SURGEX® | AMETEK®
ELECTRONIC SYSTEMS PROTECTION

AXESS Ready
FLATPAK™

SA-82-AR

Hardware Installation Guide

**FIRMWARE VERSION: 1.10.169**

SOFTWARE VERSION: 1.30.11

Table of Contents

I.   Introduction

The SurgeX® SA-82-AR is a network attached, IP addressed, web controlled AC surge protector and power conditioner. The SA-82-AR may be used to switch up to 8A at 120V. The simple web server structure allows basic control of two outlets. The extensive programming and setup capabilities are accessed by a web browser, through a Device Management Utility (DMU), or through a Command Line Interface (CLI).

- The SA-82-AR features SurgeX® Series Mode® surge protection, Impedance Tolerant EMI/RFI filtering and Over-Voltage Shutdown.

- Remote reboot any device: monitors, routers, servers, kiosks, etc. The remote device need not be network attached.

- Conserve energy by powering down equipment when not in use.

- Telnet access uses the Command Line Interface (CLI) structure and syntax to completely configure and control the SA-82-AR. This Axess Ready (AR) device also supports the DxP protocol, which allows software developers to integrate the unit into custom applications.

- Up to 2 systems can be continuously monitored with AutoPing,with automatic power control upon loss of contact. Reboot crashed systems, or provide auto power-up or - down for environmental controls and notification systems.

- The SA-82-AR utilizes 2 levels of password security, with only the administrative account having access to setup and configuration.
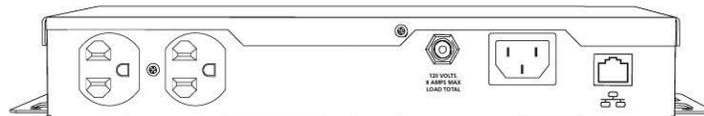
Located on the rear panel are the input IEC power plug, network connection (RJ-45), 8A circuit breaker, and output receptacles.
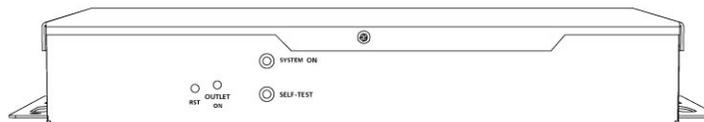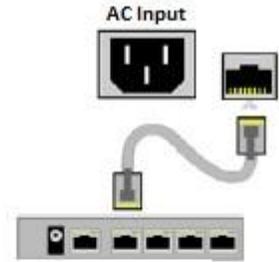
The front panel contains the Outlet On LED, Self-Test LED, System On LED, and Reset button.

II. Installation

1. **Ethernet Connection**

The RJ45 connector for 10/100 Ethernet is situated on the rear panel beside the input power plug. The default IP Address is
DHCP Assigned.

2. **AC Power Connections**

Connect the device to be powered On and Off to the output duplex receptacle.

Ensure that the total combined load of all controlled devices does not exceed 8 Amps.

Connect one end of the supplied power cord to the connector labeled "AC Input", and the other end to a properly grounded AC outlet.
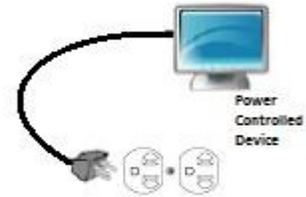
3. **LED Indicators**

The green Self-Test LED indicates that the internal surge protection circuitry is fully functional. The red Outlet On LED indicates that power is being supplied to the two receptacles.

The red System On LED indicates that the Axess system is On. This indicator will turn off if the AC voltage rises above 145V, and AC power will be removed from the output receptacles in order to protect connected equipment. When the AC voltage returns to below 135V, power will automatically be restored to the output receptacles and the System On LED will turn on.
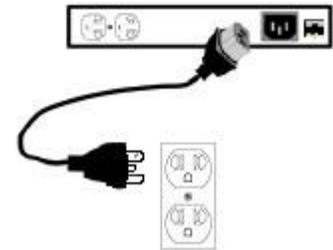
III. Initial Set-Up

1. **Device Management Utility (DMU)**

The SurgeX Device Management Utility (DMU) provides the easiest means to find and configure your AR for use. The DMU can:

1. Automatically discover multiple ARs on a local network.
2. Display the current IP address of each AR.
3. Allow the setting of a new IP address for each AR.
4. Perform firmware upgrades.
5. Return an AR to Factory Defaults.

The SurgeX Device Management Utility is available on the AR CD or on the SurgeX website at **http://www.espsurgex.com**

Note: The IP address can only be set within the first 2 minutes after powering up the AR. The utility will only work with ARs on the same local subnet as the PC.

Device

Discover: Automatically discover all ARs on the local network. The DMU will display the location name of the AR, the product ID and version number, the current IP address, and the MAC address. Factory defaulted ARs will display with the name **Axess Ready** and have an IP address that was automatically assigned by the DHCP server on your network.

- The IP address field also indicates the port for web access that is currently in use by the AR. The standard port for web browser accessibility is factory default Port 80.

Add: Manually add an AR by IP address.

Clear: Clear the list.
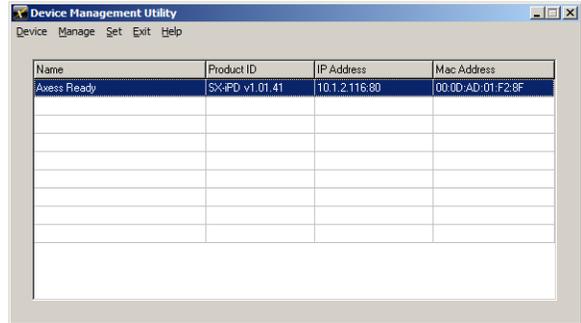
DMU automatically discovers devices on the local network.
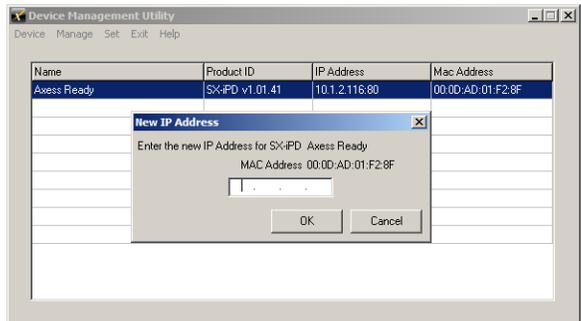
Enter new IP address for selected Axess Ready.
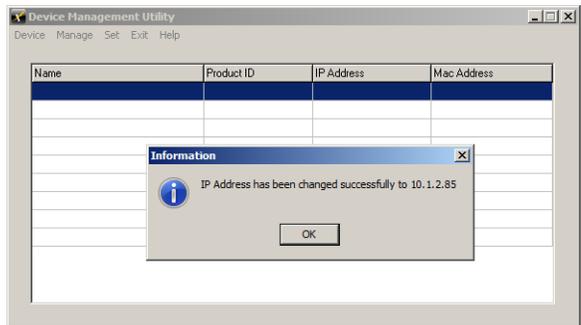
IP address successfully set.

Manage

Open Browser: Opens the web browser interface for the selected AR.

Upgrade Firmware: Starts the Firmware Upgrade dialogue. Firmware Upgrade requirements:
- Valid firmware file.
- Administrative login credentials.
- "Upgrade Enable" must be set to yes, set via web page or CLI.

Set

IP Address: Changes the IP address of the selected AR.

Factory Defaults: Return the selected AR to a Factory Default state. This action must be performed within the first 2 minutes after powering up the unit.

Local Address: Select the IP address to Discover on. This may be necessary for computers with multiple network connections.

Exit

Exits the DMU program.

Help

Online Help: Opens a web browser to online help resources.

About: Displays DMU version information.

2.   **Setting the IP Address**

ARs are configured with a DHCP assigned factory default IP address.

To set the AR's IP address using one of the following methods, the computer and AR must be on the same local network.

DMU: Follow the steps in the preceding subsection to set the IP address using the Device Management Utility (DMU).

CLI: These are the basic commands to set the network parameters. After setting these parameters, the AR will need to be rebooted for the settings to take effect. Any command that requires rebooting of the AR will provide a prompt to do so. All commands may be entered as required before rebooting. Manually specifying the IP address via CLI automatically sets the address as static.

Example: Telnet to IP address of **192.168.1.254** on default Port **23**:

```
SurgeX Axess Ready v1.01.41
User> admin
Password> *****

Axess Ready> set ipaddress 10.1.2.69

Ok
Axess Ready Reboot Required> set subnet 255.255.255.0

Ok
Axess Ready Reboot Required> set gateway 10.1.2.1

Ok
Axess Ready Reboot Required> reboot
```

The CLI command **set ipmode dhcp** followed by a **reboot** command may be used to configure the AR to automatically acquire its network settings from a DHCP server. A DHCP server will automatically assign an IP address (dynamic address), as well as the Subnet Mask and Gateway.

To determine what IP address has been automatically assigned by the DHCP server, you will need to use the Discover feature of the DMU or query your DHCP server and locate the MAC address of the AR in the DHCP server's IP/MAC table.

Web: To set the IP address using a web browser, navigate to the current IP address of the AR. Enter the administrator credentials (Factory Default User: **admin**, Password: **admin**), click on "Setup", then click on "Network" and follow the directions in the Web Server/Network/Setup section of this manual.

IV. Outlet On LED Indicator

The Outlet On LED functionality is as follows:

LED State	Description
On (Solid)	The outlets are On.
On (Blinking)	The Reset button has been pressed for 5 or more seconds. Releasing the button will restore the AR to a factory default state.
Off	The outlets are Off.

V. Web Server

The Axess Ready web interface provides the easiest means of operating the outlet and changing configuration parameters.

To access the web interface, open a web browser and enter the IP address of the AR into the address bar. The factory default IP address is DHCP assigned.

1. **Password**

The AR uses two username/password credential sets, one for normal power control (user) and one that also provides access to the Setup functions (admin). Default

credentials:

Role	Username (fixed)	Password (user set)
Administrator	admin	admin
User	user	user

Enter a valid username and password when prompted. When the proper username/password combination is received, the Control and Status Page is displayed.
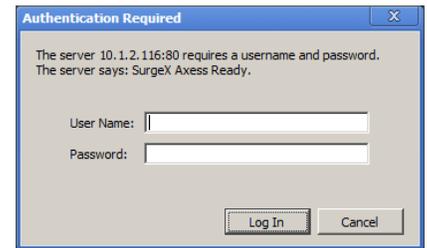
2. **Control and Status Page**

Once a user is validated, the Control and Status page is displayed. *Note: Only one user may be logged in to the AR at a time.*

Press "Power On" or "Power Off" to turn the AC output On or Off. In the event of a power outage, the AC output will return to its last known state prior to the outage.

Press "Cycle Power" to temporarily change the state of the AC output for a specified cycle time (factory default is 10 seconds). The cycle operation performed will either be On-Off-On or Off-On-Off, depending on the initial state of the AC output. During the power cycle operation, the Power Status bar will indicate the temporary status with a Blue background. Once the cycle is complete, the status bar will revert to its original condition. To abort a power cycle, press either "Power On" or "Power Off" and the outlets will assume that status.
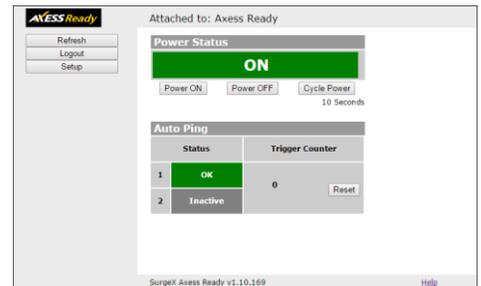
If the AutoPing feature is in use, this page will also display the current status (OK or Failed) for each AutoPing, a counter of how many times the ping failed, and a counter of how many times the defined action was triggered. Reset buttons for the Fail and Trigger counters are available for the admin login.

Use the Refresh button to update the page with the most current status. Use of the browser's refresh button may lead to inadvertent power switching. If an NTP time server is being used, the time of the last refresh will be displayed in the upper right corner.

3. Setup Pages

Setup pages are only available while logged in with Administrator credentials. Press Save to save the new settings. If the new settings require the AR to be rebooted, a Reboot button will appear at the bottom of the page. Settings requiring reboot will not take effect until the unit is rebooted.

Device

Location ID: Specifies a name label (up to 20 characters) that will be displayed at the top of all pages. Assigning unique names is helpful for management of multiple units.

Cycle Time: Specifies the length in seconds of a power cycle (1-999 seconds). This is the amount of time the outlet will temporarily be On or Off, depending on the initial outlet state.

Initial State: Specifies the initial state the AC outlet(s) will assume when the unit is powered up or reset.

Upgrade Enable: Enables the ability to upgrade the firmware of the AR.

Auto Logout: Specifies the inactivity timer duration in minutes (0-99 minutes). If there is no activity after the specified amount of time, the user will be automatically logged out. Setting the timer duration to 0 disables the timeout feature.

Important: As the AR allows only one web user logged in at any time, use caution when disabling the timeout feature, as it is possible to lock out other users by forgetting to log out. Closing the web browser will not log the user out, and will lock out web access. In this situation it will be necessary to access the AR via telnet and reboot the unit.
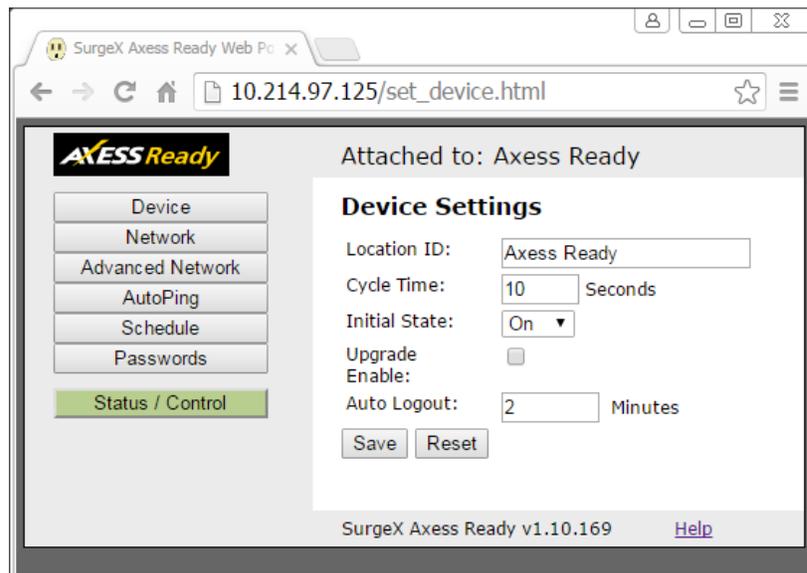
V.   Web Server (continued)

Network

IP Mode: Select Static to manually set the IP address using the fields below, or choose
DHCP to allow the AR to automatically acquire its network settings from a DHCP server.

IP Address: Enter a static IP address in dotted decimal format. This field will be automatically set if using
DHCP.

Subnet Mask: Enter the Subnet Mask in dotted decimal format. This field will be automatically set if using
DHCP.

Gateway: Enter the Gateway in dotted decimal format. This field will be automatically set if using DHCP.

DNS: Enter the Domain Name Server address. This will be automatically set if
using DHCP.
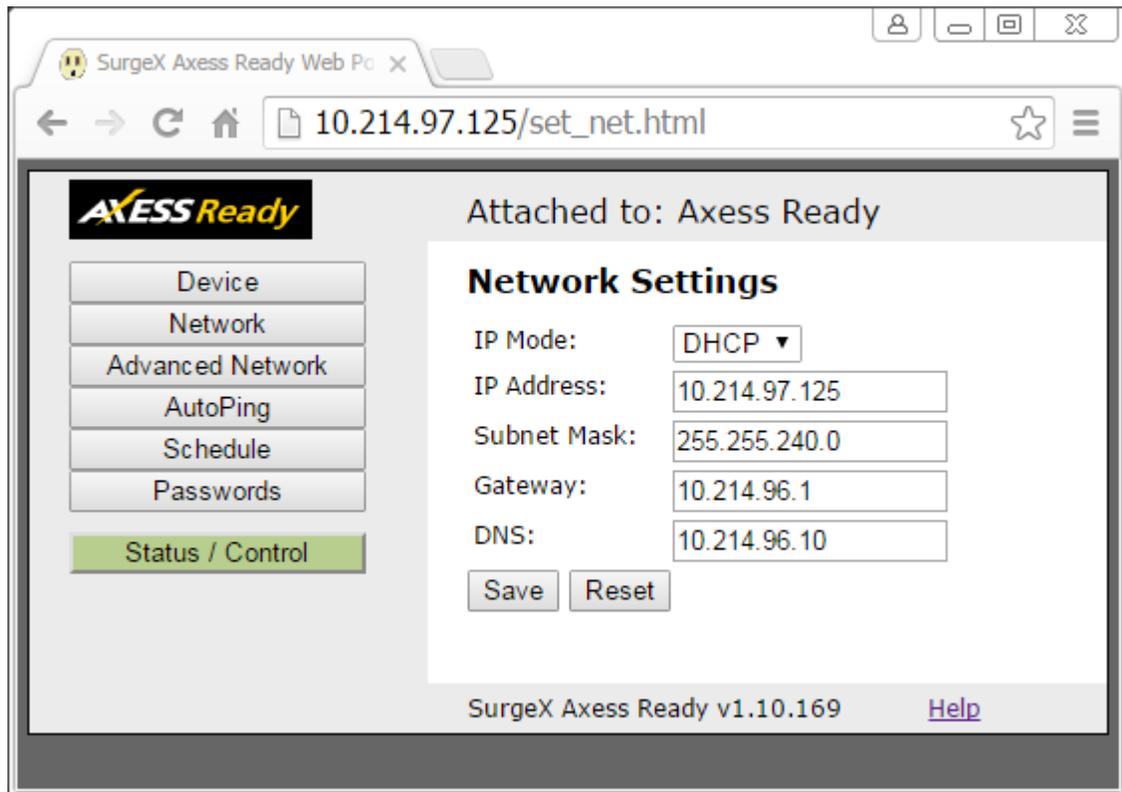
<u>Advanced Network</u>

HTTP Port: Specify the port the web server will be accessed on. If the port is changed from the default value of 80, the AR may be accessed by specifying the new port number in this format: http://IPADDRESS:NEWPORT. Example: Navigate to http://192.168.1.254:8000 for an IP address of 192.168.1.254 on port 8000.

Linkback URL: This setting allows control of the hotlink displayed on the Goodbye page. It allows use of the public IP address or DNS name instead of the internal IP address of the AR, which is the default setting. If this setting is left blank, the hotlink will be the IP address of the unit. Enter up to 128 characters.

Telnet Port: Specify the port to use for telnet access (default 23).

DxP Port: Specify the port to use for DxP protocol (default 9100).

Time Setup: Setup of the time server is required for Scheduling and Logging functions.
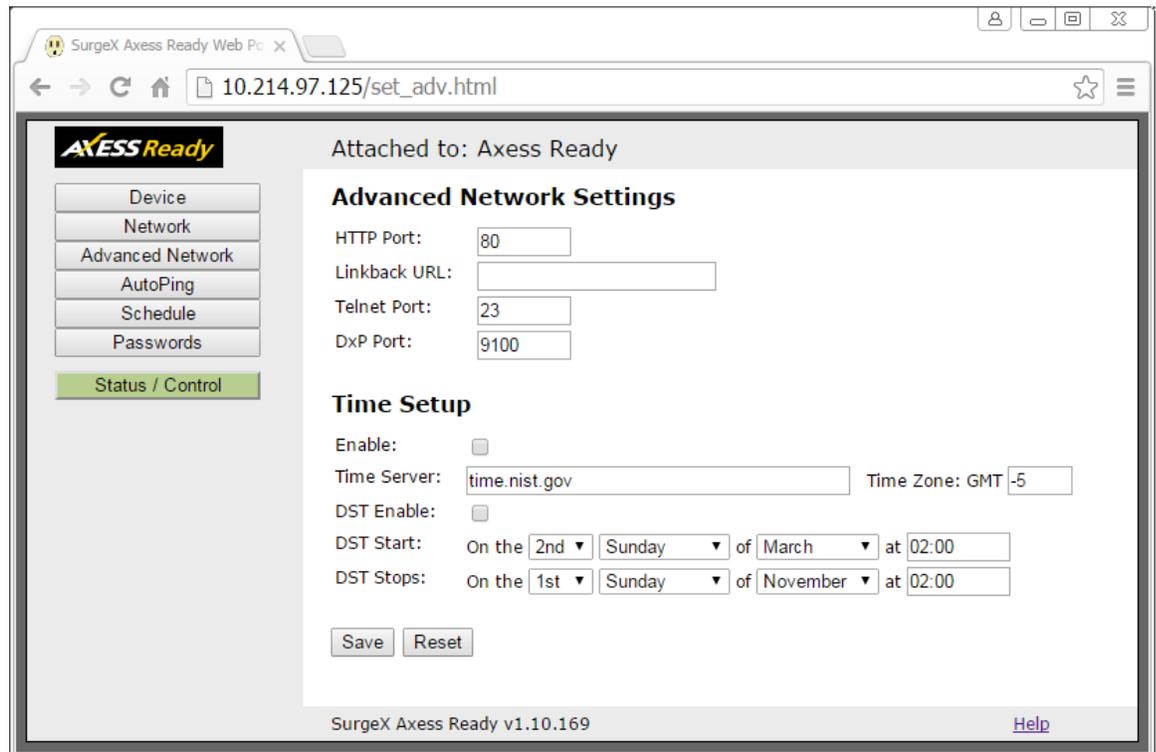
    Enable: Enable or disable the use of the time server.
    Time Server: Specify the time server. The default is time.nist.gov.
    Time Zone: Specify the time zone (-12 to +12) relative to GMT.
    DST Enable: Enable or disable the use of Daylight Savings Time.
    DST Start/Stop: Specify the start and stop times for DST.

V. Web Server (continued)

AutoPing

The AutoPing feature allows the AR to automatically detect failed equipment and perform a timed reboot or other power control function (like turning on an indicator or siren). First specify one or two IP addresses to be periodically pinged. When the AR no longer receives a response from these addresses, the programmed power control function is actuated. AND or OR logic can be applied to the two addresses, so that both (AND) or either (OR) must fail in order to trigger the selected action.

Examples:

Server monitor: AR is installed with the device it monitors and automatically reboots if there is no response. Ideal for Kiosks and Servers.

Service monitor: AR is installed with the device to be rebooted, but pings a remote host to test the communication channel. Ideal for DSL/Cable Modem verification.

AR monitors a network device, and powers up an alarm or redundant system when there is no response. Ideal for Hot Standby Servers, Environmental Control, Alert for any network failure.

AutoPing

AutoPing - Service Verification

AutoPing - Alert Generator

- IP Address 1 and 2: Enter the IP address(es) of the device(s) to be pinged.

- Frequency 1 and 2: Enter the desired ping frequency in seconds for the device(s) to be pinged (1-999 seconds).

- Fail Count 1 and 2: Enter the number of times the ping must consecutively fail (1-999) before the selected action is triggered.

- Mode: Select the logic to be used (AND, OR, or Single). With AND logic, both AutoPings must exceed their fail count to trigger the action. With OR logic, the action will be triggered if either AutoPing exceeds its fail count. With Single, only AutoPing 1 is used.

V.   Web Server (continued)

- Action: Select the action to be triggered.

None	AutoPing not used
Power On – Latch	Upon triggering, AR will power on and remain so until changed via web, telnet, or DxP.
Power On – Follow	Upon triggering, AR will power on. When the ping response returns, AR will power off.
Power Off – Latch	Upon triggering, AR will power off and remain so until changed via web, telnet, or DxP.
Power Off – Follow	Upon triggering, AR will power off. When the ping response returns, AR will power on.
Power Cycle	Upon triggering, AR will cycle the power. AR will then wait for (Ping Frequency x Fail Count) seconds; if the response does not return, the power will be cycled again. This will repeatedly continue until the ping response returns or AutoPing is turned off. Ensure that the AutoPing frequency is longer than the time required to reboot the device.
Power Cycle - Once	Upon triggering, AR will cycle power one time. It will not cycle again automatically until the ping response returns and is lost again.

- Restart: This setting delays the restart of the AutoPing tests after the Action is completed. This setting allows time for the boot sequence of the failed device to complete.
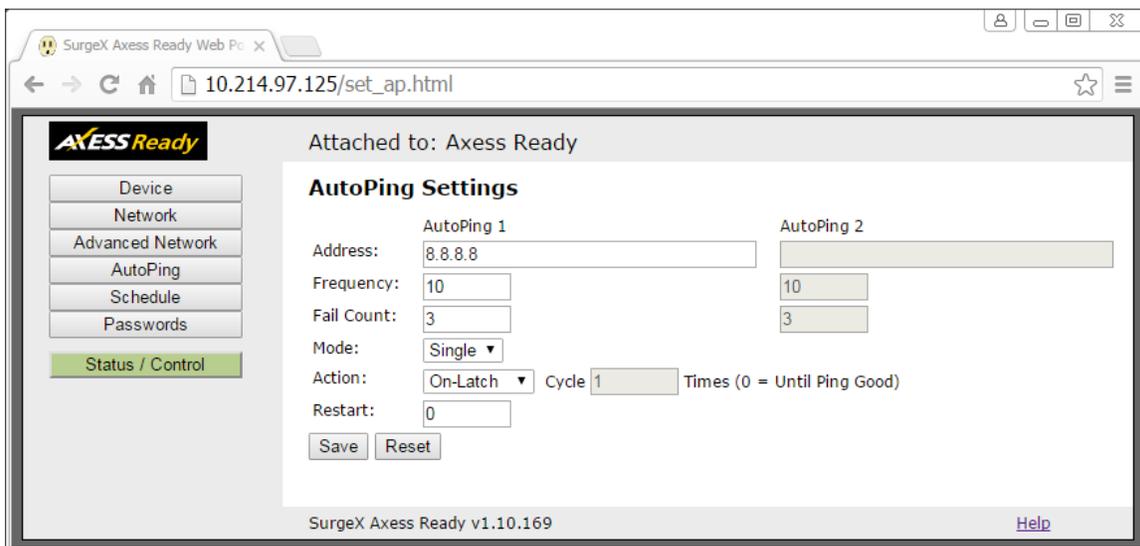
Schedule

The AR can schedule up to 8 recurring power events. For each event, you may define the starting date and time, the action to be taken, and the repetition interval (optional).

Important: A Network Time Server (NTS) must be specified and enabled in order to use the time scheduling feature. A list of public time servers is available at http://www.ntp.org.

- Date: Set the initial date for the event in mm/dd/yyyy format.

- Time: Set the initial time for the event in hh:mm format. Hours are specified in 24 hour format; for example, 8:05 pm would be entered as 20:05.

- Repeat (Optional): Set the repetition interval. 0-999 Days, Hours, or Minutes.

- Action: Set the action to be scheduled. On, Off, or Cycle.

- Hold/Run: Click Hold to pause the scheduled event. Click Run to re-start the scheduled event.

- Clear: Deletes a schedule.
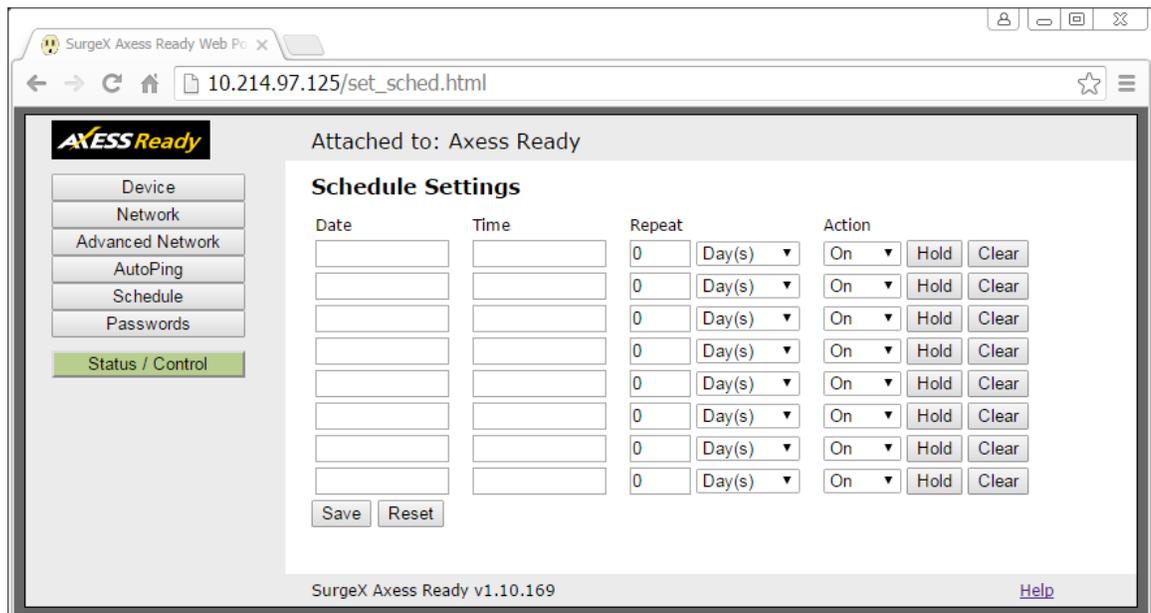
V.   Web Server (continued)

Passwords

Two passwords are used by the AR. The User password allows control of the AC output state, but provides no access to Setup functions. The Administrator password allows full control and setup of the AR.

Passwords may be up to 20 characters long, and are case sensitive.

The AR supports three modes of user and password operation.

- Login Required: Login with password is required for web and telnet access.

- Auto Login: No login challenge will be required for any mode of operation, until a Setup function is requested.

- User Disabled: There is no User account. The Admin username and password will be required for operation and setup functions across all modes of operation. This is the factory default mode.

- Old Password: Enter the password currently in use.

- New Password: Enter the new password to be used.

- Confirm Password: Enter the new password to be used again. Default

credentials:

Role	Username (fixed)	Password (user set)
Administrator	admin	admin
User	user	user
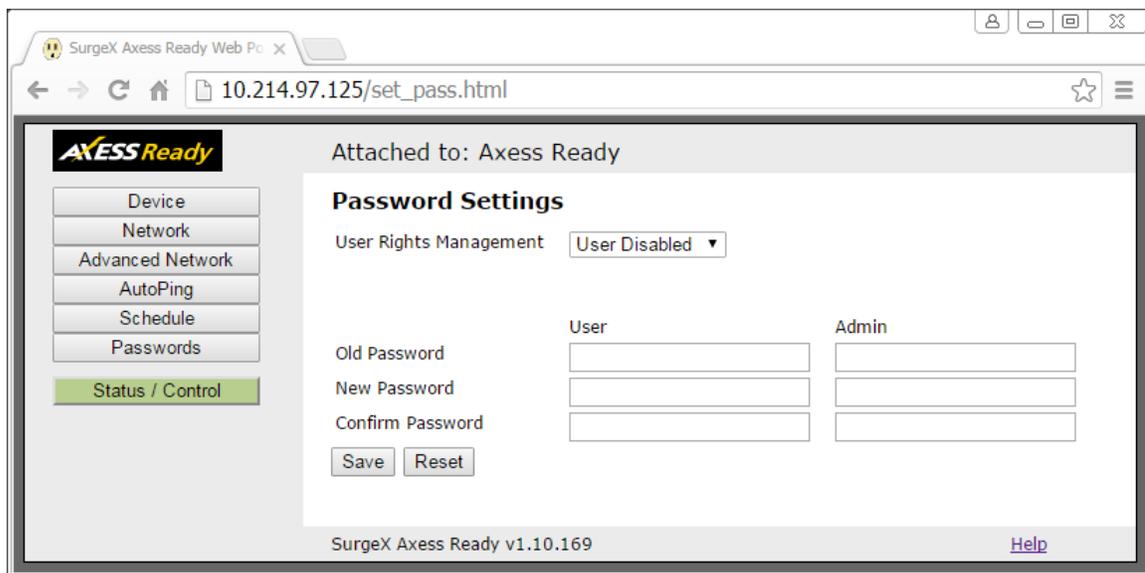
VI. Command Line Interface (CLI) Protocol

The Command Line Interface provides complete setup of all functions of the AR. The CLI may be accessed through the Telnet protocol, and requires a Telnet client program. Some commands of the CLI require administrative rights; these are indicated in the following tables.

1. **Prompts**

Prompt	Description
User>	Prompts the user to enter the user name (either user or admin).
Password>	Prompts the user to enter the password.
Axess Ready>	Prompt displayed while logged in.
Axess Ready Reboot Required>	Prompt displayed after changes have been made that require a reboot. This prompt will remain active until the AR has been rebooted.

2. **Control Commands**

Command	Description	Admin	Fact Def
get outlet	Returns the current status of the outlet.	No	
set outlet < on | off | cycle >	Sets the outlet to the selected state.	No	

3. **Device Commands**

Command	Description	Admin	Fact Def
get location	Returns the location ID.	Yes	Axess Ready
set location < 20 character max >	Sets the location ID.	Yes	
get cycle	Returns the cycle time currently in use in seconds.	Yes	10
set cycle < 1-999 >	Sets the cycle time in seconds.	Yes	
get upgrade enable	Returns the upgrade enable status.	No	Disabled
set upgrade enable < yes | no >	Enables or disables the ability to upload new firmware.	Yes	
Login	Prompts for admin credentials when logged in as user.	No	
Logout	Terminates the telnet session.	No	
Reboot	Reboots the AR.	Yes	

4. **Network Commands**

Command	Description	Admin	Fact Def
get network	Returns all network settings currently in use. Example: Mode: DHCP IP Address: 10.1.2.69 Subnet: 255.255.255.0 Gateway: 10.1.2.1 HTTP Port: 80 Telnet Port: 23 DxP Port: 9100 Timeout: 20	Yes	
set ipmode < static | dhcp >	Sets the IP address mode. Static mode locks the IP address as set; DHCP mode allows a DHCP server to assign the address.	Yes	DHCP
set ipaddress < dotted decimal >	Sets the IP address.	Yes	DHCP
set subnet < dotted decimal >	Sets the Subnet Mask.	Yes	DHCP
set gateway < dotted decimal >	Sets the Gateway address.	Yes	DHCP
set http port < 0-65535 >	Sets the port that the internal Web server listens for incoming connections on. When set to 0 the web server is disabled. May not be disabled when Telnet and DxP are both disabled.	Yes	80
set telnet port < 0-65535 >	Sets the port that the internal Telnet server listens for incoming connections on. When set to 0 the Telnet server is disabled. May not be disabled when Web and DxP are both disabled.	Yes	23
set dxp port < 0-65535 >	Sets the port that the internal DxP service listens for incoming connections on. When set to 0 the DxP service is disabled. May not be disabled when Web and Telnet are both disabled.	Yes	9100
Set linkback <url>	This command sets the linkback URL displayed on the logout page.	Yes	
set timeout < 0-999 >	Sets the automatic network timeout in minutes.	Yes	2

5. AutoPing Commands

Command	Description	Admin	Fact Def

get autoping	Returns all AutoPing settings currently in use. Example: AutoPing 1
	
	                                    AutoPing 2
	IP Address: 10.1.2.36 0.0.0.0
	Frequency: 60 10
	Fail Count: 3 3
	Status: OK OK
	Trigger Count: 0 0
	
	----------------------------------- 	
	
	Mode: Single Action:
	                 On-Latch
		Yes	

set autoping < 1 | 2 > address < dotted decimal >	Sets the IP address to be pinged for AutoPing 1 or 2.	Yes	0.0.0.0
set autoping < 1 | 2 > frequency < 1-999 >	Sets the frequency (how often the ping is sent) for AutoPing 1 or 2 in seconds.	Yes	10
set autoping < 1 | 2 > failcount < 1-999 >	Sets the number of consecutive failures the AutoPings must detect before the AutoPing considers the pinged device to be failed.	Yes	3
set autoping mode < single | and | or >	Sets single AutoPing (AutoPing 1) or two AutoPing relationship AND or OR.	Yes	AND
set autoping action < none | on-latch | on-follow | off-latch | off-follow | cycle | cycle-once >	Sets the action to be performed when the AutoPing is triggered.	Yes	None
set autoping cycle <0-999>	Sets the maximum number of power cycles when the AutoPing triggers. 0 = Unlimited	Yes	1
set autoping restart <1-999>	Sets the delay in seconds to restart AutoPing tests after Action.	Yes	0

6. User Commands

Command	Description	Admin	Fact Def
set password < user | admin > < old > < new > < repeat >	Sets the password of the User or Administrator.	Yes	user | admin
set user account <yes | no>	Sets whether or not a user account is used.	Yes	No
set login required <yes | no>	Sets whether or not a login is required for user level operation. A login is always required for admin functions.	Yes	Yes

7. **Event Commands**

Command	Description	Admin	Fact Def
get events	Returns all scheduled events currently in use. Example: Date Time Repeats Action 1. 12/22/2011 14:00 every 2 Hour(s) Cycle 2. every 0 Day(s) On 3. every 0 Day(s) On 4. every 0 Day(s) On 5. every 0 Day(s) On 6. every 0 Day(s) On 7. every 0 Day(s) On 8. every 0 Day(s) On	No	
get time	Returns the current time and time server. Example: Current Time: 10:14:17 12/20/2011 Server: 10.1.2.12	No	
set time server < dotted decimal >	Sets the IP address of a Network Time Server.	Yes	64.90.182.55
set time enable < yes | no >	Enables or disables the use of a time server and scheduled events.	Yes	No
set event <1-8> <run | hold>	Allow the event to run, or put the event on hold.	Yes	Run
set event < 1-8 > date < mm/dd/yyyy >	Sets the scheduled event's starting date.	Yes	
set event < 1-8 > time < hh:mm:ss >	Sets the time the scheduled event will occur in 24 hour format.	Yes	
set event < 1-8 > repeat < day | hour | minute >	Sets the repetition interval type for the selected event.	Yes	
set event < 1-8 > mult < 0-999 >	Sets the number of repetition intervals for the selected event. For example, 20 days, 30 minutes, 24 hours, etc.	Yes	
set event < 1-8 > action < on | off | cycle >	Sets the action to be performed at the scheduled time.	Yes	
del event < 1-8 >	Deletes the scheduled event.	Yes	

1. **Overview**

   The DxP Protocol is a packet-based protocol designed to be extensible. This protocol is transmitted over TCP on a user-defined port. The factory default DxP port is 9100.

   The protocol uses a Hello handshake to establish unique sequence numbers to allow for advanced security when AES encryption is used. With AES enabled, all messages must be encrypted with the AES Passphrase set in the device.

   After the Hello, a Command and Response sequence follows. Any number of
   Command → Response sequences are permitted after Hello.

2. **Hello Handshake**

   The client sends a Hello message in the form of a text string 'hello-000'. The DxP enabled device will respond with a packet containing the unsigned 16 bit sequence number. This sequence number is incremented by the client and server with each correct packet sent.

   Example:

Client		Server
hello-000	→	
	←	1234 (seq 1234)
Command (seq 1235)	→	
	←	Response
Command (seq 1237)	→	
	←	Response

3. DxP Packet

The packet is broken up into 2 parts: the Header and the Payload.

<u>Header</u>

The header is used to carry general information, such as is shown in the C programming structure below:

```
typedef struct {
    eCmnd command;
    char[21] uName;
    char[21] password;
    uChar desc;
    uChar param;
    uint16 seq;
} THeader
```

Variable	Description
command	Enumerated type that tells the DxP server what class of command is being sent. See the Commands subsection for a full list of command classes.
uName	Reserved for future use. It will contain the user name of a user on the ipIO that is being accessed.
password	Reserved for future use. It will contain the password of the user above.
desc	Command descriptor that describes the individual command within a command class. By extension it lets the server know what the payload is. There is a different set of descriptors for each command class; see the Descriptors subsection for a full list of descriptors by command class.
param	Reserved for future use. Optional parameter that may be passed to the server in addition to the descriptor.
seq	The packet's sequence number. Used as part of the security scheme.

<u>Payload</u>

The payload is determined by a combination of the command class and the descriptor. The payloads are described with the descriptor; see the Descriptors subsection for details.

4. **Commands**

There are currently 7 command classes. All classes are defined in the C programming enumerated type definition below:

```
typedef enum { eCmnd_null,
        eCmnd_set,
        eCmnd_get,
        eCmnd_io,
        eCmnd_keepAlive,
        eCmnd_rss,
        eCmnd_rcu
} eCmnd;
```

	Command	Description
0	eCmnd_null	This is a null command and should not be sent to the server.
1	eCmnd_set	This command is used to set programmable variables on the server.
2	eCmnd_get	This command is used to get programmable variables from the server.
3	eCmnd_io	This command is used to monitor and control the I/O on the server.
4	eCmnd_keepAlive	This command is sent to the server as a means of allowing the client to validate the communications path to the server.
5	eCmnd_rss	This command class is used to control the RSS nest using the RCU. **Note: Project specific command. Not for general use.**
6	eCmnd_rcu	This command class is used to update the display of the RCU. **Note: Project specific command. Not for general use.**

5. **Descriptors**

Descriptors are used to describe the individual command within a command class, and the payload that the packet contains. All of the descriptors and their payloads are outlined by command class below.

eCmnd_set
The descriptors for this command class will be product specific.

eCmnd_get
The descriptors for this command class will be product specific.

eCmnd_io

```
typedef enum{ eIO_null,
    eIO_changeRelay,
    eIO_changeRelays,
    eIO_getRelay,
    eIO_getRelays,
    eIO_getInput,
    eIO_getInputs,
    eIO_pulseRelay,
} eIO;
```

Command	Description	Server Response
eIO_changeRelay	This command is used to change the status of an individual relay. It carries the TChangeRelay payload; see the Payloads subsection for details.	0 → Successful 1 → Error
eIO_changeRelays	This command is used to set all of the relays in a device. It carries the TChangeRelays payload; see the Payloads subsection for details.	0 → Successful 1 → Error
eIO_getRelay	This command has not yet been implemented.	
eIO_getRelays	This command is used to get the status of all the relays on the server.	Byte Array containing status of each relay.
eIO_getInput	This command has not yet been implemented.	
eIO_getInputs	This command is used to get the status of all inputs on the server.	Byte Array containing status of each input.
eIO_pulseRelay	This command is used to pulse a relay. It carries the TPulseRelay payload; see the Payloads subsection for details.	0 → Successful 1 → Error

eCmnd_keepAlive

```
typedef enum{
    eKeepAlive_null;
} eKeepAlive;
```

Command	Description	Server Response
eKeepAlive_null	This is the only valid descriptor that the keep alive command supports. It is defined as null, as it carries no payload.	0 → Successful 1 → Error

6. **Payloads**

TChangeRelay

```
typedef struct{
        unsigned char relay;
        unsigned char state;
} TChangeRelay;
```

Where relay is the number of the relay to be affected – 1 (For example, 0 for relay 1 and 1 for relay 2) and state sets the state of the relay (1=Energize; 2=Relax).

TChangeRelays

```
typedef struct{
        unsigned char relayStates[32];
}TChangeRelays;
```

Where relayStates is an array of relay states as defined below:

```
#define NO_CHANGE  0
#define ENERGIZE         1
#define RELAX            2
```

This payload is supported by devices that support the DxP protocol with 2-32 controllable relays.

TPulseRelay

```
typedef struct{
        unsigned char relay;   //the relay to be pulsed unsigned
        char state;   //the state to pulse
        uint16 pulseWidth;         //the pulse width in seconds
}TPulseRelay;
```

Where relay is the number of the relay to be affected, state is the state to pulse, and pulseWidth is the time to pulse in seconds.

VIII.   Firmware Upgrades

The AR can be upgraded via the network if the upgrade feature has been enabled. To perform a field upgrade, follow the steps below.

Important: Upgrading the firmware with a minor upgrade (For example, 1.01.xx to 1.01.yy) will not alter the user defined settings. Major upgrades may or may not reset the AR to factory defaults. Check the release notes for the upgrade before making any changes.

1. Download the latest firmware version and Device Management Utility (DMU) from the SurgeX website: http://www.espsurgex.com.

2. Enable the upgrade feature. Use the CLI **set upgrade enable yes** command via telnet, or check the "Upgrade Enable" box on the Device web page.

3. Run the DMU. If the AR you would like to upgrade is not visible in the list box, either:

    •   Select Device | Discover from the menu to locate the ARs on the local network.
    •   Select Device | Add from the menu to manually add the AR by IP address. Once the

    device is displayed in the list, highlight it.

4. Select Manage | Upgrade Firmware.

   Enter User Name admin and the password for the Administrator.

    Enter the filename of the new firmware, or click Browse and navigate to the firmware file to be used. AR firmware files use the file extension **.g2u**. If no files of that type are displayed, ensure that the "Files of Type" box is set for SX-iPD or All Files.

    Click OK when all details are entered.

5. The upload will begin, and a progress bar will be displayed.

6. When the firmware upload is complete, the AR will automatically reboot and will be ready for use.

IX.   Reset Button

The recessed reset pushbutton located on the front panel performs 3 functions as detailed below:
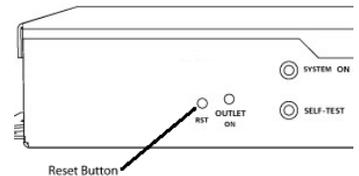
Action	Result
Momentary	Soft Reset. Will not affect outlet state.
5 Second Push	Reset to Factory Defaults. Hold until the "System On" LED is blinking, then release.
Hold while powering up	Recovery Mode. Allows upload of new firmware to the current IP address.

X.   Specifications

Physical	
Height	1.8125"
Width	11.375"
Depth	7.625"
Weight	4.75 lb.
Temperature	5 - 35° C
Humidity Range	5% to 95% R.H., non-condensing

AC		
Load Rating		8 Amps @ 120 Volts
Power Requirement (no load)		10 Watts
UL 1449-2 Adjunct Classification Test Results		1000 surges, 6000 Volts, 3000 Amps,C1 pulse, measured suppressed voltage 290 Volts, no failures
Maximum Applied Surge Pulse Joule Rating		Unlimited, due to current limiting (8 x 20 µs)
Maximum Applied Surge Pulse Voltage		6000 volts (1.2 x 50 µs pulse),industry standard rating
Maximum Applied Surge Pulse Current		Unlimited, due to current limiting (8 x 20 µs)*
Endurance		IEEE C62.41-1991 Category B3 (C1)
Pulses		1 kV>500,000; 3 kV>10,000; 6 kV>1000
Overvoltage Shutdown		145 Volts (resume at 135 Volts)
EMI/RFI Filter	Normal Mode (50 Ω load)	30 dB@100 kHz; 56 dB@300 kHz;64 dB@3 MHz; 24 dB@30 MHz
	Common Mode (50 Ω load)	9 dB@300 kHz; 16 dB@1 MHz;28 dB@5 MHz; 35 dB@20 MHz

Compliance	
UL/cUL	UL60950 Listed I.T.E. File No. E225914 Conforms to UL Stds 1283 & 1449
CSA	Certified to CSA Std C22.2 No. 8
CE	Directives 89/336/EEC, 92/31/EEC and 93/68/EEC EN 60950: 3rd Edition EN55022: 1998 Class B
FCC	Part 15 Class B

Network
Single 10/100 Unshielded Twisted Pair Ethernet Jack
IP Addressed: DHCP Assigned or Static
Internal HTTP Web Server
Forms Processing Browser Required
Internal Telnet Server

*1.2 x 50 µs pulse, industry standard combination wave surge,as per IEEE C62.41