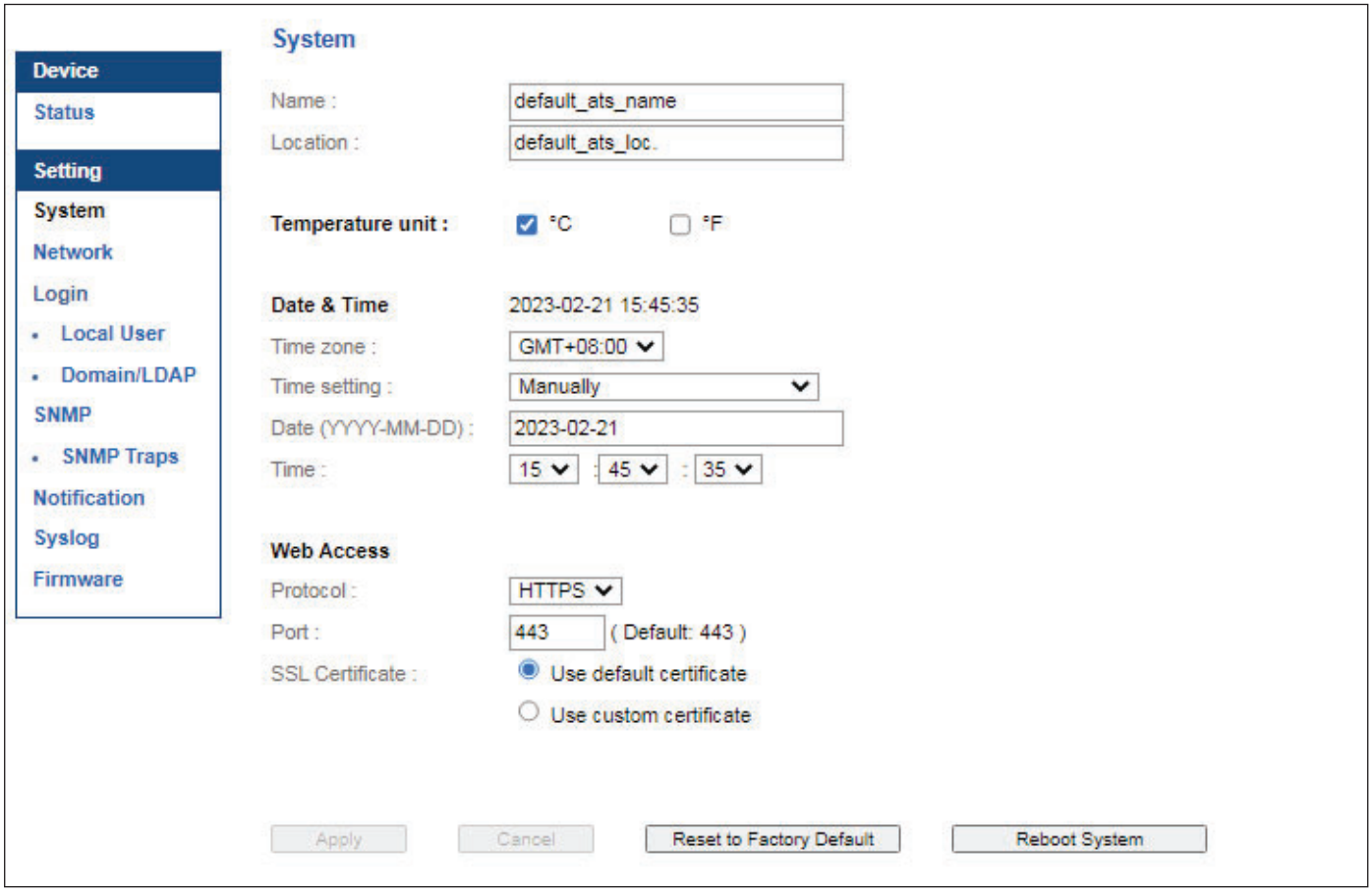
- Change PDU outlet name
- Change " Power up sequence delay " (Outlet Switched PDU only)
- Change " Alarm amp. " , " Rising alert amp. " & " Low alert amp. " (Outlet Measurement PDU only)
  Click " Apply " to finish the above settings
- Click " Reset " to reset peak amp. or kWh (Outlet Measurement PDU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

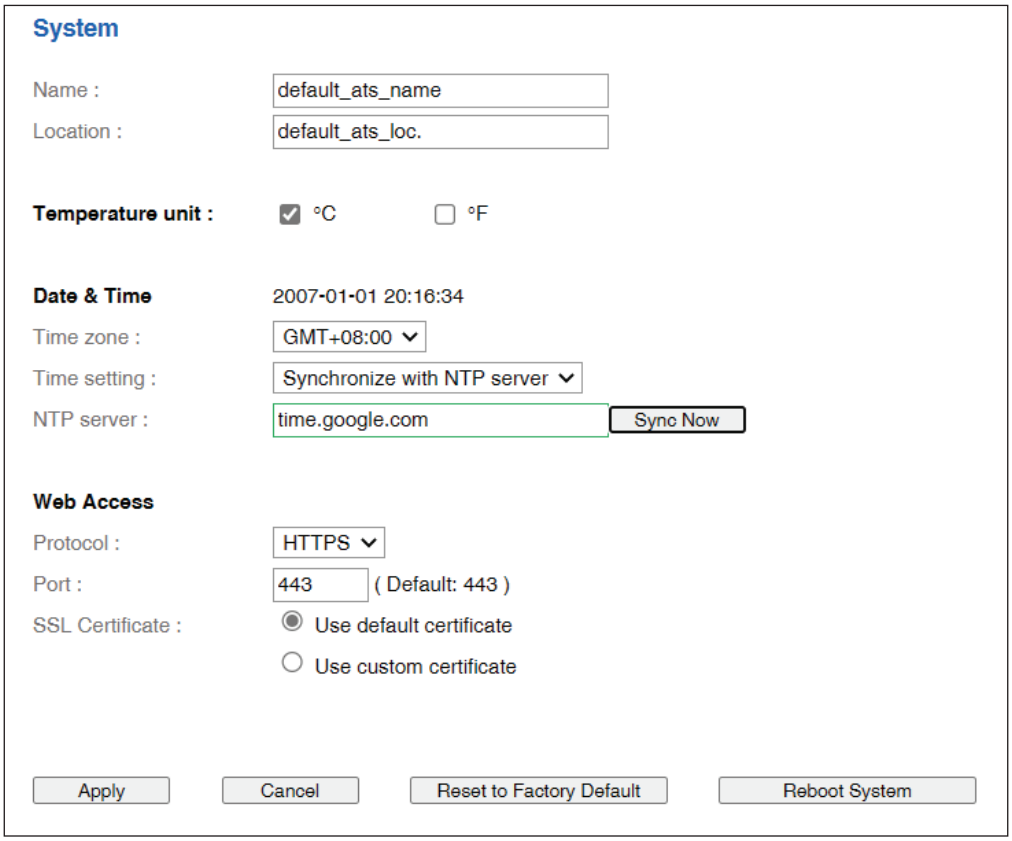


< 1.8 > System

In < **System** >,

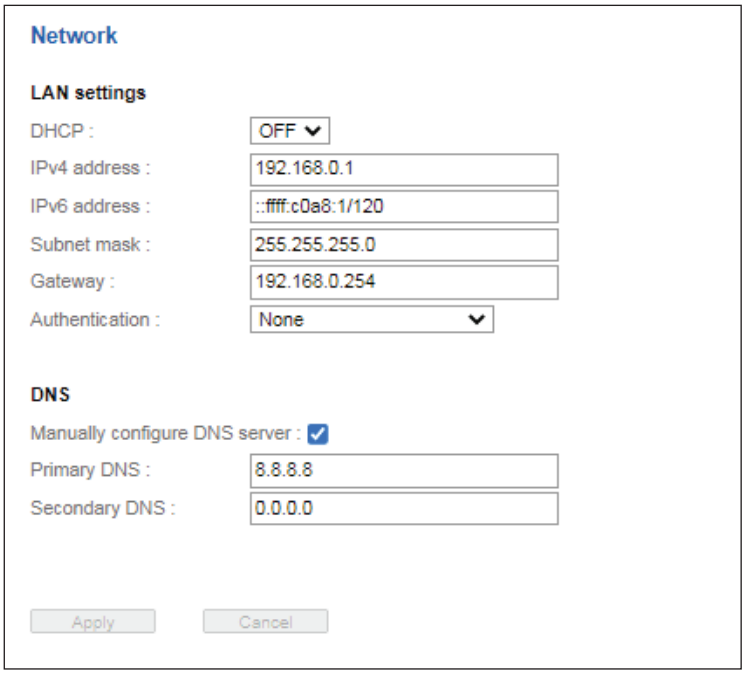
- Change the built-in IPD-03-S name & location
- Change temperature unit displayed in GUI
- Set “ **Date & Time** ” of the ATS (by “ **Manually** ” or “ **NTP server** ”). Default is “ **Manually** ”
- Click “ **Apply** “ to finish the above settings





< 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.



< 1.10 > DHCP Setting

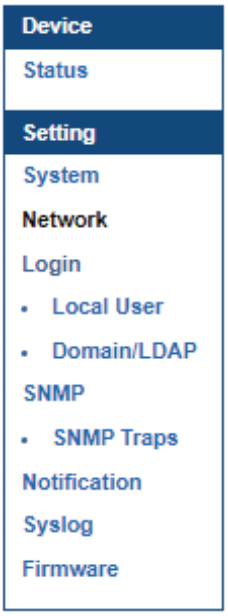
Step 1. Connect the Intelligent ATS to the computer (Please refer to < 1.6 > IP Configuration)

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

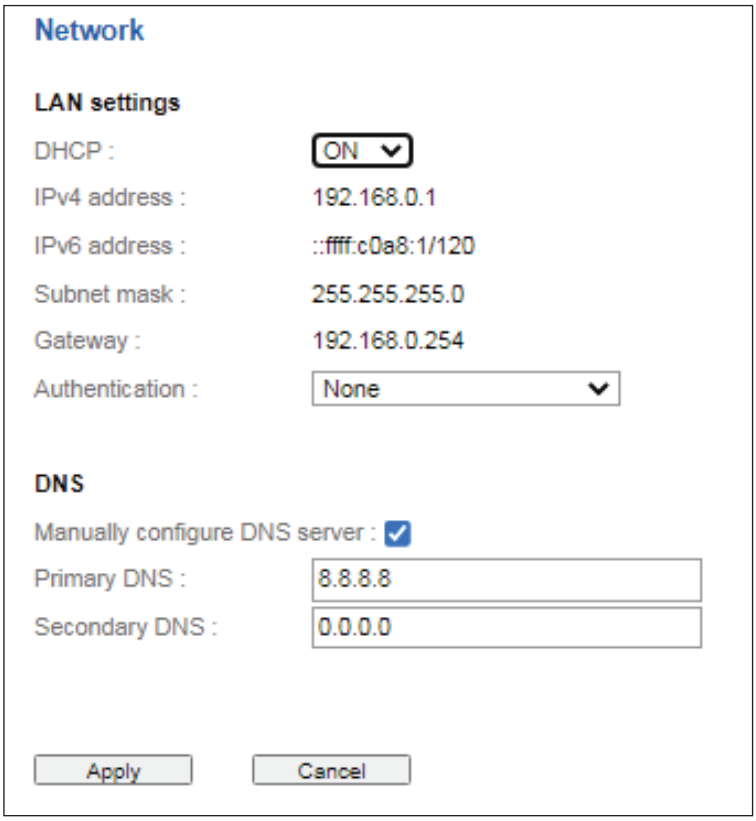
Step 3. Enter the configured ATS's IP address into the address bar
(Please refer to < 1.6 > IP configuration)

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

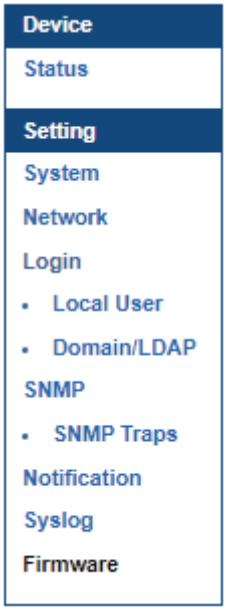


Step 6. Select " ON " from " **DHCP** " & Click " **Apply** " to save the settings.

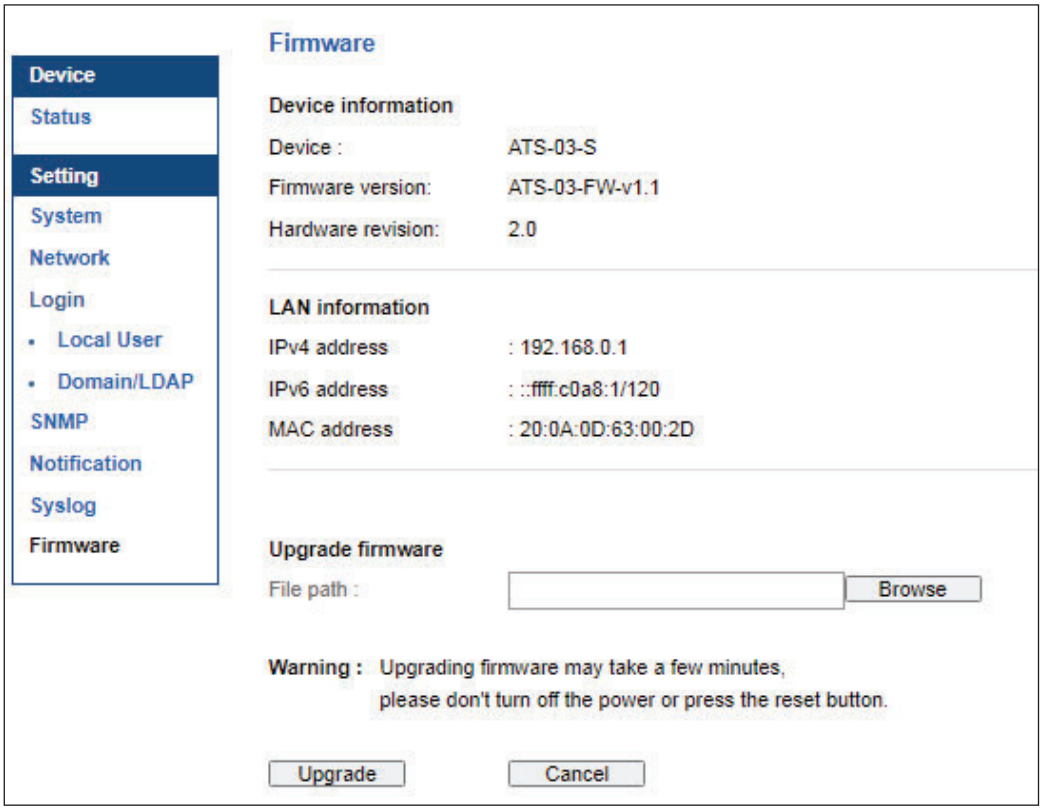


< 1.10 > DHCP Setting

Step 7. Select " **Firmware** " from the left navigation pane



Step 8. Record the " **Device MAC address** "



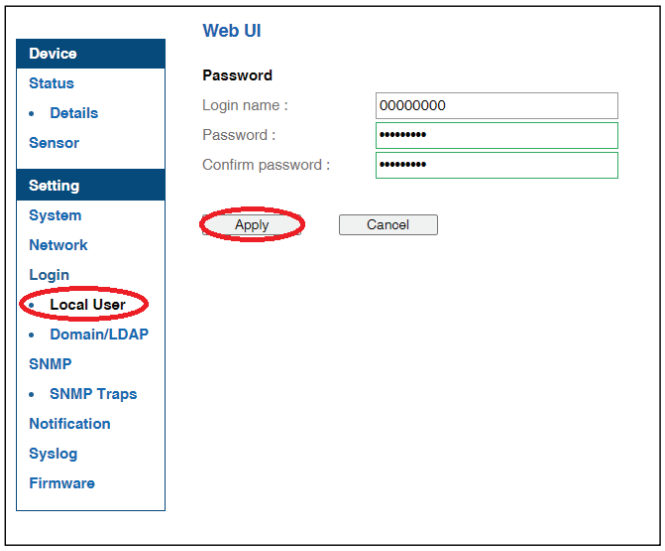
Step 9. Assign an IP address to the Intelligent ATS from your DHCP server.

< 1.11 > Login

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

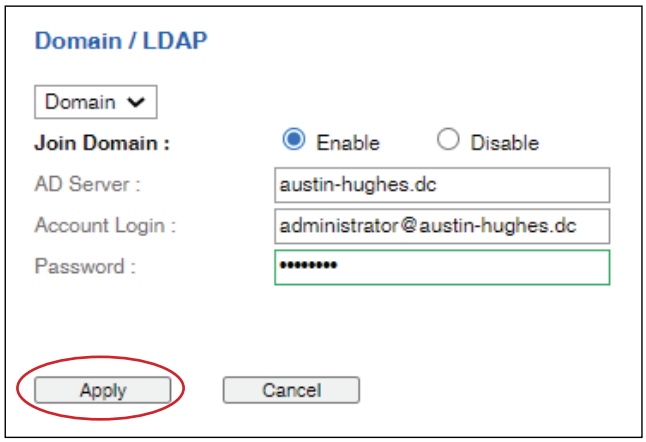
Local User :

- 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 :

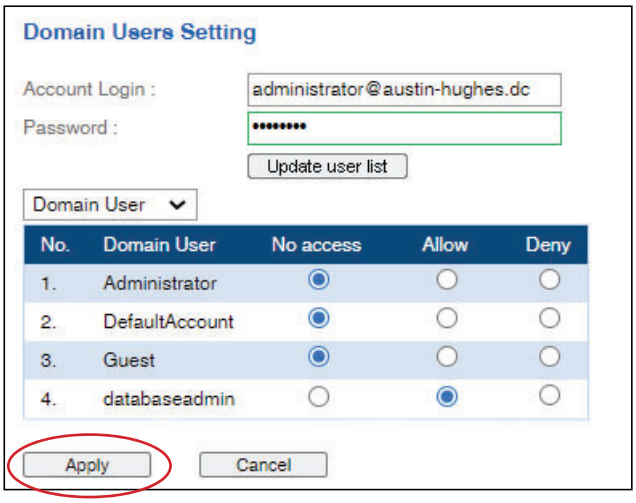
- Default Join Domain is **“ Disable “**
- Enable “ **Join Domain** ” only when you want to login the ATS WEBUI by AD server
- Enter “ **AD Server** ”,“ **Account Login** ” & “ **Password** ”
- Click “ **Apply** ” and “ **OK** “ on the pop up window to make changes effective
- You can now go to “ **Domain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



< 1.11 > Login

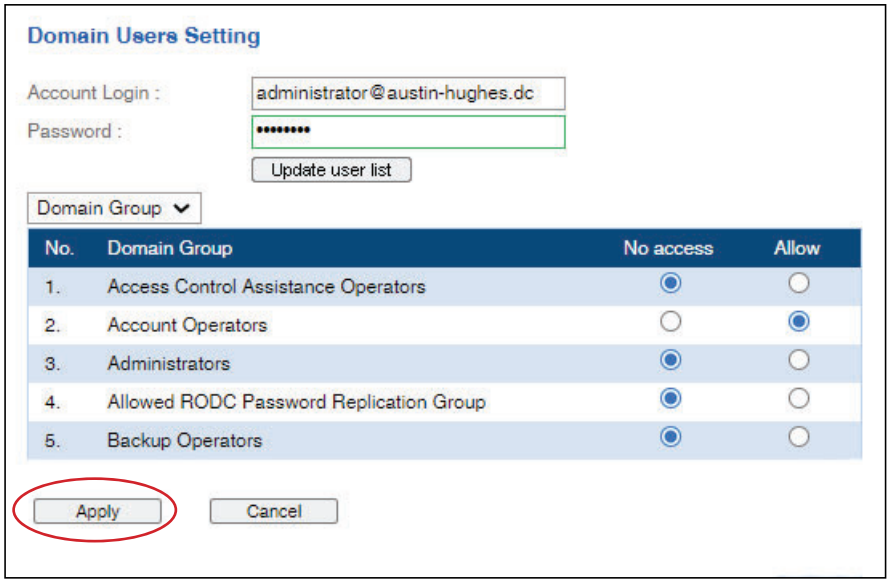
In " **Domain Users Setting** ",

- 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.



In " **Domain Users Setting** ",

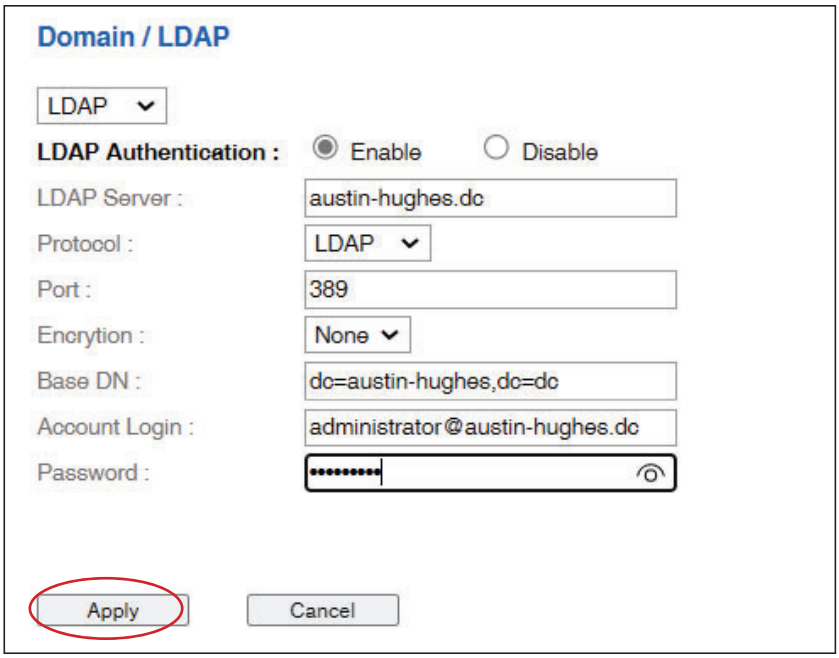
- Click **" Update domain data "** to update domain group list.
- Assign access right (No access / Allow) to **" Domain Group "** and click **" Apply " .**
- The Users of the Domain Group assigned **" Allow "** access right can login the ATS WEBUI.



< 1.11 > Login

Domain/LDAP :

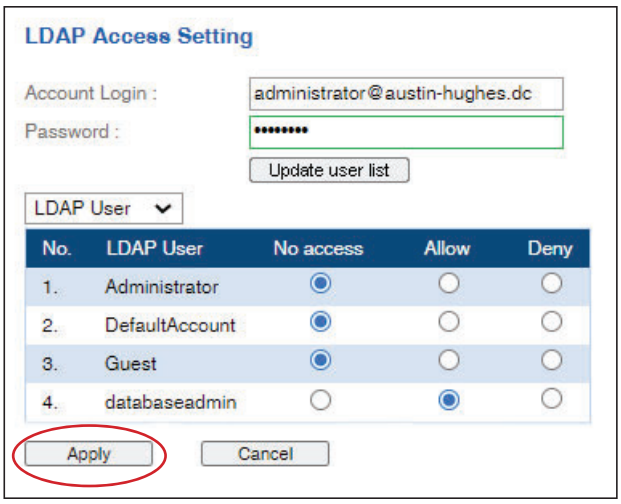
- Default LDAP Authentication is **“ Disable “**
- Enable **“ LDAP Authentication ”** only when you want to login the ATS WEBUI by LDAP server
- Enter “ **LDAP Server** ”,
- Select “ **Protocol** ”(LDAP / LDAPS). Default is **“ LDAP “**
- Enter **“ Port “**. Default is **“ 389 “**
- Select “ **Encrytion** ”(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 ”**



< 1.11 > Login

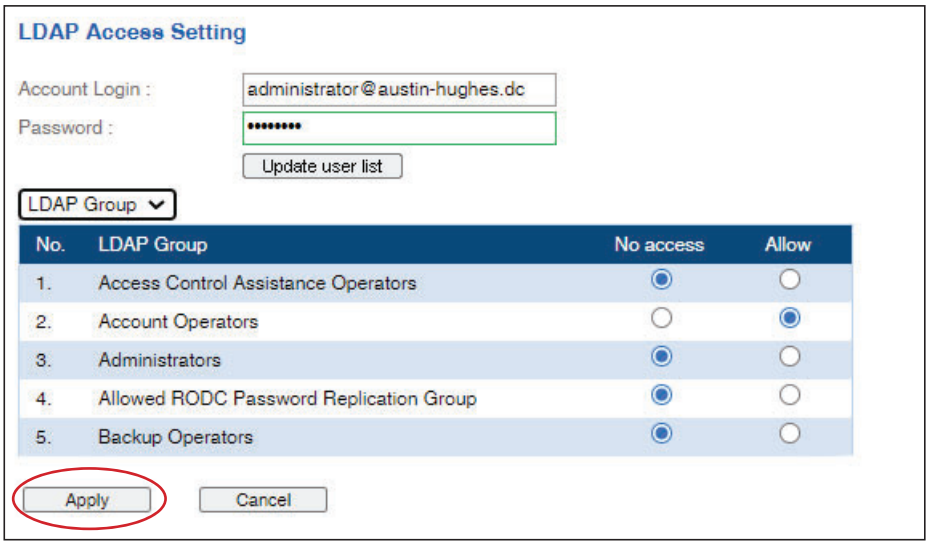
In “ **LDAP Access Setting** ”,

- 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.



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.



< 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.

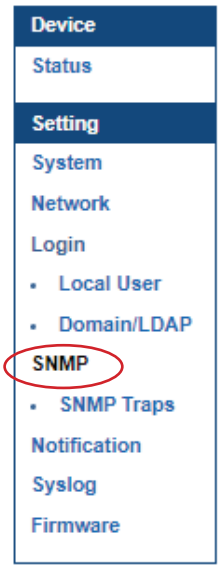
Step 1. Connect the ATS to a computer. (Please refer to < 1.6 > IP configuration)

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)

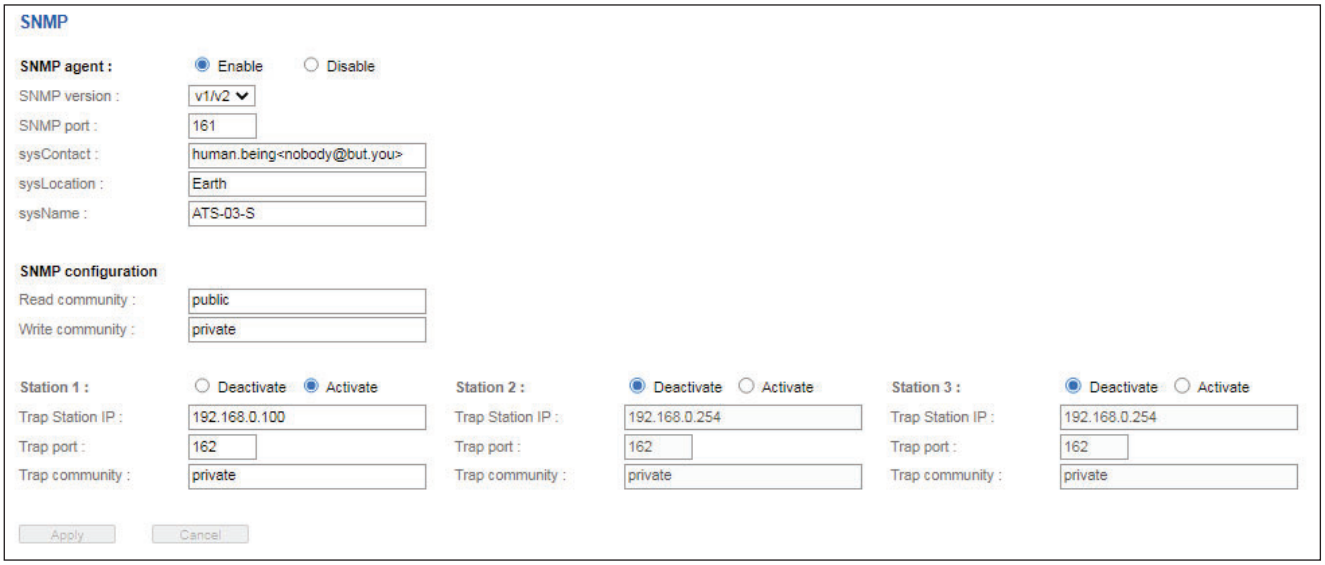
Step 4. Enter the " **Login name** " , " **Password** "
Default Login name : 00000000
Password: the one you set in Step 7 of < 1.6 > IP Configuration.

Step 5. Select the SNMP from the left navigation pane



< 1.12 > SNMP Setup

Step 6. The SNMP settings window appears as below :



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 fi nish the SNMP v1 / v2 settings

< 1.12 > SNMP Setup

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

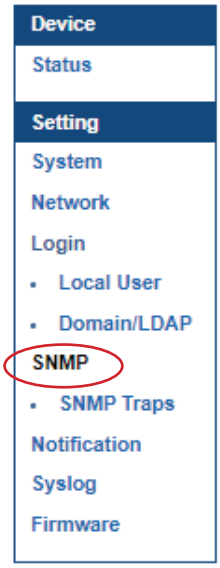
Step 1. Connect the ATS to a computer. (Please refer to < 1.6 > IP configuration)

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

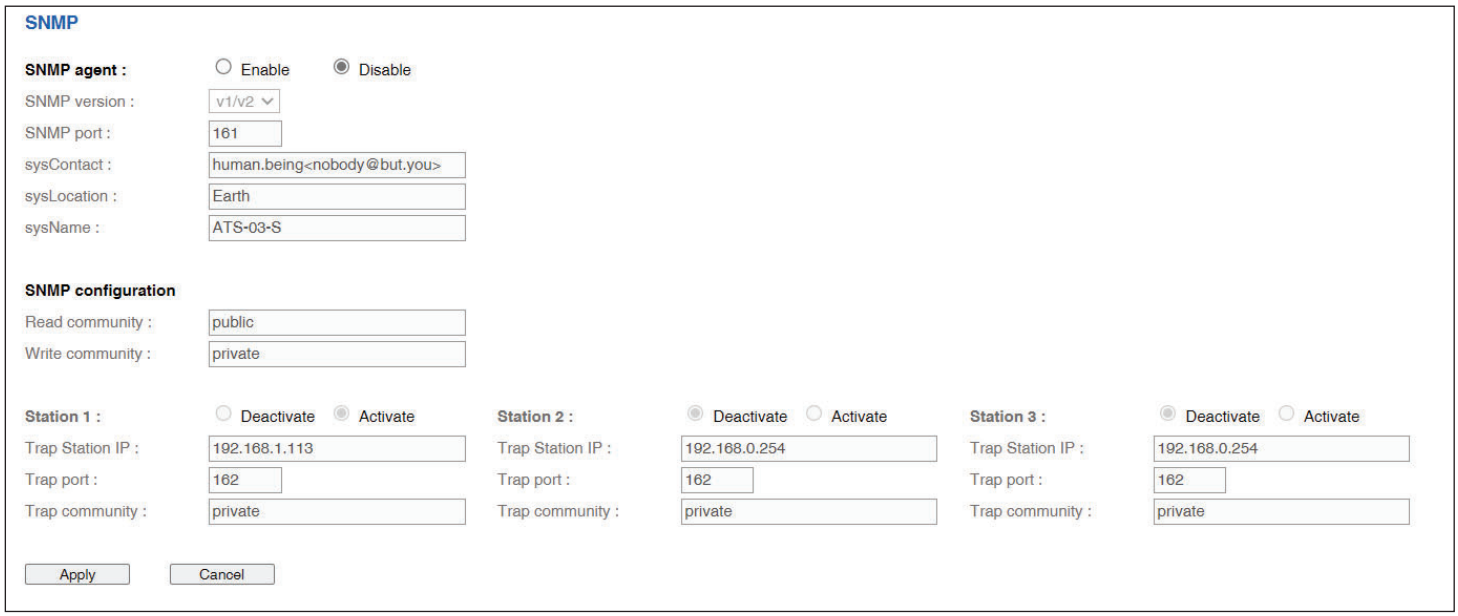
Step 3. Enter the configured ATS's address into the address bar
(Please refer to < 1.6 > IP configuration)

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



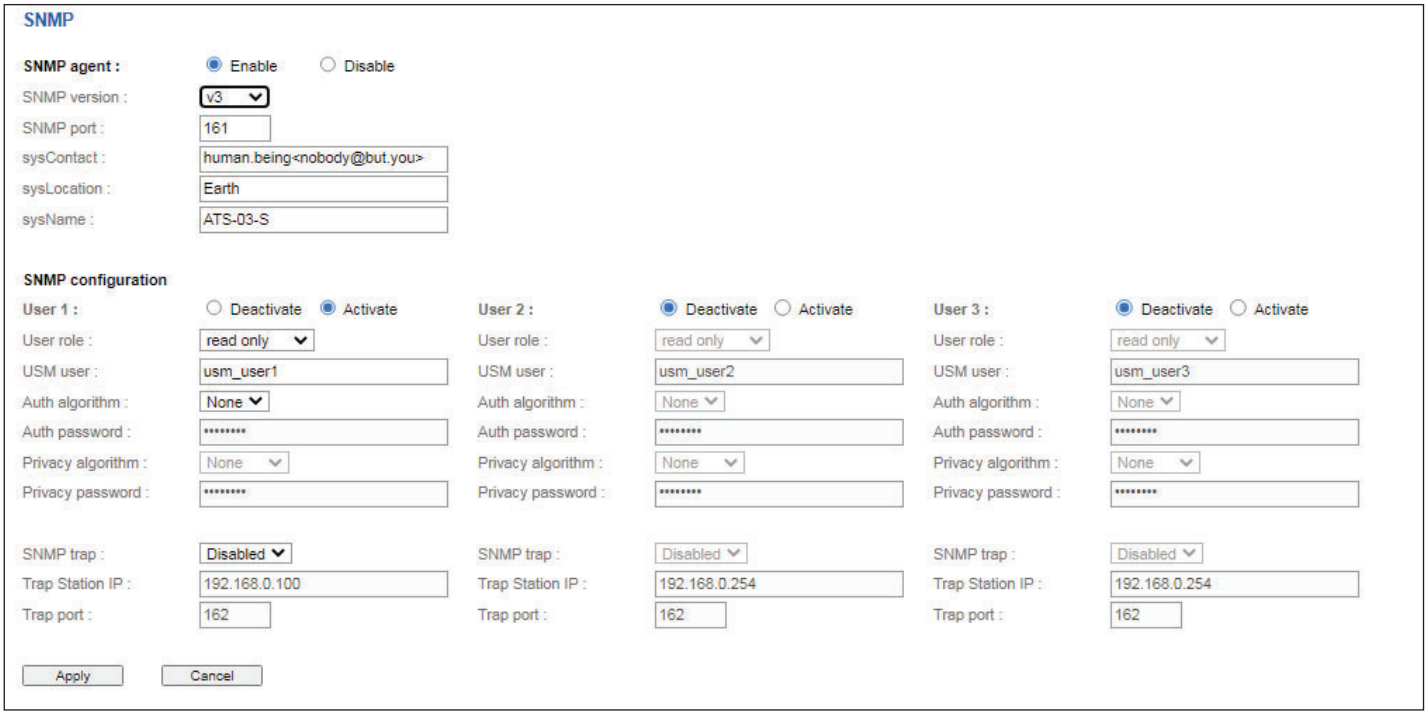
Step 6. The SNMP Settings window appears as below:



< 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 :



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 fi nish 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 SNMP authentication is enabled

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

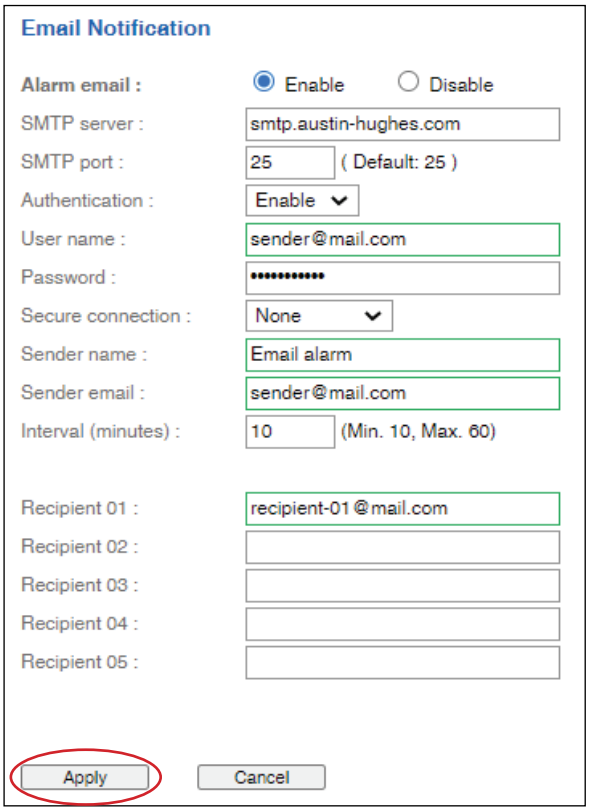
Step 6. Enter the **“ Sender Name ”** and **“ Sender Email ”**

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



< 1.14 > Syslog

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

Syslog 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)

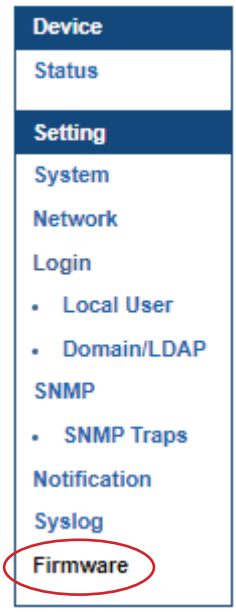
Step 3. Connect the intelligent ATS to the computer. (Please refer to < 1.6 > IP configuration)

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)

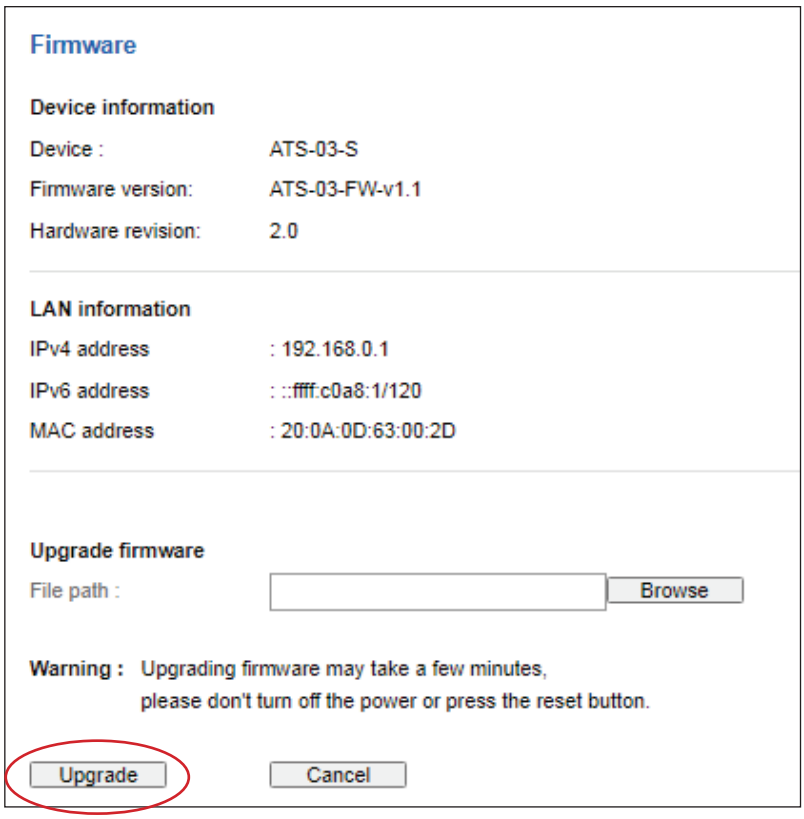
Step 6. Enter " **Login name** " & " **Password** ".
Default Login name : 00000000
Password: the one you set in Step 7 of < 1.6 > IP Configuration.

Step 7. Select the Firmware from the left navigation pane



< 1.15 > ATS Firmware Upgrade

Step 8. The firmware upgrade window appears as below :



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***

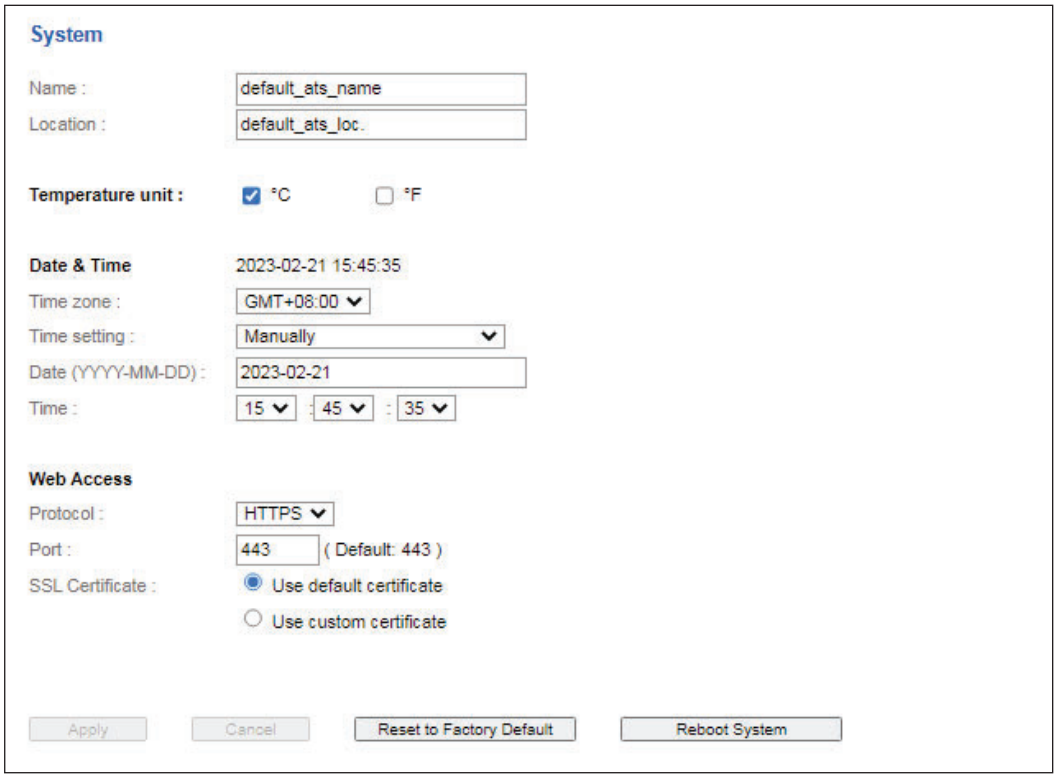
Step 3. Put ALL required files into a folder and COPY the folder to the TFTP root directory

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** "

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.



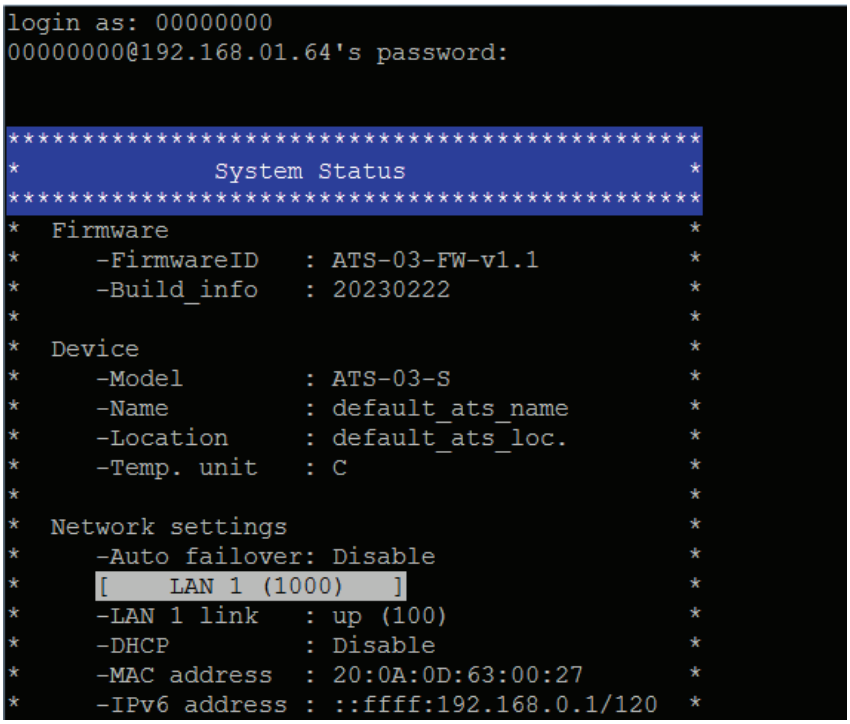
You must enable firmware upgrade via DHCP in SSH (default is ENABLED) and input the username and password for bulk firmware upgrade in the " **fwupdate.cfg** " file. You can change the username and password for bulk firmware upgrade via SSH. **See *Configuration of username / pass word for bulk firmware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

< 1.16 > Bulk Firmware Upgrade

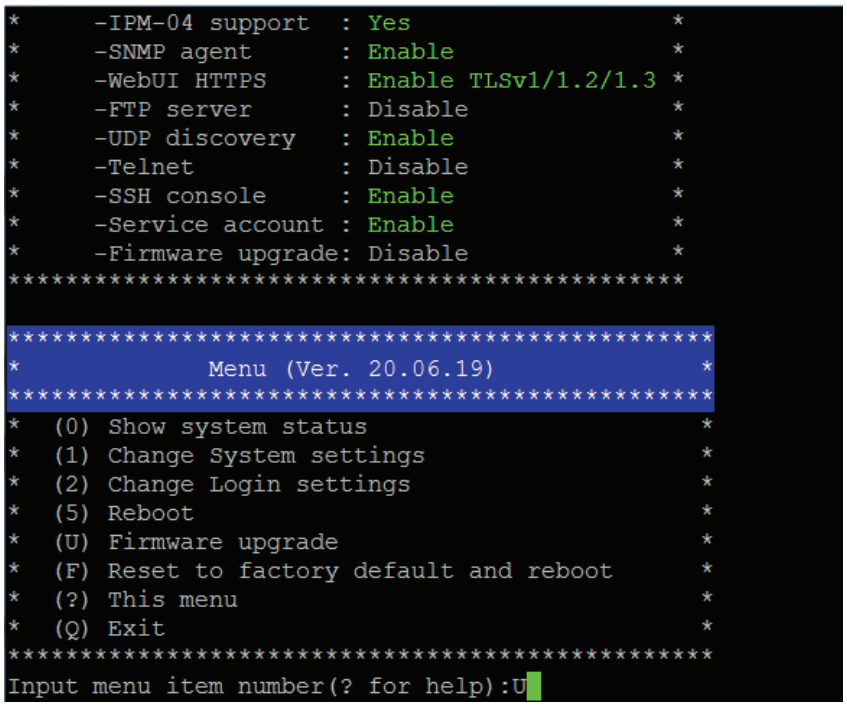
Configuration of username / password for bulk firmware upgrade

Step 1. Access the SSH using putty

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

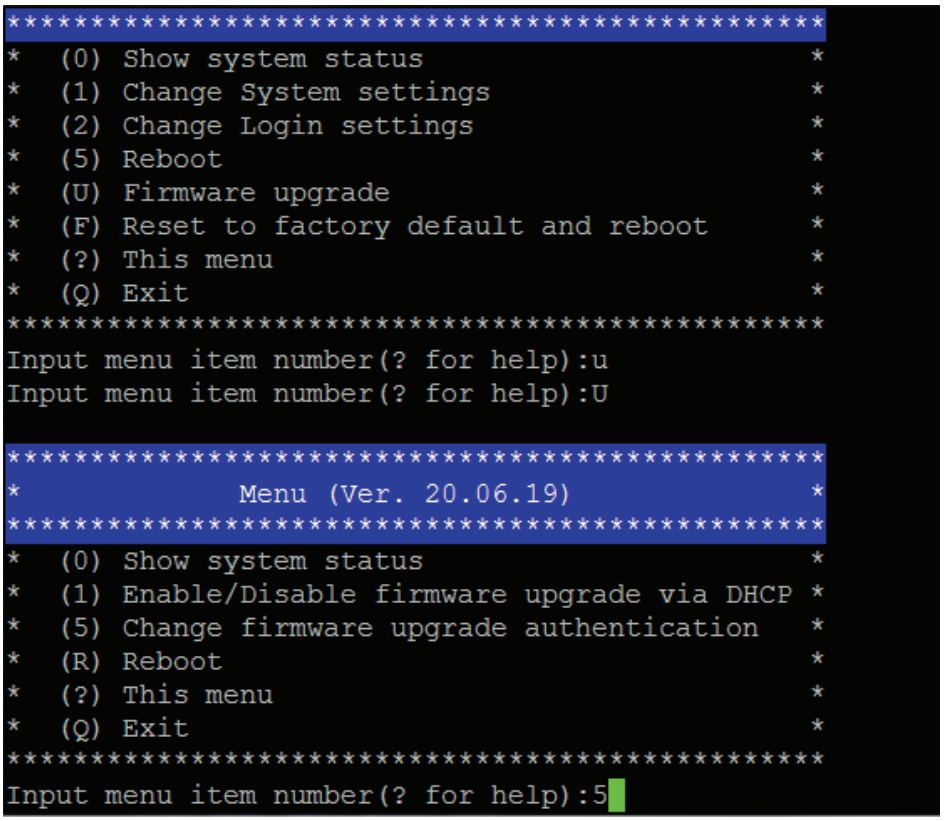


Step 3. Select " **(U) Firmware upgrade** " and " **Enter** "

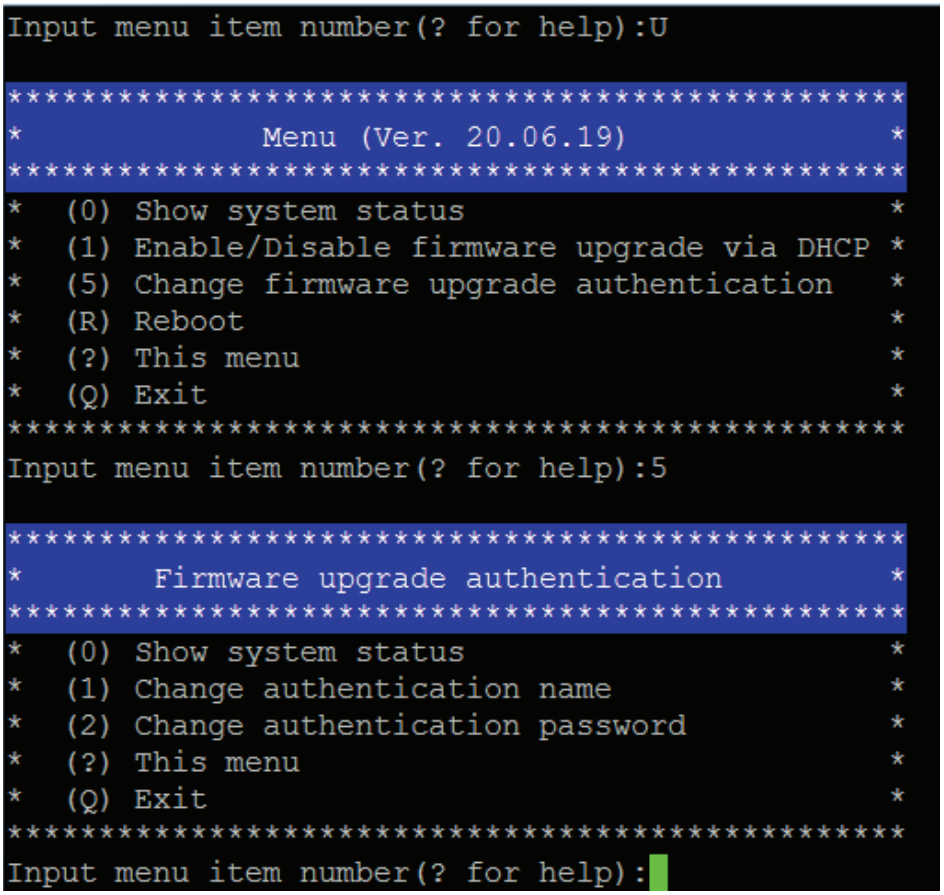


< 1.16 > Bulk Firmware Upgrade

Step 4. Select " **(5) Change firmware upgrade authentication** " and " **Enter** "



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



< 1.16 > Bulk Firmware Upgrade

< TFTP Requirements >

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

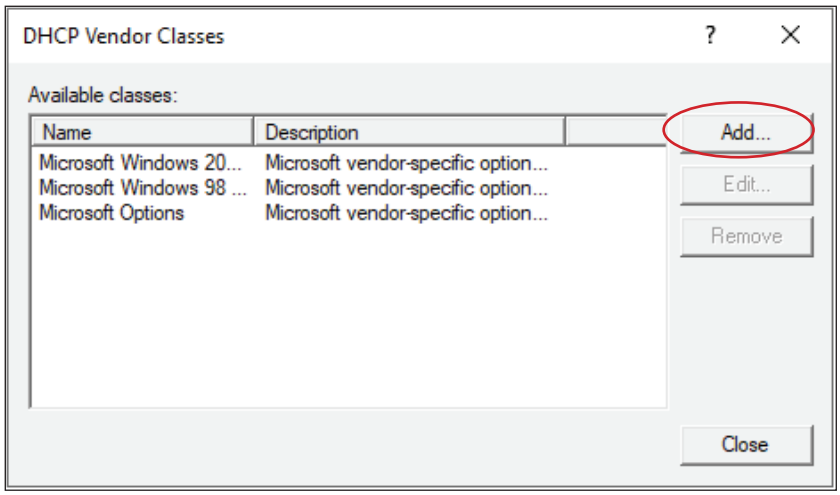
- Able to work with IPv4
- A folder containing all required files is available in the TFTP root directory. The folder name MUST be the same as the String value of the Magic code. Details please refer to DHCP IPv4 Configuration in Winodws
- The TFTP server supports the write operation including file creation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

< DHCP IPv4 Configuration in Windows >

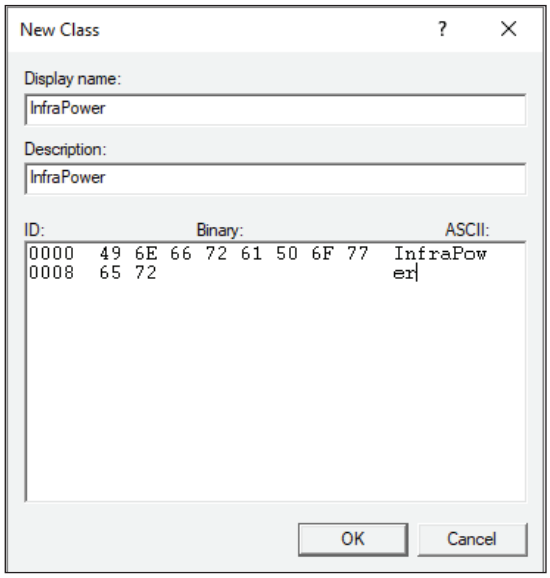
Please follow the procedures below to configure your DHCP server. The illustration below is based on Microsoft Windows Server 2019

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.

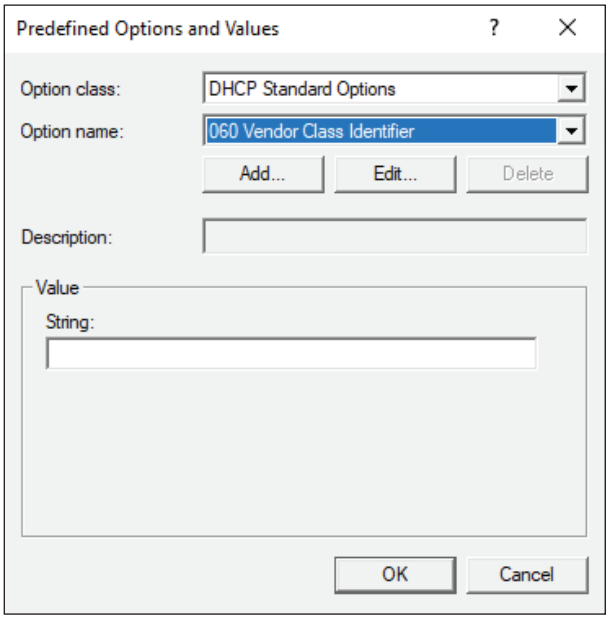


- Specify a unique name for this vendor class and type the binary codes of " **InfraPower** " in the New Class dialog. The vendor class is named " **InfraPower** " in this illustration.



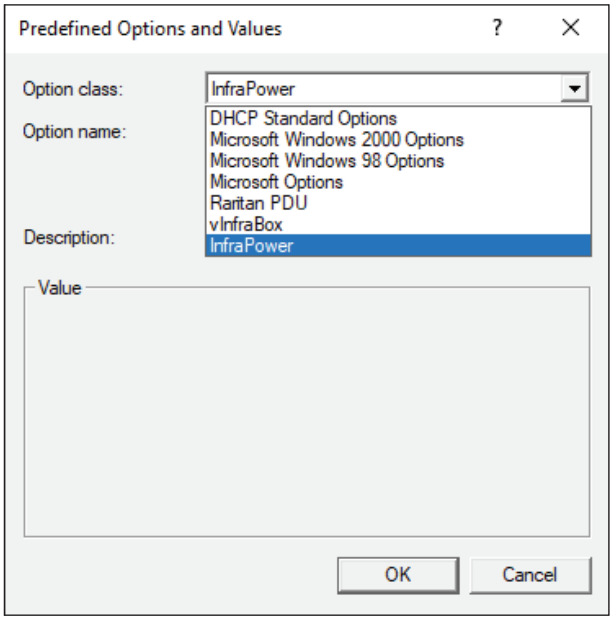
Step 2. Define one DHCP standard option – Vendor Class Identifier

- 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.

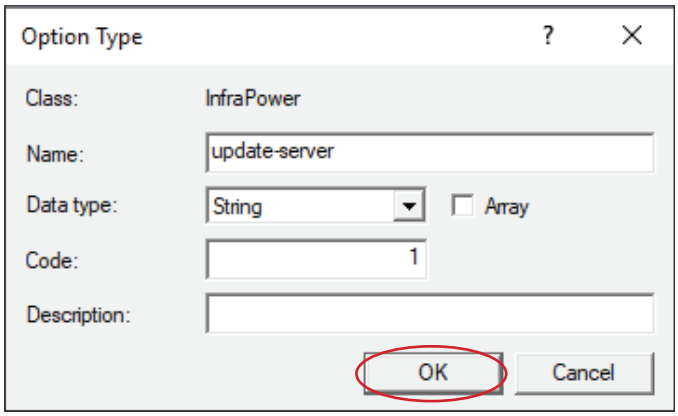


Step 3. Add four options to the new vendor class " **InfraPower** " in the same dialog. The fourth option is an optional item if the UDP port you set for the TFTP server is NOT 69.

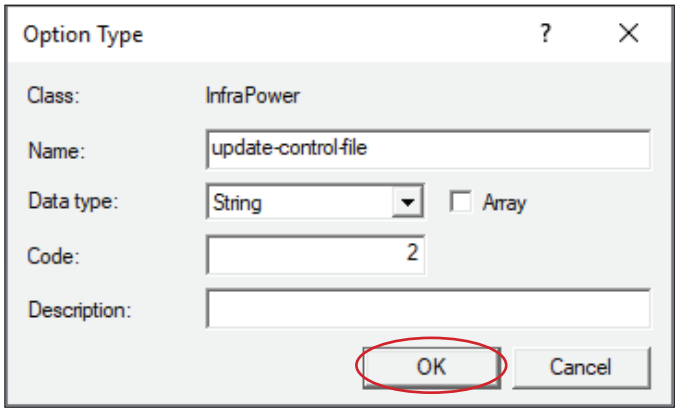
- Select " **InfraPower** " in the " **Option class** " field.



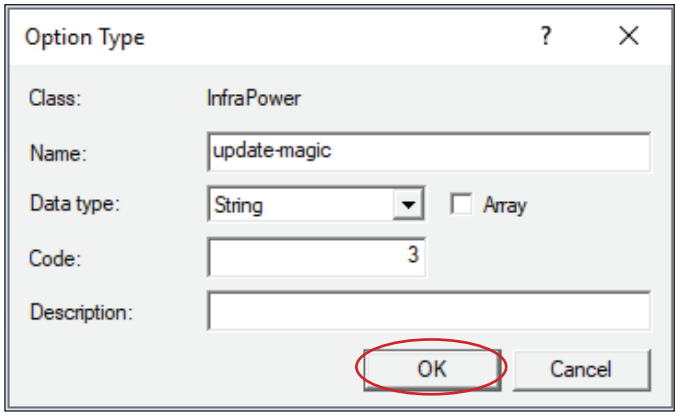
- Click “ **Add** “ to add the first option. Type “ **update-server** ” in the Name field, select String as the data type, and type 1 in the Code field and Click “ **OK** “.



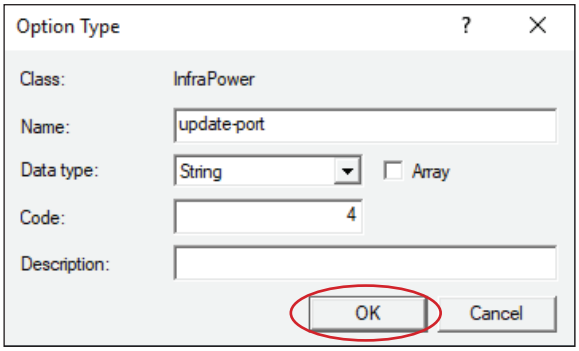
- Click “ **Add** “ to add the second option. Type “ **update-control-file** ” in the Name field, select String as the data type, and type 2 in the Code field and Click “ **OK** “.



- 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** “.



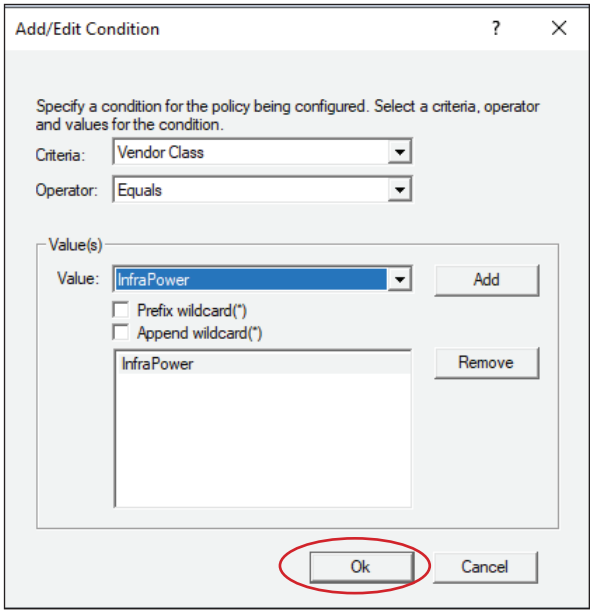
- Click “ **Add** “ to add the fourth option. Type “ **update-port** ” in the Name field, select String as the data type, and type 4 in the Code field and Click “ **OK** “.



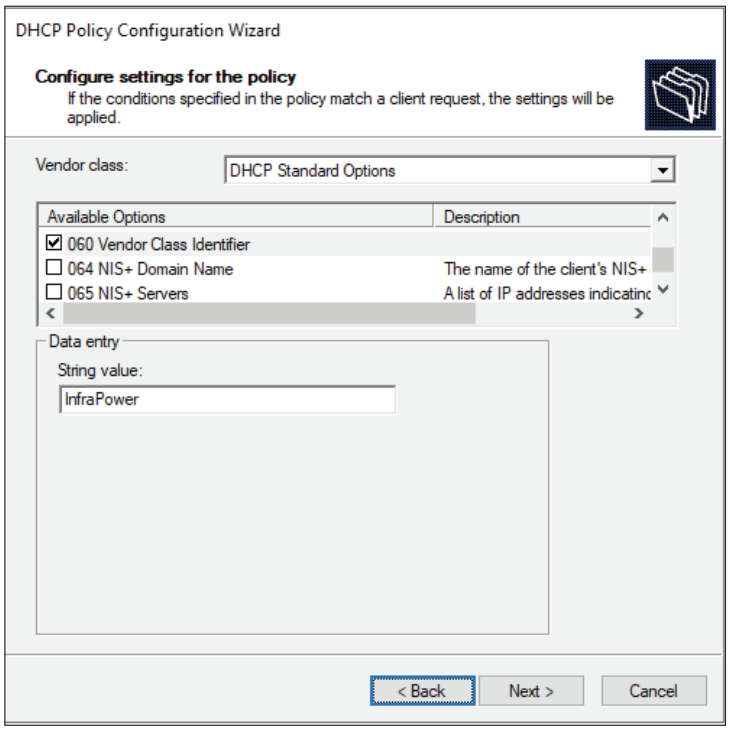
Step 4. Create a new policy associated with the “ **InfraPower** ” vendor class.

- 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.

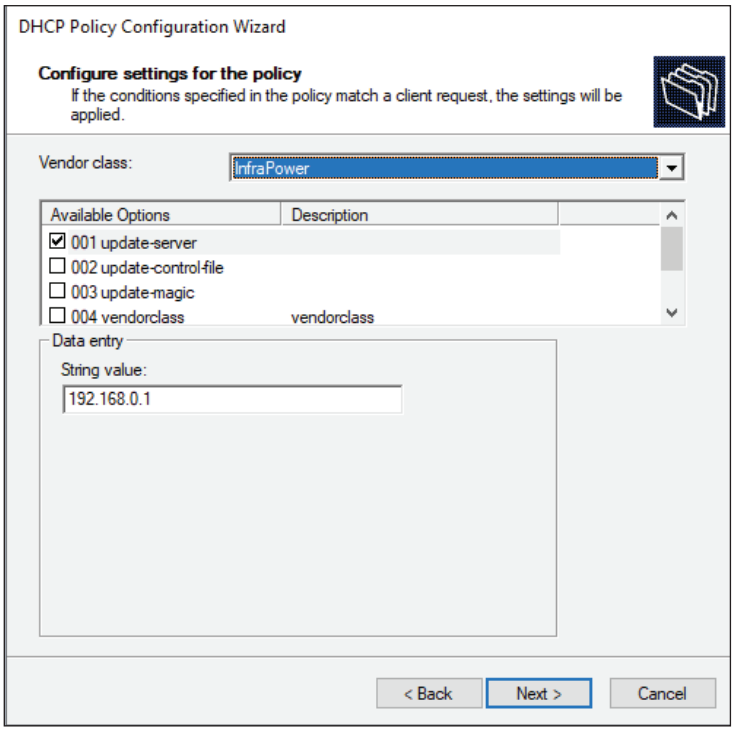
- Click “ **Add** “ to add a new condition
- Select the vendor class “ **InfraPower** ” in the Value field, click “ **Add** “ and then “ **OK** “.



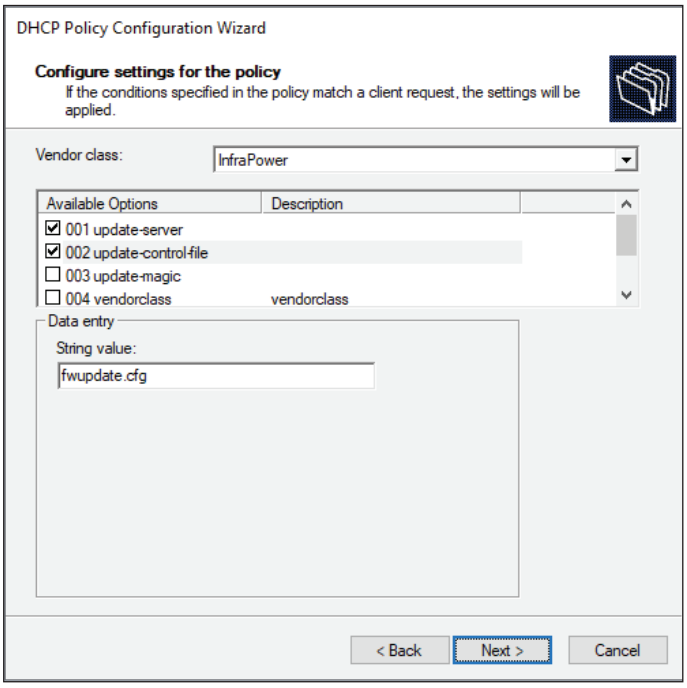
- Click “ **Next** “.
- Select “ **DHCP Standard Options** “ in the “ **Vendor class** ” field, select “ **060 Vendor Class Identifier** ” from the Available Options list, and type “ **InfraPower** ” in the “ **String value** ” field.



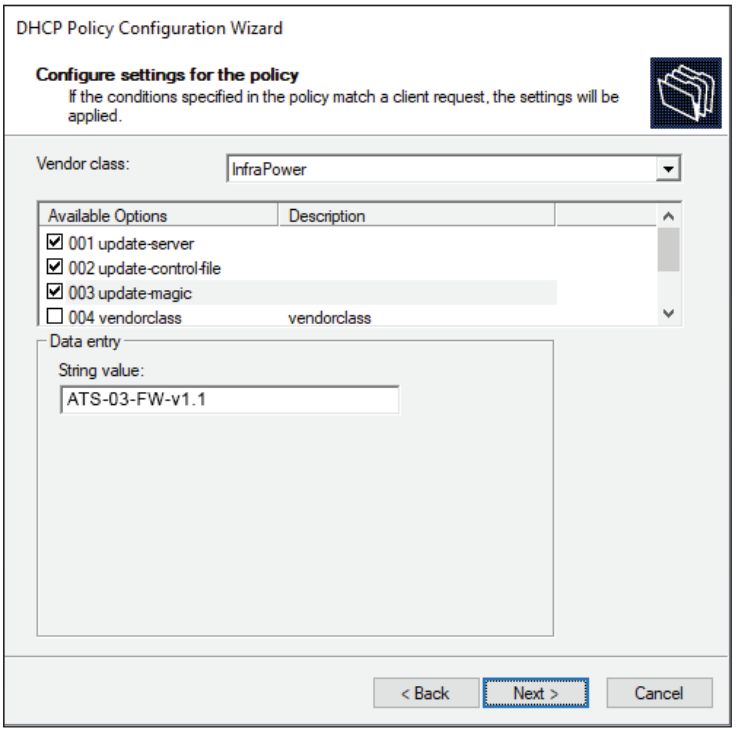
- Select the “ **InfraPower** ” in the “ **Vendor class** ” field, select ” **001 update-server** ” from the Available Options list, and type your TFTP server’s IPv4 address in the “ **String value** ” field.



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

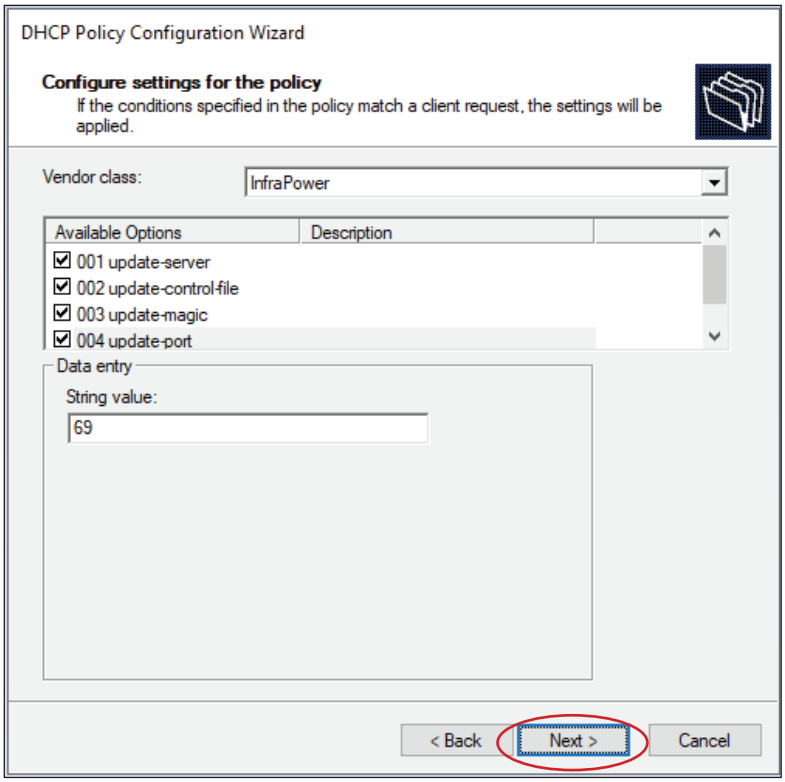


- Select “ **003 update-magic** ” from the Available Options list, and type folder name of the files you stored in the root directory of the TFTP server in the “ **String value** ” field. This String value is the magic code to prevent the fwupdate.cfg commands from being executed repeatedly.



The 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.

- 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.



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

< 1.16 > Bulk Firmware Upgrade

Description of Devices.csv

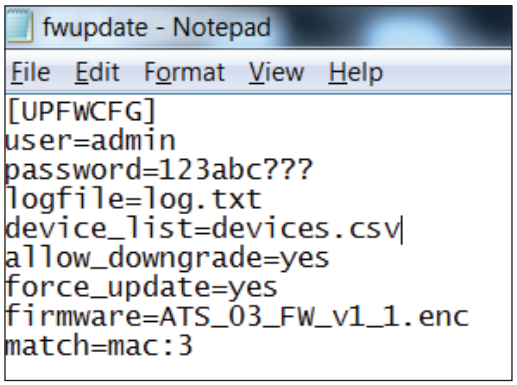
	A	B	C	D	E
1	1	1	20:0A:0D:FF:CA:BF	192.168.0.123	192.168.0.1
2	1	1	20:0A:0D:FF:3C:E6	192.168.0.122	192.168.0.1
3	#--keep this be the last line of this file--				
4					
5					

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



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.

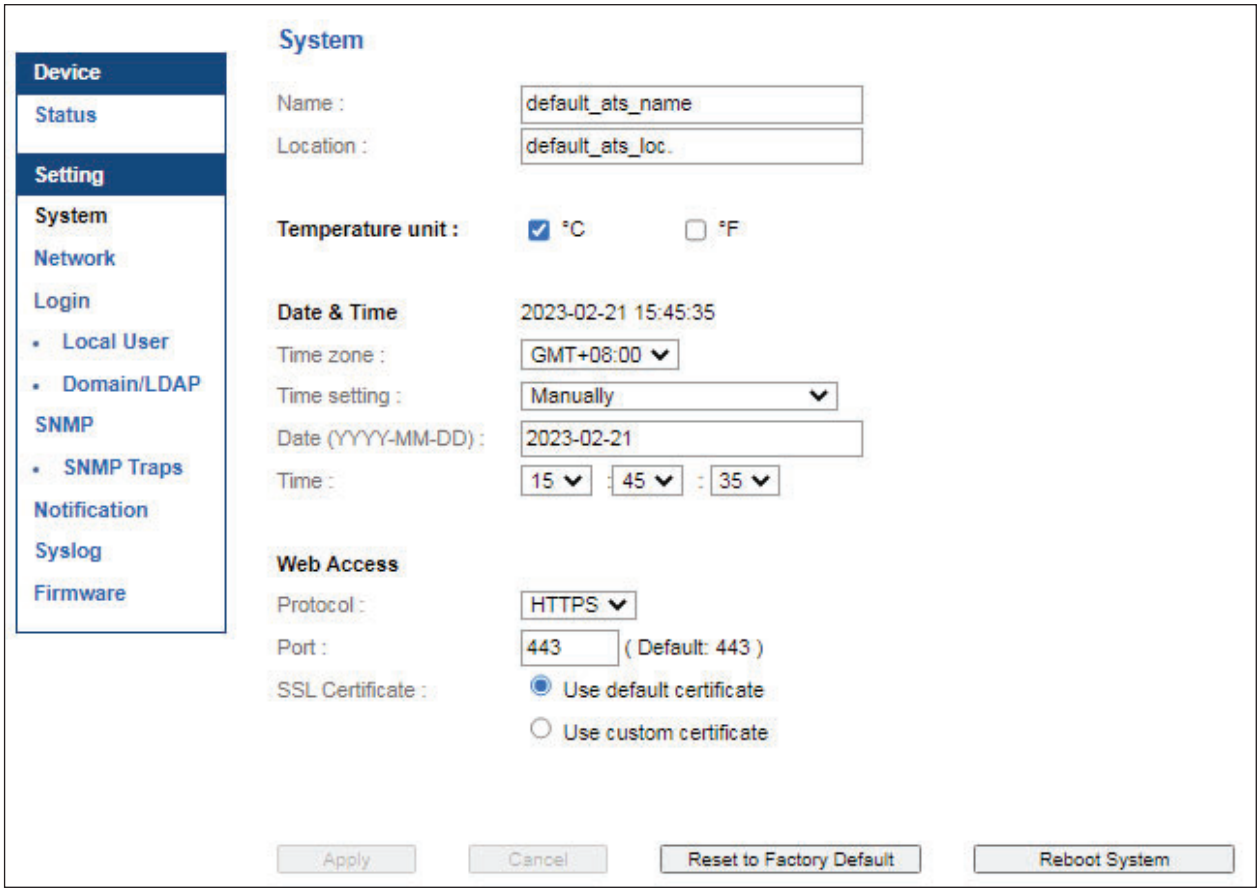
< 1.17 > 802.1X authentication

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.

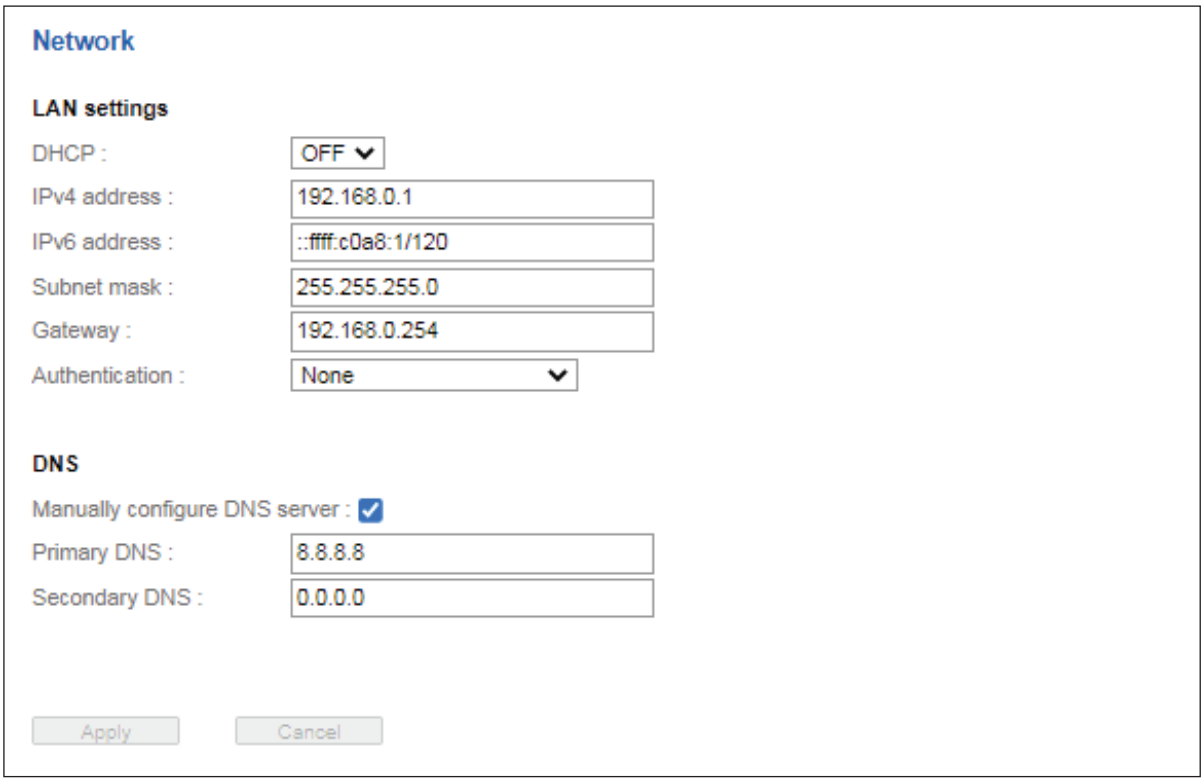
Before configure the 802.1X authentication, ensure the system clock of the Intelligent ATS is set up properly. Otherwise, the authentication will fail while the RADIUS server verifies the validity of the certificate. You can go the System page to set up the date and time of the Intelligent ATS.



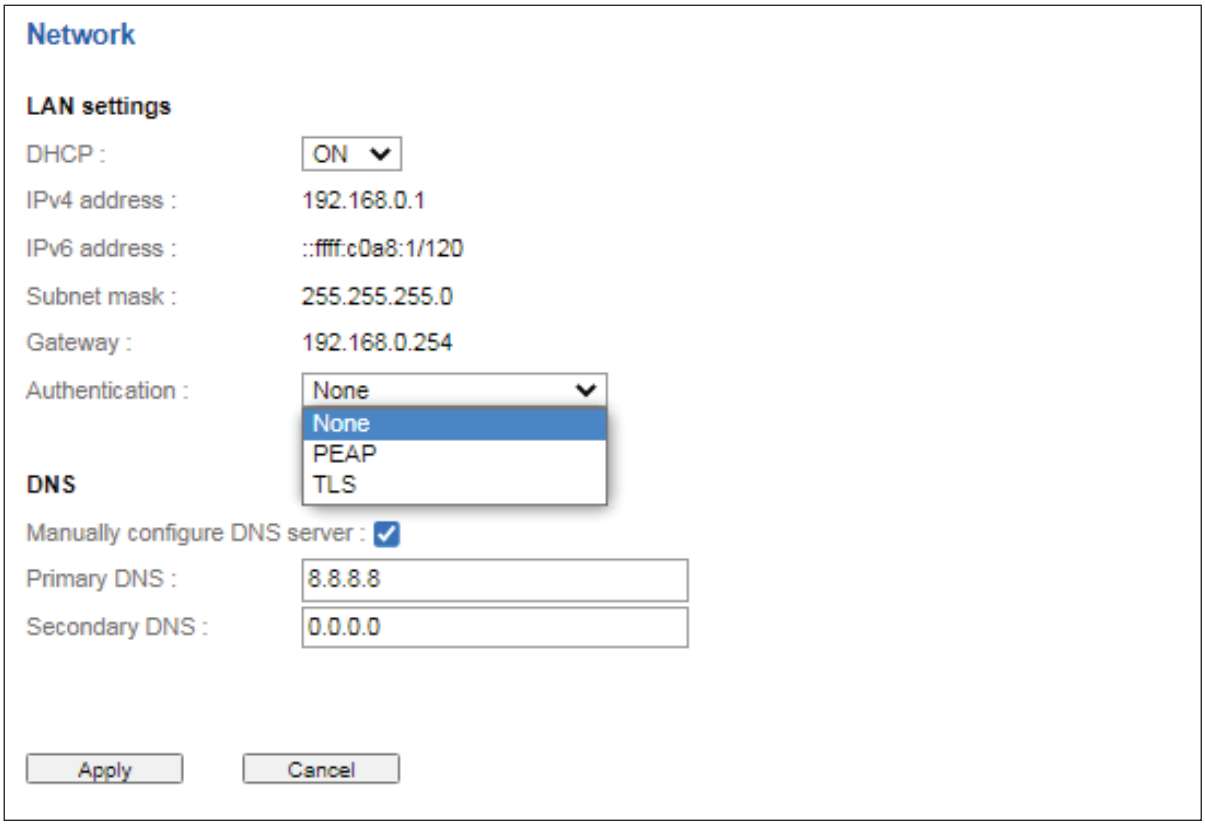
< 1.17 > 802.1X authentication

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.

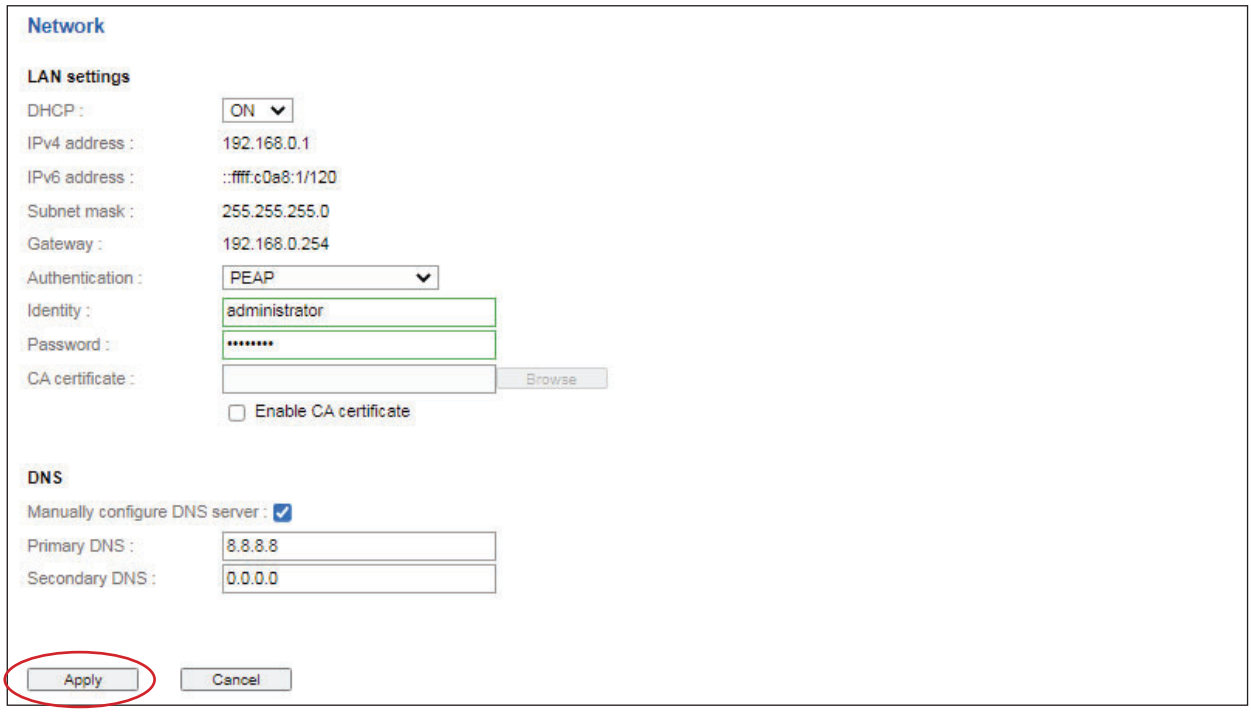


Step 2. Click the Authentication pull down menu and you will see the authentication method.



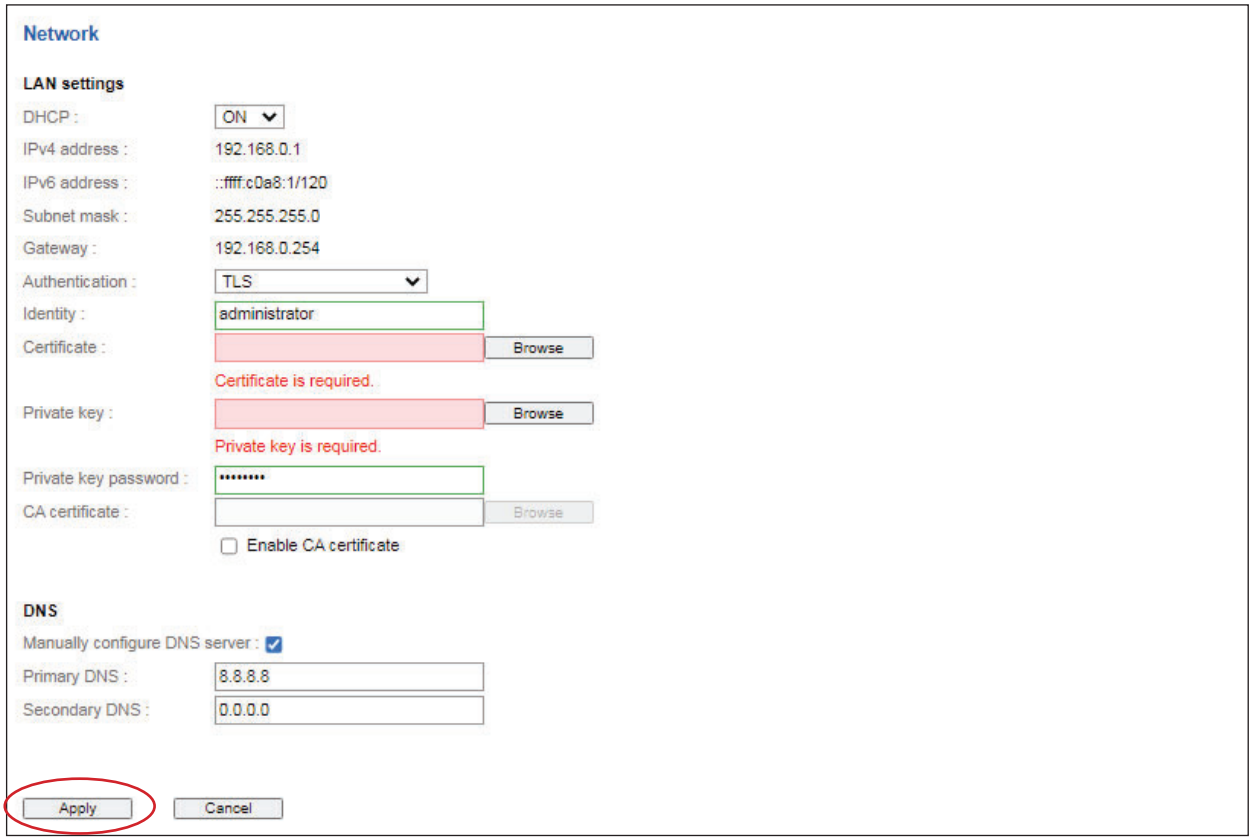
Step 3. To use PEAP as authentication method, select PEAP. Then input the " **Identity** ", " **Password** " and " **CA certificate** " in PEM format. You can uncheck " **Enable CA certificate** " to bypass the authentication using CA certificate.

Click " **Apply** " to save the configuration.



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.



< 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).