CHAPTER 1
Introduction

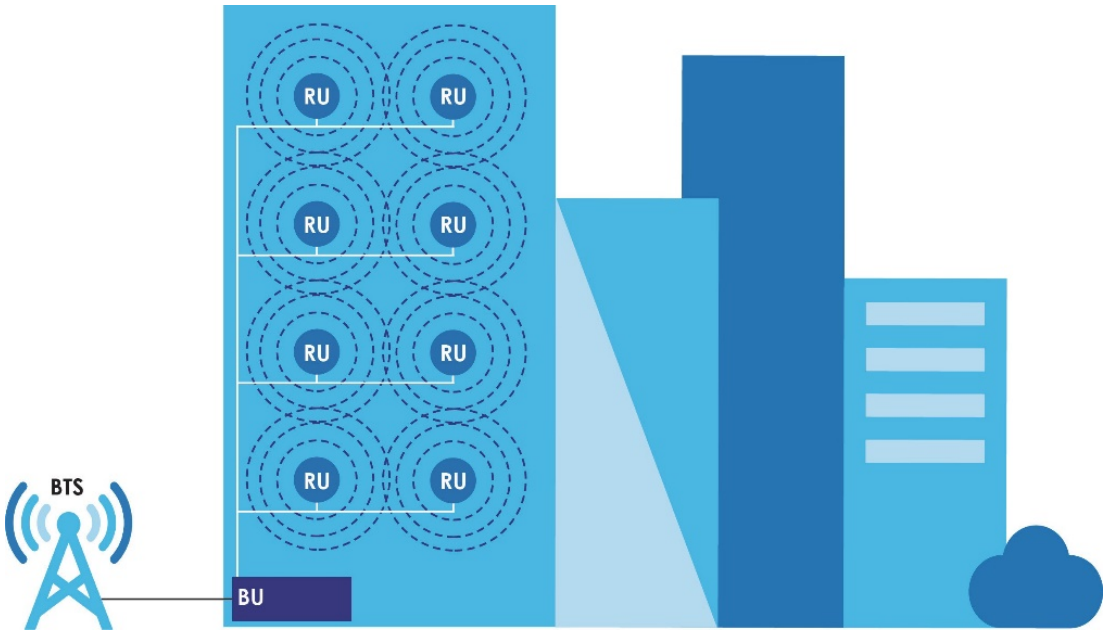
1.1 Design Overview

ZoneDAS is a brand-new take on Active DAS architecture, one that is simple, flexible, and highly functional. Being analogue based, it avoids digital conversion and its inherent signal delays. Being CAT5 based, it avoids the trouble and cost of deploying coaxial cables and fiber optics. Being modular, it offers unrivaled flexibility in band configuration, coverage, and upgradability. Being active, it offers precise, real-time control over output signal strength and pattern. And being smart… it compensates for cable loss and sets system gain to match user-defined RF output—all automatically.

Like passive DAS, ZoneDAS begins with signal source(s) from one or more operators. Instead of having a passive combiner that merges signals and sends them to passive antennas, however, it has a *Base Unit* (BU) that replaces the combiner, and *Remote Units* (RUs) that replace the passive antennas. And whereas passive architecture is a complex series of compromises around limited signal strength and delicate antenna output, ZoneDAS architecture replicates signal strength and guarantees full-strength antenna output. This allows for a far simpler, *goal-oriented* design: simply place an RU wherever signal is required and know that it will have high quality signal! After all, CAT5 cabling goes anywhere.

Basic layout looks like this: up to 4 input signals come through RF coaxial cables and plug into the BU, which often sits in the machine room along with telephone and networking equipment. The BU then processes these signals and sends them via CAT5 cable to its RUs (1 per cable), which are placed throughout the building to broadcast the signals. Each CAT5 cable can be up to 100 meters long, and the whole system requires just one power plug, for the BU. RUs get power over Ethernet and do not require additional power. **That's it! As simple as Active DAS can be.**

Figure 1 Basic ZoneDAS Architecture

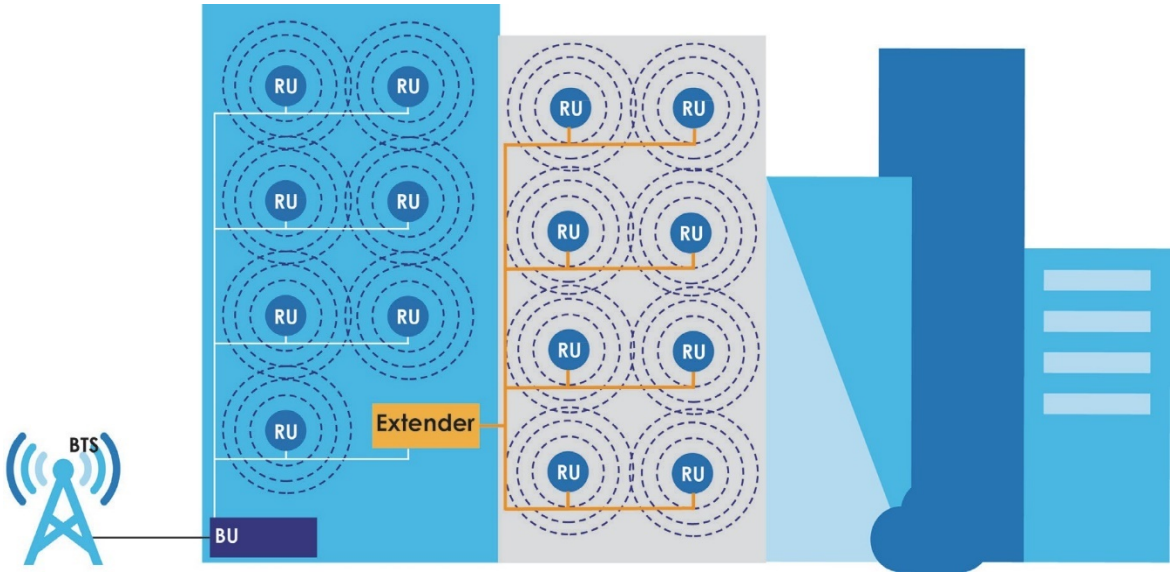


Like the combiner in passive DAS, the BU combines its input signals and sends the combined signal to each RU. Unlike in passive DAS, cable loss has been compensated for and signal quality is preserved for every RU. Each RU simply amplifies the signal to its specified strength and broadcasts it through its antenna(s), up to 4 of which it may fit onto each RU. The RU has powerful integrated amplifiers (up to 23 dBm per band) and uncompromised low noise figures (down to 5dB) for optimizing system footprint and thus lowering overall TCO of the site solution. With ZoneDAS, you can software select between *directional* and *omnidirectional* configurations for optimal coverage and best signal-to-noise ratio. For RUs configured with external antennas, output signal pattern depends on the antennas installed. Strategic RU placement and configuration will then ensure optimum coverage and strong cellular signal.

ZoneDAS is highly scalable and supports additional coverage through its companion device, the *Extender*. An Extender is essentially a subsidiary BU: it plugs into the BU like an RU and supports a brand-new set of RUs. It receives RF signal from the BU, transmits the signal to its RUs, and sends its RUs' signals back to the BU.

In this guide, "ZoneDAS" refers to the entire BU-RU system. ZoneDAS is capable, flexible, expandable, and elegantly simple. Its modular design enables it to support operator bands and frequencies from around the world and ensure future upgradability when new technologies arrive. Its ability to use CAT5 cables and PoE/RFoE technologies facilitates cost-effective, quick, and simple deployment, with no need for separate power supplies for its RUs. In addition, its simple, single-wire RU connections mean easy re-deployments should the host building undergo modifications to its layout.

Figure 2 ZoneDAS with Extender



1.2 Coverage & Applications

ZoneDAS is ideal for medium sized buildings and installations. Its BU connects up to 8 RUs, each of which supplies cell phone signals for an area up to 2,500m^2, so a basic ZoneDAS setup covers up to 20,000m^2. ZoneDAS is also highly extensible and can service larger areas when required, through Extenders. Installing an Extender adds capacity for 1~8 additional RUs, further increasing maximum coverage by 20,000m^2. With a full complement of 8 Extenders, one ZoneDAS can connect up to 64 RUs for a total coverage area of 160,000m^2— the area equivalent of 3 football fields! This could represent multiple floors in a high-rise office/residence, a large factory, or a large shopping center.

1.3 Hardware Overview

Before installation, it is helpful to go over the system's parts and what this User Guide calls them. In particular, one needs to be familiar with the ports and modules on the BU, Extender, and RU. This section describes these devices' front panels and provides information that may require special attention. Where "left" and "right" are mentioned, this Guide assumes that the user is sitting opposite to and looking *at* the front panel of the device.

1.3.1 Names and Terminology

ZoneDAS devices use a 2-letter naming scheme. Each device is abbreviated into 2 letters. For example, the Base Unit (a device) is abbreviated into just "BU". Below is a short list of 2 letter device abbreviations and what they represent:

BU	Base Unit
RU	Remote Unit
ET	Extender

Major ports and modules are also abbreviated into 2 letters. A Radio Frequency module, for example, is referred to as an "RF" module. Likewise, the slot for inserting that module is called the "RF" slot, and the port on that module is referred to as the "RF" port. Below is a short list of 2 letter port/module abbreviations and what they represent:

RF	Radio Frequency port / slot / module
SD	Signal Distribution port / slot / module (for connecting ETs and RUs)
MB	Motherboard

As each BU supports up to 4 RF connections and up to 8 RUs through its 4 RF modules and 2 SD modules (4 SD ports on each), a third character is added to differentiate each RF or SD module/port. Below is a summary of such differentiation:

RFA ~ RFD	Left-most RF module/slot/port is A, right-most is D, etc.
SD-U, SD-L	SD-U is the "upper" SD module/slot, SD-L is the "lower" SD module/slot
SD1 ~ SD8 (a.k.a. RU1~RU8)	The left-most SD port on SD-U is SD1, the right-most is SD4. The left-most SD port on SD-L is SD5, the right-most is SD8. *But on the SD module front panel, they are labelled RU1~RU8 instead of SD1~SD8.*
ET5	The Extender that's connected to SD5 on the BU.

Finally, because ports and modules reside on devices, and because some of the most important ports and modules actually exist on different ZoneDAS devices, device abbreviations are placed in front of port/module abbreviations to specify specific ports on specific devices. The (single) SD port on an RU, for example, is called an RU-SD, while the 5th SD port on the BU is called BU-SD5. Below are some examples of combined abbreviations and what they mean:

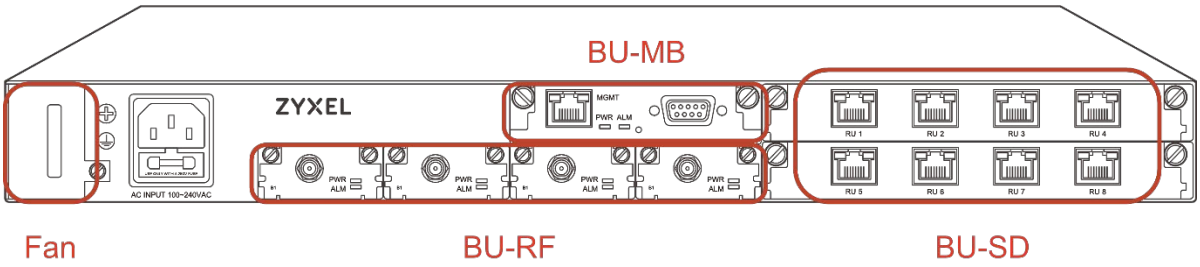
BU-RFA	Left-most RF module/slot/port on the BU.
RU2-RFA	The RF module that is installed onto the RF slot "A" on RU2. This module would match the BU-RFA in terms of Band and frequency.
BU-SD1	The 1st SD port on the BU
ET5-SD2	The 2nd SD port on the Extender that's connected to the 5th SD port on the BU.

Only the most frequently connected devices and ports have 2-letter abbreviations. For example, the Fan module has no abbreviation, and words like Power and Alarm have 3-letter abbreviations.

1.3.2 BU (Base Unit)

The Base Unit is the command center for the entire system. Every device on the system is controlled by or through the Base Unit. To a large degree, the Base Unit's LED indicators also reflect the state of the entire system. These LEDs and ports are located on the BU's Front Panel. The figure below shows the Front Panel and its different parts.

Figure 3 BU Front Panel



The following table describes the parts that are labelled in the figure above.

Table 1 BU System Parts

SYSTEM PART	DESCRIPTION
Fan Module	The BU's fan module provides active cooling for the entire BU, which can operate safely for just a few minutes fan free. The fan module is hot-swappable and user replaceable. See the Hardware Installation Guide for replacement instructions.
BU-MB	The BU's Motherboard (BU-MB) is the user's gateway to controlling everything in ZoneDAS. To access the Web Configurator, connect a computer to the **MGMT** port via a CAT5 cable. To access the Command Line Interface (used by the vendor only), connect it to the Serial Port with a serial cable.
BU-RF (A to D) **A is the left most slot** **D is the right most slot**	This is where the BU houses its collection of Radio Frequency (RF) modules. Each BU has 1 to 4 of these modules, and each module provides one RF port. To connect the BU to a signal source, install an RF module into an RF slot and connect a coaxial cable from the module's RF port to the coaxial outlet at the signal source. The base station can be a picocell, femtocell, LTE RRU (Remote Radio Unit), etc. See the *Hardware Installation Guide* on how to properly install a BU-RF module. Note: The frequency used by the RF module in each RU must match the one used by the corresponding RF module in the BU. For example, if you use a Band 1 RF module for **BU**-RFA, then you must also use a Band 1 RF module for **RU**-RFA.
BU-SD (ports labeled **RU1** to **RU8**)	This is where the BU houses its Signal Distribution (SD) modules. Each BU comes with one SD module and has room for one other. Each SD module comes with 4 SD ports, and each SD port can connect one RU or Extender. To connect an RU or Extender, simply pick an SD port (install a second SD module if the first is full) and connect a CAT5e cable from the RU's SD port (or the Extender's Extender port) to the BU's SD port. The BU supports the IEEE 802.3af PoE standard and can supply power to any connected RU (only RUs, not Extenders). For instructions on installing BU-SD modules, please see the *Hardware Installation Guide*.

Note: See the *Hardware Installation Guide* for information on the proper installation of BU-RF and BU-SD modules.

LEDs (Lights)

Most ports/modules on the BU come with their own set of LED signal lights. These include the MGMT port, each BU-RF, each BU-SD, and the BU-MB. These LEDs provide important information, and the following table explains what the different lights mean.

Table 2 BU LEDs

LED	COLOR	STATUS	DESCRIPTION
MGMT port (Management)	Green (Left)	Blinking	The BU is transmitting or receiving to/from an Ethernet device.
	Amber (Right)	On	The **MGMT** port is connected.
	None	Off	The **MGMT** port is not connected to a compatible device, or the port is disabled.
PWR (Power)	Green	On	The BU is powered on and functioning properly.
		Off	The power is off or the system is malfunctioning / not ready.
ALM (Alarm)	Red	On	There is a hardware failure, such as device overheat, wrong voltage, or abnormal fan speed.
		Blinking	The BU is being reset.
		Off	The system is functioning normally.
BU-RF Module			
PWR (Power)	Green	On	The inserted RF module is powered on.
		Blinking	Firmware upgrade in progress; do not disconnect power supply.
		Off	The inserted RF module is not ready.
ALM (Alarm)	Red	On	The system detects an operational error.
		Off	The inserted RF module is functioning normally.
BU-SD Module			
RUx port	Green (Left)	On	An RU is connected to this port and receiving power from the BU.
		Blinking	An RU is attempting to connect to this port.
		Off	The connected RU is not powered on.
	Amber (Right)	On	Cable signal loss between the BU and the connected RU has exceeded the threshold.
		Blinking	An RU hardware failure, such as device disconnection, high device temperature, or abnormal fan speed, is detected.
		Off	The connected RU is functioning properly.

1.3.3 RU (Remote Unit)

Remote Units are important because they are the active antennas that actually broadcast the signals that are routed through the BU. Being smart, active devices, they also have LED indicators on their front panels that show their current condition. These LEDs are divided into two groups: one reports on the RU-MB; the other reports on the RU-RFs. The figure below shows the front panel and where the LEDs are located, and the tables that follow will provide the details.

Figure 4 RU Front Panel

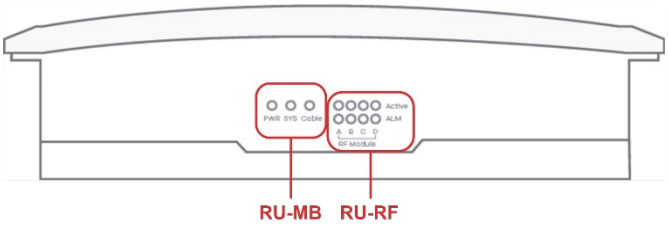


Table 3 RU System Parts

SYSTEM PART	DESCRIPTION
RU-MB	The RU Motherboard (RU-MB) provides the platform upon which up to 4 RU-RF modules may reside. Each RU-RF slot is labelled A, B, C or D, to match the RF slots on the BU. The system is able to power the RU-MB and each RU-RF independently. These devices also provide LEDs signals independently. Three LEDs are used to provide signals for RU-MB. The next table explains what their signals mean.
RU-RF	The RU's Radio Frequency modules (RU-RF) are the devices that actually broadcast RF signals to users' cell phones. Each RU-RF comes with its own antenna (external antenna models excluded), and each RU has up to four RF modules, referred to as RU-RFA to RU-RFD. The letter after RU-RF represents the slot in which the RF module is installed. Note: The frequency used by the RF module in each RU must match that of the RF module in the BU. For example, if you use a Band 1 RF module for BU-RFA, then you must also use a Band 1 RF module for RU-RFA.

LEDs (Lights)

The following table describes the LED signals on the RU.

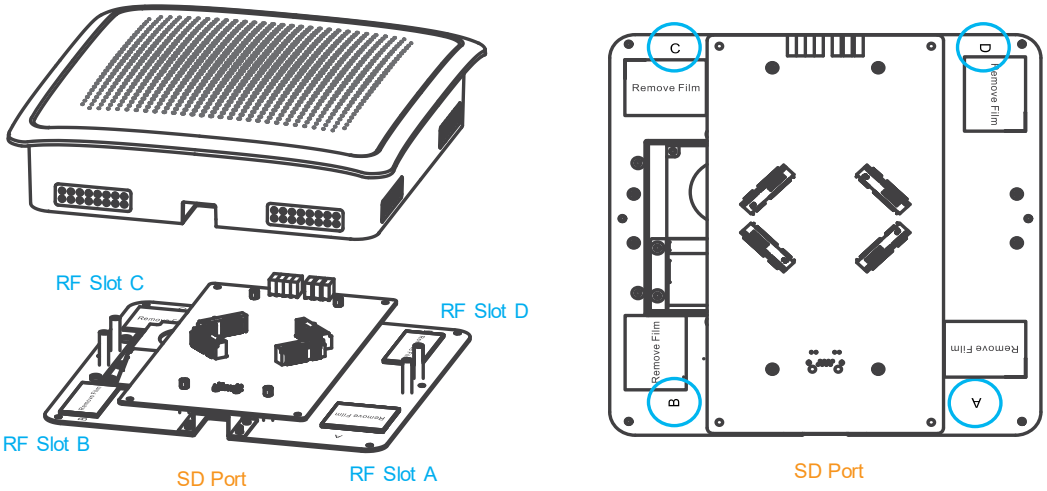
Table 4 RU LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR (Power)	Green	On	The system is powered on
		Off	The DC power is off.
SYS (System)	Red	On	There is a hardware failure, such as device overheat or abnormal fan speed.
		Off	The system is functioning normally.
Cable	Red	On	The cable signal loss currently exceeds the threshold.
		Off	The signal is below the threshold.
Active	Green	On	The inserted RU-RF module is powered on.
		Off	The inserted RU-RF module is not ready.
ALM (Alarm)	Red	On	The system detects an operational error.
		Off	The inserted RU-RF module is functioning normally.

RF Module Placement

Each Remote Unit has an RJ45 port on one side and LED lights on the opposite side. The following illustration shows where RF modules A, B, C and D are placed in relation to the port and lights.

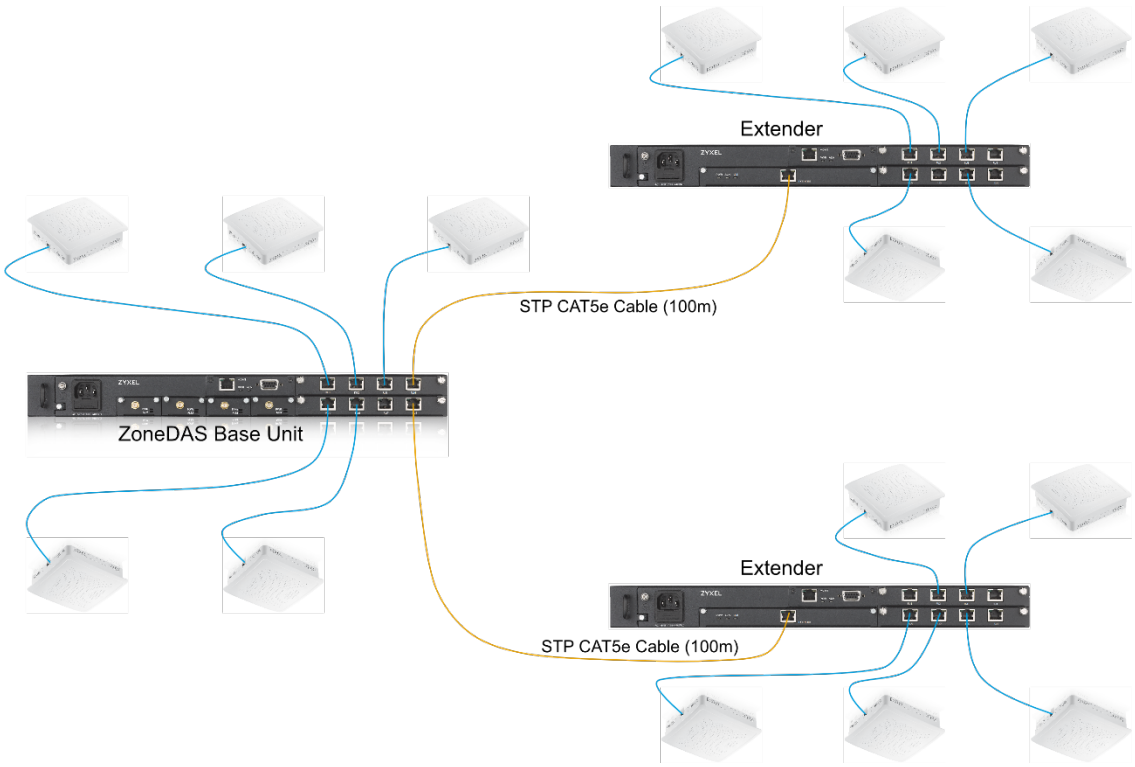
Figure 5 Remote Unit RF Modules



1.3.4 Extender

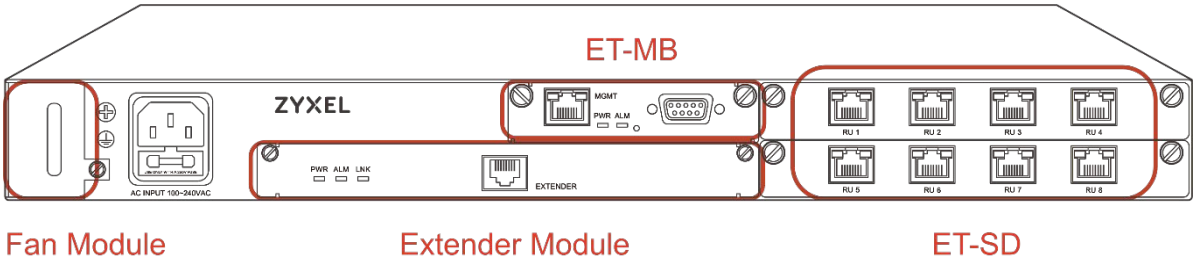
The Extender is a free-standing add-on unit that can greatly expand both the reach and capacity of any ZoneDAS system. Whereas an RU takes up one SD port to provide just one service point, the Extender would take that same SD port and turn it into 8 more! By nature of being a "mid-point station", it also provides another 100 meters of reach between the BU and the RU. So, whereas before there could be a 100-meter cable distance between the BU and the RU, with an Extender there can be 200.

Figure 6 Extender Connection Illustration



The Extender has the same ports and LEDs as the BU, except it has replaced the BU's 4 RF modules with a single Extender module. LED indicators and ports are located on its front panel, with near identical layout as the BU. The figure below shows its front panel and its different parts and ports.

Figure 7 Extender Front Panel



The following table describes the system parts and ports on the Extender:

Table 5 Extender System Components and Ports

SYSTEM PART	DESCRIPTION
Fan Module	This is the Extender's fan module. See the Hardware Installation Guide for replacement instructions.
ET-MB	This is the Extender's Motherboard (ET-MB). You *may* connect your computer to the **MGMT** port using an RJ-45 Ethernet cable and access the Extender directly using its Web Configurator, but this is for special situations only. Likewise, the Serial Port is used only by the vendor to access the Command Line Interface. For normal operation, everything is controlled through the BU, which connects to the Extender though the Extender Port.
Extender Module	The Extender Module houses the Extender Port: the portal through which the Extender connects to the BU. Connecting a shielded CAT5e (or better) cable from one of BU's SD ports to the Extender Port will activate the Extender. **Note**: The cable connecting the BU to the Extender is responsible for transferring signal for up to 8 RUs. As such, we must protect the cable's signal quality. Make sure you **use a shielded or foiled CAT5e cable** for this connection. This includes STP, FTP, S/UTP, S/FTP, or S/STP. **DO NOT use a plain UTP (unshielded twisted pair) cable**.
ET-SD (ports labeled **RU1** to RU8)	This is where the Extender houses its Signal Distribution (SD) modules. As with the BU, each Extender comes with one SD module and has room for one more. Each SD module comes with 4 SD ports, each of which connects one RU. To connect an RU, simply pick an SD port (install a second SD module if there are no more) and connect it to the RU's SD port via a CAT5e cable. The Extender supports the IEEE 802.3af PoE standard and can supply power to any connected RU. For instructions on properly installing ET-SD modules, please see the Hardware Installation Guide.

The Extender looks like a BU and even has its own Web Configurator interface. But it cannot be controlled through the MGMT port like a BU. Instead, it must be connected to a BU (through its Extender port) and controlled through the BU's Web Configurator. *The only function that requires direct MGMT port connection to the Extender is firmware updates.* For that, simply plug a computer console into the Extender's MGMT port and proceed as if the Extender is a BU. All other functions are unavailable from the Extender itself; they must be accessed through the BU.

1.3.5 The Reset Button

If ZoneDAS ever gets stuck and prevents you from accessing the Web Configurator, use the Reset button on the BU front panel to revert settings to factory-default values. The Reset button is located inside a small pinhole, right between the MGMT and Serial ports.

Before pressing the Reset button, make sure the **PWR** LED is on. Then do one of the following:

1. To set the system's **IP address back to factory defaults, press the Reset button for three (3) seconds**, then release. The system indicates that three seconds have passed by flashing the ALM LED. Simply release the Reset button at that time and you will find that the IP address has reverted back to default *192.168.1.1*. To keep this setting, save it before restarting the device again.

   Note: Admin password will not reset to factory default upon resetting the IP address. However, it *will* reset to factory default with a hard reset, as described below.

2. To hard reset all variables back to factory defaults, press the Reset button for ten (10) seconds. Whereas the ALM LED will begin to blink at three seconds, it will stop blinking at ten seconds and automatically reboot. Once the reboot is done, all settings will have been restored to default.

1.4 System Management

The primary interface through which ZoneDAS is managed and configured is called the Web Configurator. It is accessible through any modern web browser and is designed for easy setup and management. It can be accessed on-site through a single network cable, elsewhere in the building through VLAN, or across the globe through VPN. Details on using Web Configurator will be discussed in later chapters.

In addition to Web Configurator, ZoneDAS can be managed via SNMP (Simple Network Management Protocol) using EMS (Element Management System) or a compatible Network Management System. This allows ZoneDAS to be managed as part of a large group of devices—remotely monitored, remotely controlled.

1.5 Best Practices for ZoneDAS Management

Once ZoneDAS is deployed, do the following regularly for effective management and optimal security.

- Change the password. Use a **strong** password that's hard to guess and includes different character types, such as a mix of numbers, symbols, and small and capital letters.
- Write down the password and place it in a safe location.
- Back up the configuration file and make sure you know how to make a restore with it. See Section 7.3 for more on dealing with configuration files. Restoring an earlier functional configuration may be useful if the device becomes unstable and/or crashes. Compared to re-configuring ZoneDAS from scratch, it is often easier to restore your last working configuration and go from there.

CHAPTER 2
First Time Installation

2.1 Overview

This chapter takes the user through setting up ZoneDAS for the first time. In addition to providing step-by-step instructions, it goes through basic system concepts (some of which are unique to ZoneDAS) and briefly explains many parts of the Web Configurator (ZoneDAS's browser interface). For a comprehensive coverage of each Web Configurator menu item, explaining all the LED lighting codes and selectable items, please refer to the chapters that follow, starting with Chapter 3.

2.2 System Setup

There are two steps to setting up ZoneDAS for the first time: Preparation and Configuration. Preparation refers to the hardware placement and installation that must be done before configuration starts. Configuration refers to the software adjustment of settings and parameters. This section provides a brief overview of each; the next section explains Configuration in detail.

2.2.1 Preparation

ZoneDAS setup and planning is quick and easy, but it is still prudent to do everything in the proper order and tick items off a list. Here we provide a list of everything that must be done before software configuration can begin.

1. Decide where to place the BU and all the RUs.
    a. make sure the BU can access source signals from its planned location
    b. make sure that each RU will be within a 100-meter cabling distance from the BU
2. Run CAT5e (or higher spec'd) cables from the BU location to each RU location.
3. Physically install the BU and RUs at their planned locations. For this, please see the BU and RU Hardware Installation Guides.
4. Connect each RU to the BU with the CAT5e cables.
5. Connect each RF signal source to the BU.
    a. Before connection, *be sure* that the RF signal is **always below +30dBm** (1W). Anything above 30dBm will permanently damage the BU! The specified operational range for ZoneDAS is 0 ~ +24 dBm, while the recommended input signal range is 0 ~ +15 dBm.

6. As each RF module is band-specific and likely pre-installed, ensure that each signal source is plugged into the RF module with corresponding frequency range. The 3GPP band (number) is printed on the RF module front panel. **Unlike SD ports, RF ports are not freely interchangeable**.
7. Plug in the BU's power cord and turn on the BU.
8. Connect a computer to the BU, through the BU's MGMT port.
9. Open the browser on the computer and go to http://192.168.1.1.

2.2.2 Configuration

Once all the hardware has been installed, connected, and powered up, configuration may begin. Please follow the steps below to ensure that everything is properly done.

1. Log into ZoneDAS
2. Set the System Time
3. Ensure that RF inputs are within range (0 ~ 24 dBm)
4. Configure BU parameters
5. Mount each RU
6. Configure RU parameters
7. Turn Service On
    a. this will activate System Calibration automatically
    b. ensure that system remains error free after System Calibration
8. Fill in descriptive information such as Site Name and Site ID
9. Configure network settings (Syslog Server etc.) for central management
10. Save settings
11. Create Configuration File, and back it up on a computer

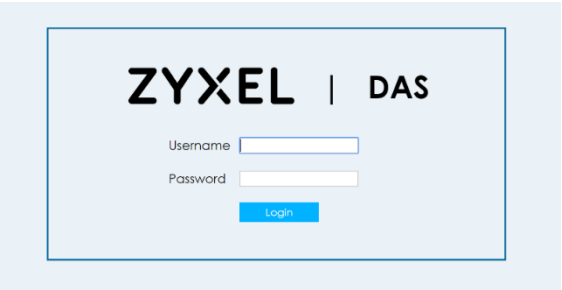
2.3 Configuration Step by Step

As the Configuration steps outlined in the previous section involves numerous details, this section will go through each detail to ensure smooth installation.

2.3.1 Log into ZoneDAS

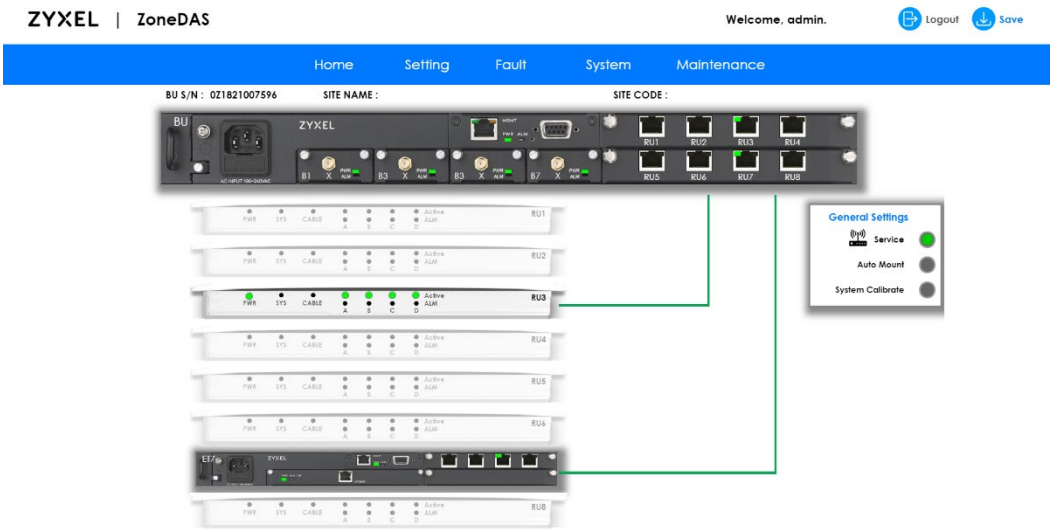
Logging into ZoneDAS is fairly straightforward. Simply connect your computer's LAN port to the BU's MGMT port, then open a browser window (any modern browser will do). In the Address field, type http://192.168.1.1 and press Enter. The following screen should appear:

Figure 8 ZoneDAS Login Screen



From here, simply enter the Username and Password. **Default user name is "admin" and default Password is "1234"**. Once logged in, the *Home screen* would appear. The following is a sample *Home screen*.

Figure 9 ZoneDAS home screen

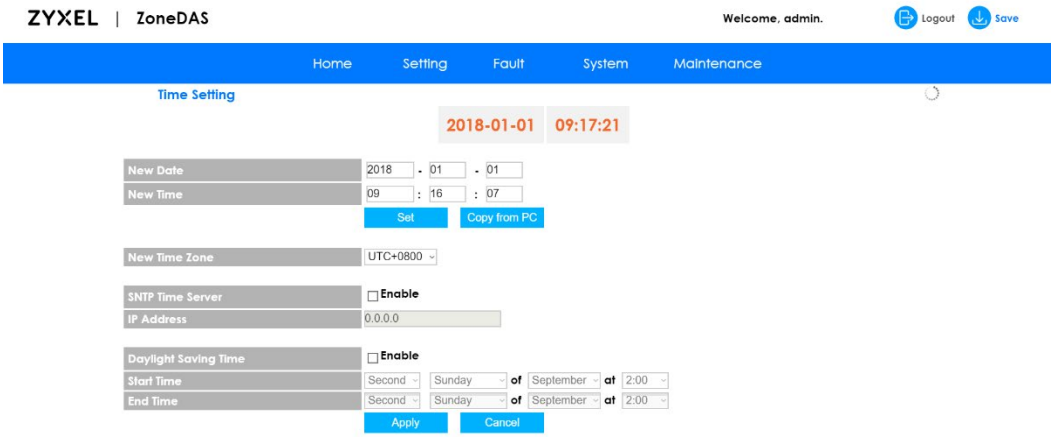


If you have any problems logging into the Web Configurator, please refer to Chapter 3.2, Accessing the Web Configurator, where the process is explained in greater detail.

2.3.2 Set System Time

Once logged in, the first thing to do is to set the System Time and Time Zone. This will ensure that all System Messages (and the Syslog) are stamped with the correct time and date. To do that, click **System** on the *Navigation Panel* (the blue bar) and select **Time Settings**. You will see the *Time Setting screen*, as shown below:

Figure 10 ZoneDAS home screen



If the computer console is set to the ZoneDAS BU's local time, simple click on **Copy from PC** and click **Apply** (blue button, at bottom). This will update the *System Time* (shown in orange, top center) and *Time Zone* to those of the console and show them under *New Date*, *New Time*, and *New Time Zone*.

If the computer console is not a suitable source of time information, then set the time and date manually. Be sure to set the correct Time Zone before setting the time. Simply select the ZoneDAS BU's time zone from the *New Time Zone* drop down menu, noting that UTC is

effectively the same as GMT. If the area also uses Daylight Saving(s) Time, please click the **Enable** checkbox under *Daylight Saving Time* and set the correct values for *Start Time* and *End Time*. The former indicates when Daylight Saving(s) Time starts every year (in the Spring); the latter indicates when it ends (in the Fall).

It is possible to set / maintain the system time automatically via an SNTP Time Server. That is not required at this point, but you may refer to Chapter 7.4 Time Settings Screen to see how this can be done.

2.3.3 Ensure that RF Inputs are Within Range (0 ~ 24 dBm)

Having set the *System Time*, one can move on to configuring the system's RF inputs. These come from two sources: directly from the Operator through a BTS / small cell, or off-air through an Off-Air Kit / SymmRepeater. Either way, the signal will come through a coaxial RF cable and ZoneDAS will treat all signal the same way.

The important thing is to ensure that the signal strength of each RF input falls within the system's operating range of 0 to 24 dBm. ZoneDAS operates optimally when each RF input signal is between 0 and 15 dBm. It will continue to work properly from 15 to 24 dBm, but anything less than 0 dBm is too weak for the system to work with and any level over 24 dBm is too strong for the electronics. If an input signal falls between 24 and 30 dBm, the system will activate its Protection Mode and shut down all operation for that RF channel (and *only* that channel). Input signal stronger than 30 dBm may cause permanent system damage!

The easiest way to see if an RF input is within range is to look at the *Home screen*, at the BU. There, under each RF port, will be an "X", "✓", or "!" mark, like this:

Please note that Module A is the one on the left-most side. Module B is the one to its right, Module C is the next one on the right, and Module D is the right most module. The frequency band used by each module is clearly marked on its face plate.

If the strength of RF input for a module falls within the 0 to 15 dBm optimum range, there will be a check mark (✓) under that RF port. If the RF signal is on the strong side, between 15 and 24 dBm, there will be an exclamation mark (!) to warn of sub-optimal performance. If the RF signal is too weak, below 0 dBm, there will be an X mark to show "no signal".

Please ensure that all connected inputs are marked with check marks (✓). If not, please consult the signal source provider, such as the telecom operator, and resolve the issue.

2.3.4 Configure BU Parameters

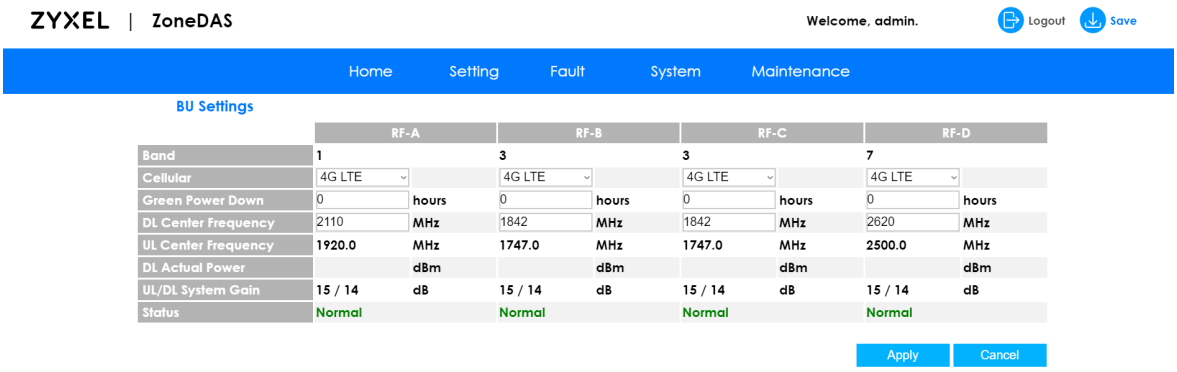
Once all RF signal sources are verified to be within range, it is time to configure the BU's parameters. Specifically, this means RF parameters. If this installation is on behalf of a telecom operator, simply upload their ready-made config file onto the BU, using the steps covered in the next section. If not, the following information is required for each RF signal source:

1. The Frequency Band used by the RF signal (e.g. Band 1, Band 3, Band 7, Band 41, and so forth).
2. Cellular technology used (choose **2G, 3G, or 4G LTE**).
   This matters, because it affects the system's internal parameter settings and tuning algorithms. However, if the information is unknown, a selection called *Auto* is also available.

3. Center frequency for the RF channel. ZoneDAS operates on 20 MHz-wide channels. So if the frequency band is from 2140 to 2160 MHz, simply enter 2150 as the center frequency.

Once the information is ready, simply enter them into the Web Configurator (the system's web-based interface). To do that, click **Setting** on the *Navigation Panel* (the blue bar) and select **BU Settings**. You will then see the *BU Setting screen*, as shown below:

Figure 11 ZoneDAS BU Settings screen



The gray bar at the top of the table shows RF-A to RF-D, from left to right. These correspond to RF modules A, B, C and D. Four identical columns lie below each of these labels, and the first few rows in each column correspond to the information requested above. Note that the system has detected the Frequency Band for each channel, so only verification is required. Simply fill in all the rows for each connected channel, using the information on hand. The system is also equipped with error detection, so frequency values that do not fall within the detected Frequency Band will not be accepted as valid input.

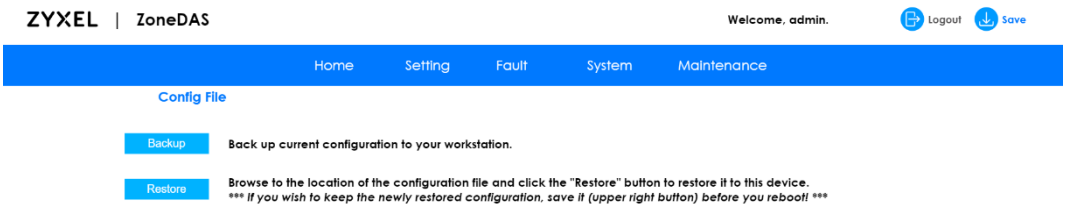
The only row not yet mentioned is *Green Power Down*, which dictates whether a channel will go into Power-Saving Mode if there is no input signal for a time. The unit is hours, so simply input how many hours the system should wait before switching the channel to Power-Saving Mode. To disable Power-Saving Mode, simply enter 0 (factory default).

Once everything has been input correctly, click **Apply**. For verification, go to the *BU screen* and check the RF activity graph for each active RF channel to ensure that signal is as expected. This will be discussed in the section after next.

2.3.5 Loading a Pre-Set Configuration with a Config File

As mentioned above, if this installation is on behalf of a telecom operator, simply upload their ready-made Config file onto the BU, using the steps covered in this section here. The process is very easy. First, click **Maintenance** on the *Navigation Panel* (the blue bar) and select **Config File**. You will see the *Config File screen*, which looks like this:

Figure 12 ZoneDAS Config File screen



From there, click **Restore** and locate the target Config file from the browser's file manager. Double click on the file once it is found, and ZoneDAS will begin the restoration process, which typically takes less than 10 seconds. When it is done, you will see "**Success**" at the top center of the screen.

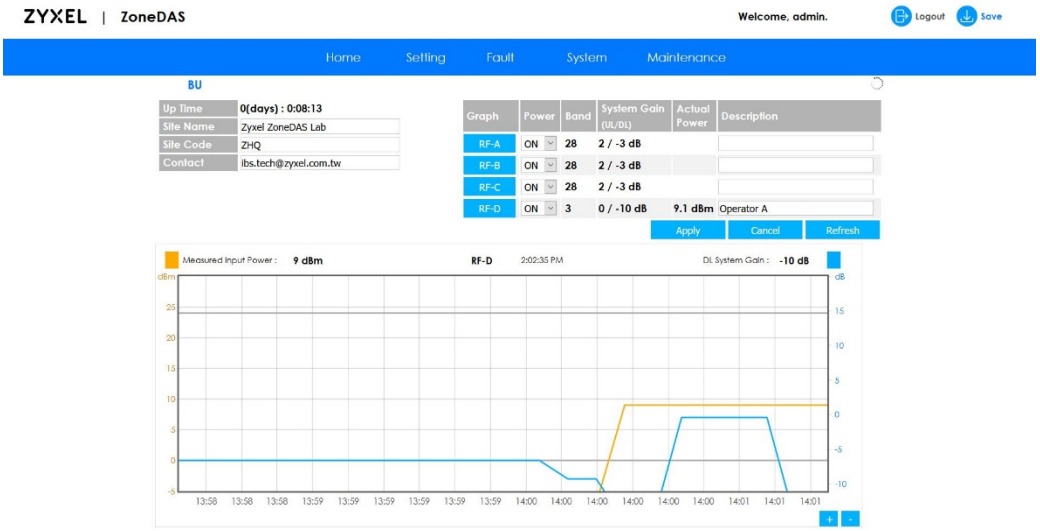
Done! Now all the settings have been loaded and, depending on how the Config file was written, there should be no more setting left to do, and only verification remains to be done.

2.3.6 Checking RF Activity from the BU Screen

As mentioned above, it is prudent to go to the *BU screen* and check the RF activity graph for each connected RF channel to ensure that signal is as expected. To do this, start by clicking **Home** on the *Navigation Panel*. From there, move the mouse pointer to the black Base Unit, such that it is encased in blue, as shown below, then click.

Once clicked, the *BU screen* would appear, as shown below:

Figure 13 ZoneDAS BU screen



The large graph at the bottom of the screen depicts RF activity for the RF module selected. In the above scenario, it is RF-D. To see RF activity for other RF modules, simply click one of the four blue buttons near the top center, marked RF-A, RF-B, RF-C, and RF-D.

The graph has 2 lines: one yellow and one blue. The yellow line marks the Source Signal Strength at any given time, measured against the left axis. The blue line marks the Downlink System Gain that the system automatically generates at the same time, measured against the right axis. The bottom axis indicates the time. *With the cursor on top of the graph, turning the scroll wheel on the mouse shrinks or expands the scope of the time axis*, while holding on to the left mouse button and moving the mouse left and right makes the graph go back and forward in time.

What needs to be done at this point, for all active RF channels, is that the user must click through all the graphs and check that no input signal ever goes beyond the normal operating range of 0 to 24 dBm. If they do, there could be a potential problem and the situation must be reported.

2.3.7 Mount Each RU

With the BU ready for operation, it is time to configure all the RUs. This involves mounting, adjusting parameters, and calibration. Mounting is first.

Mounting is the process by which the system turns on an RU and registers its connection. **Until it is mounted, an RU is dormant** and has no function except self-identification. Mounting an RU turns on its systems, creates a record for the SD port connection, and associates the port with the unique characteristics particular to that combination of cable and RU. After system calibration, this record will also store the connection's calibration information, so recalibration will not be required when an RU is unplugged temporarily (e.g. to hard reset).

Once an RU is mounted, if you plug in a different RU into the same port, ZoneDAS will detect the difference and display a **Mount** button beside the newly connected device. Click it for ZoneDAS to activate the connection to the new RU. As ZoneDAS only remembers one device per SD port, this will also overwrite the previous record with data from the newly plugged in RU/Extender.

Mounting is important because it prevents RU confusion. As each SD port is set with its own output parameters, such as power and pattern, it can be troublesome when an RU gets unplugged and the user forgets where it was plugged into before. With mounting, the system would know if an RU was previously plugged into a particular SD port—and would notify the user, as described above. This helps the user plug each RU back into its place, save confusion, and prevent time-consuming recalibrations.

To mount RUs, go to the *Home screen* and find the blue **Mount** button at each RU's left side, like this:

Figure 14 ZoneDAS Mount button

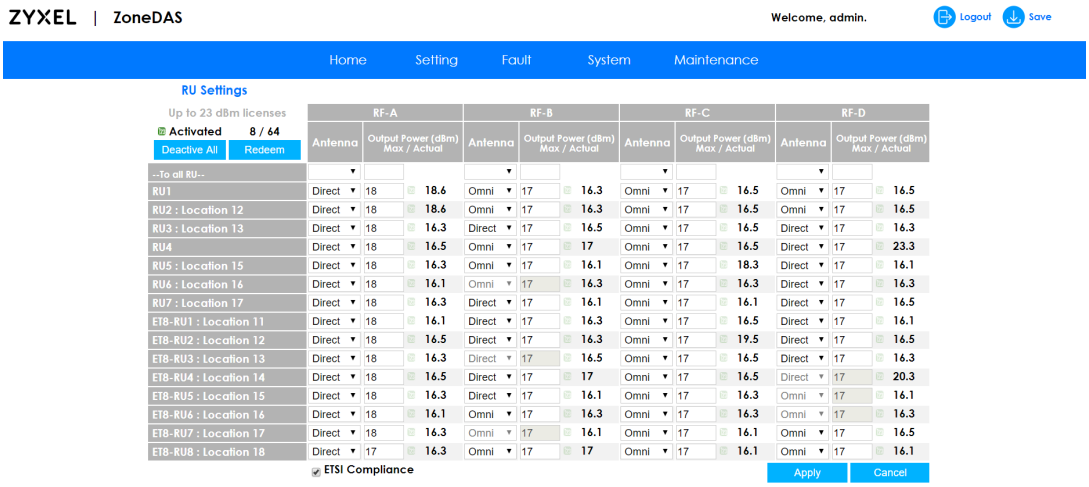
The on-screen line connecting the BU to the RU should be colored **gray**. This indicates an **unmounted state**. Click on **Mount** and wait for the line to turn yellow. Yellow line means the device has been correctly mounted. Once mounted, it becomes possible to configure the RU's parameters. If all the RUs have been plugged in properly, go ahead and click **Mount** for each RU. Once all the lines have turned yellow, proceed to the next section.

2.3.8 Configure RU Parameters

Once an RU has been mounted, it may be necessary to adjust its output parameters. In particular, each RU must be configured for a specific output signal strength and a specific antenna configuration. The default RF output signal strength for RUs is +17 dBm per RF band module, while the default antenna configuration is "Omni". If these are not the desired values for all RUs, it is possible to adjust them from the *RU Settings screen*.

To reach the *RU Settings screen*, click **Setting** from the *Navigation Panel* and select **RU Settings**. The following screen layout will appear:

Figure 15 ZoneDAS RU Settings screen



Like the *BU Configuration screen*, the gray bar at the top of the table shows RF-A to RF-D, from left to right. These correspond to RF modules A, B, C and D. Four identical columns still lie below each of these labels. The difference is, the gray bar at the table's left now lists all the RUs the system can connect to. As each RU has up to 4 RF modules, this table allows one to configure the output of each RF module for each RU.

Output Power is fairly straight forward. Simply enter a value that represents the RU antenna's maximum (*not* constant) RF output. A 17 dBm output would typically service an area that's equivalent to a 25m x 25m open-space zone, while 23 dBm would service an area-equivalent of 50m x 50m. *Antenna* configuration is also simple, with only 2 to choose from. The first, "**Omni**", instructs the antenna to broadcast evenly in all directions. It is perfect for square or round areas, where placing an RU on the **ceiling** at the center of the room creates the best coverage. The second, "**Directional**", instructs the antenna to concentrate its broadcasting in a single direction—through the top of the RU. This configuration is perfect when coverage is desired for a hallway. Simply mount the RU on the **wall** at one end of the hall, and the entire hallway will have signal.

Of course, RU placement would have been determined by now, so simply change the configuration for all RUs to pre-planned values. Note that you can only change values for mounted RUs. Once configuration is done, please press **Apply**.

2.3.9 Turn Service On

At this point, both the BU and RUs should be fully configured. This means the system is ready for activation through turning on Service.

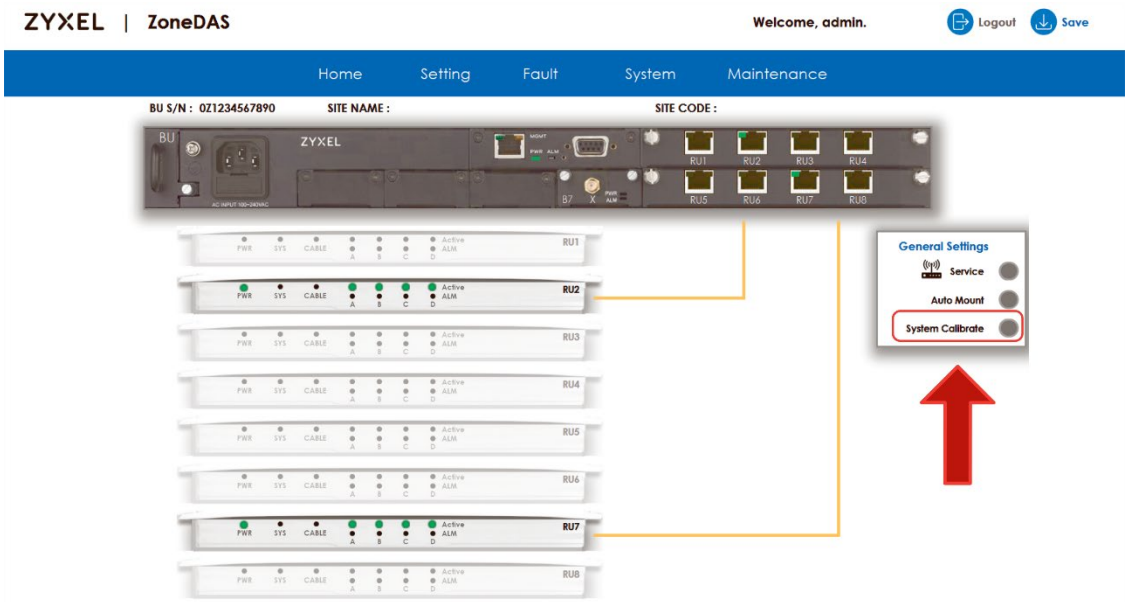
Turning on "Service" allows RF signals into the system for distribution. ON represents the normal working state for a ZoneDAS system. ZoneDAS is effectively "under maintenance" when Service is off.

To turn Service On, simply go to the *Home screen*, locate the box titled **General Settings**, (below the right side of the BU) and click on the top circle, marked **Service**. The circle will light green to indicate that Service is now On.

One important feature of turning Service On is **Calibration**. Calibration fine tunes the system by having it detect the path loss of all RF pathways and adjust internal parameters accordingly, thus achieving ***optimum system performance***. Although ZoneDAS can operate without the benefit of calibration, performance will be affected adversely. Calibration, therefore, is an important part of proper ZoneDAS installation.

As mentioned, simply turning on Service applies a System Calibration. However, if RUs or Extenders get unplugged and re-plugged into different ports without turning off Service, manual calibration may be necessary. Activating System Calibration manually is easy. Simply go to the *Home screen* (by pressing **Home** on the *Navigation Panel*), locate the box titled **General Settings**, (below the right side of the BU) and click on the bottom circle, marked **System Calibrate**, as shown below.

Figure 16 System Calibrate button



Just as the on-screen lines connecting the BU to the RUs turn yellow when each RU is mounted, each line turns green when calibration is complete for that connection—and red when calibration fails there. It is important to ensure that all lines are green by the end of this calibration stage. If a line is not, it may become necessary to check for cable quality/connection or for alarms and resolve them.

Note that the system *will not* operate while it is calibrating! During the half minute or so that the system takes to calibrate everything, it is effectively *under maintenance*. Note also that any unmounted connections will not receive system calibration.

2.3.10 Fill in Descriptive Information

Now that the system is operating, it is time to prepare it for management. The first step, which everyone should do, is to identify all the relevant parts. The second step, only for those who require central management, is to connect to the server. Here let us take care of the first step.

To identify all the relevant parts, we must **give names (and codes) to the BU and all the RUs**. To name the BU, go to the *BU screen* (click on Home and then on the BU), find **Site name and Site code** near the screen's upper left, and fill in their values.

Site name refers to the name of the building that ZoneDAS is servicing. If the building has multiple DAS systems, then name the part of the building this unit services. Example Site names may be: "Costco Milan 1", "Wells Fargo Houston", or "Big Camera Tokyo".

Site codes are like Site names, but in short, coded forms. Using Site codes help central management by providing easy-to-input, structured IDs for each site. Example Site codes for the previous site names might be CCML1F3, WFHTX_ER_34F, or BCTKO123.

Once the values have been filled, click **Apply**.

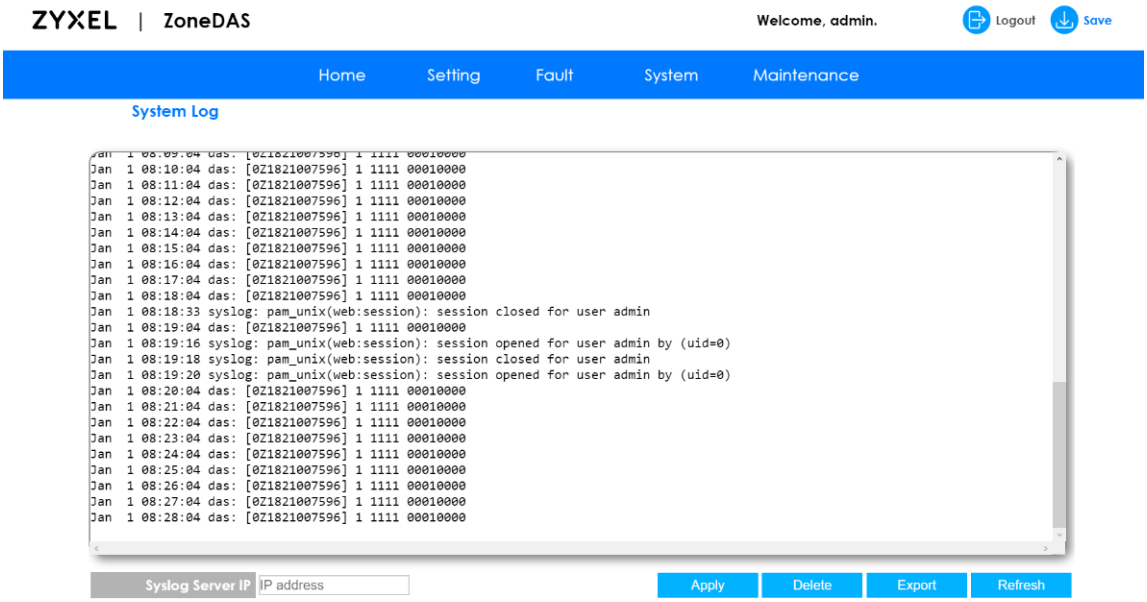
Now let's give names to each RU. RUs are mostly named by their respective location. To name an RU, go to the Home screen and click on an active RU (one that is not grayed out). This will take you to the RU screen. Find **Location** near the screen's upper left corner and fill in its value. Example Location entries for an RU may include "Lobby", "2F Hallway", and "Meeting Room #1". Once the value has been filled, click **Apply** and move on to the next RU.

2.3.11 Set Central Management

if this installation site uses central management, it is time to set the Syslog Server and other parameters. If central management is not required, please skip to the next section.

First, go to **Fault** on the *Navigation Panel*, wait for the menu to appear, and click on **System Log**. This opens the *System Log screen*, as shown below:

Figure 17 SlimDAS System Log screen

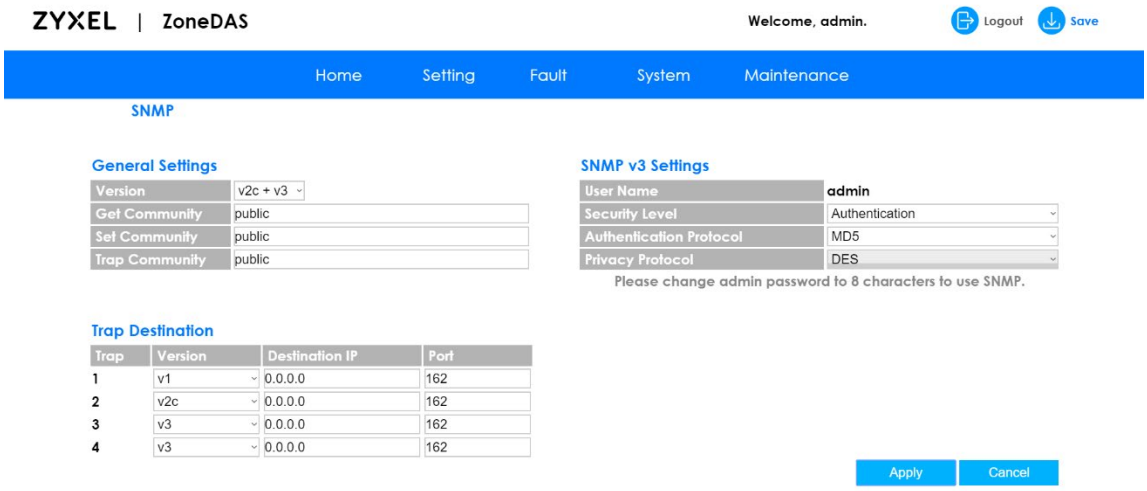


On the bottom of that screen, there is an input box labelled *Syslog Server IP*. Simply input the IP for the central syslog server, click **Apply**, and Syslog Setup is complete! A button labeled "**Export**" is also available for saving the log file onto your client computer as a text file.

Note: The default port for the Syslog Server is 514. To change the port, simply specify the new port after the IP address, using a colon ":" as the separator. For example, if you type in "193.173.20.153:214", then 214 is the port.

Next, mouse to **System** on the *Navigation Panel*, and click **SNMP** from the menu. This opens the *SNMP Screen*, as shown below:

Figure 18 ZoneDAS SNMP screen



The *SNMP screen* has 3 sections for setting up remote management: General Settings, Trap Destination, and SNMP v3 Settings. ZoneDAS supports all SNMP specifications, up to version 3. Simply enter the appropriate information for each of the fields, skipping SNMP v3 Settings if only SNMP version 2 is being used. Once the correct parameters have been entered, click **Apply** and central management setup is complete.

Note: To make SNMP work, it is necessary to have an Administrator password that has 8 characters or more. The default Administrator password only has 4 characters. To change the Administrator password, please refer to Chapter 9.4, User Account Screen.

2.3.12 Save Settings

ZoneDAS is now set up! Please save all the settings that have been made over the previous steps, and backup everything to a configuration file.

Saving settings is easy: simply click on the Save button on the top right of any screen. The Save button looks like this:

Figure 19 The Save button

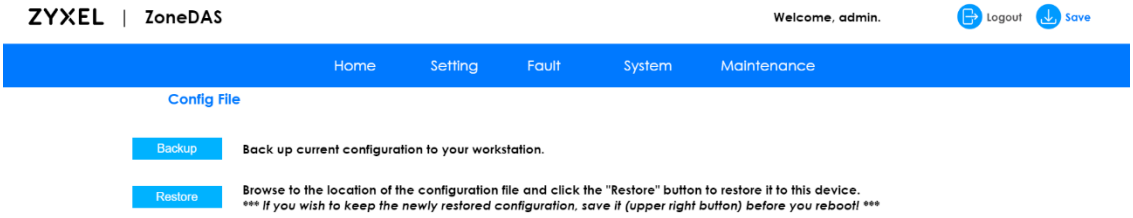
If Save is not clicked, all updated settings will exist only in volatile memory and will disappear upon system reboot.

Once Save is selected, the current settings will transfer to the system's non-volatile memory and still exist after power off or reboot.

2.3.13 Backup Configurations

To backup current configurations to a file, select **Maintenance** from the *Navigation Panel* and click on **Config File**. This opens the Config File screen, shown below. From the Config File screen, click Backup and ZoneDAS will create a backup file in the default download folder, using its Serial Code and Date as part of the file name.

Figure 20 The Config File screen



Once the backup config file has been created, be sure to keep a copy safe for future use. Setting up a system via loading a config file would be far quicker than doing it again from scratch.

CHAPTER 3
The Web Configurator

3.1 Overview

This chapter, along with the five that follow, describe the ZoneDAS Web Configurator in detail, including access, login, and an overview of its functions and interface.

The Web Configurator is an HTML-based management system that allows easy setup and management for ZoneDAS via an Internet browser. It is compatible with Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions, and Google Chrome 26.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator, you need to allow:

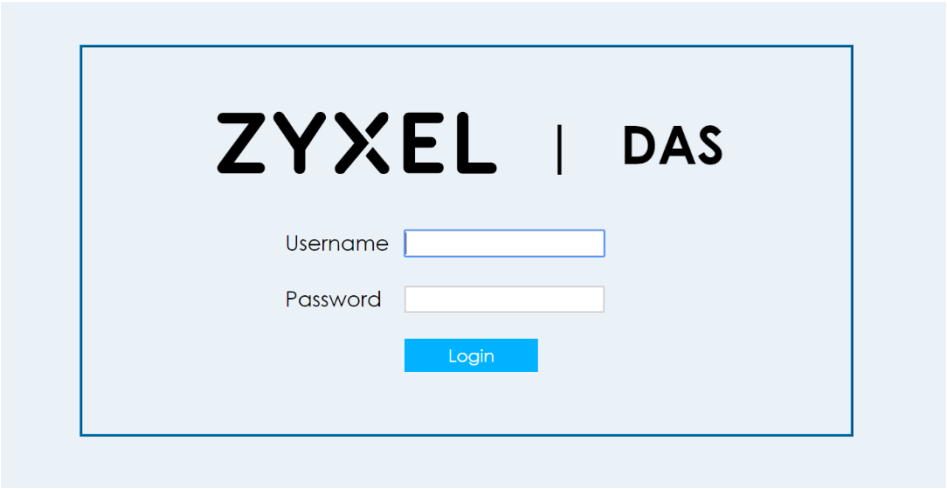
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

3.2 Accessing the Web Configurator

1. Make sure your ZoneDAS hardware is properly connected (refer to the Hardware Installation Guides).
2. Prepare your computer for a wired network device connection. Make sure your computer's IP address is in the same subnet as the BU's IP address. Your computer must be in the same subnet to access this website address. It must also be given a fixed IP address in the range between 192.168.1.3 and 192.168.1.254.

   To prepare for such a connection on a Windows 10 computer, go to Start > Settings > Network & Internet > Ethernet > Change Adapter Options. A new window will open. From there, double click on your Ethernet device, click on Properties, click on the line with (TCP/IPv4), and click Properties. Another new window will open. From there, select "Use the following IP address:" and input 192.168.1.100 under IP address. Windows will fill in 255.255.255.0 under Subnet mask. Click okay and you will be ready. Feel free to close all the configuration windows,
3. Once ready, connect your computer's Ethernet port to the ZoneDAS BU's MGMT port.
4. Launch the web browser and go to *http://192.168.1.1.*
5. The Login screen should appear. To access the Web Configurator and manage ZoneDAS, type the default username: **admin** and password: **1234** in the password screen and click **Login**.

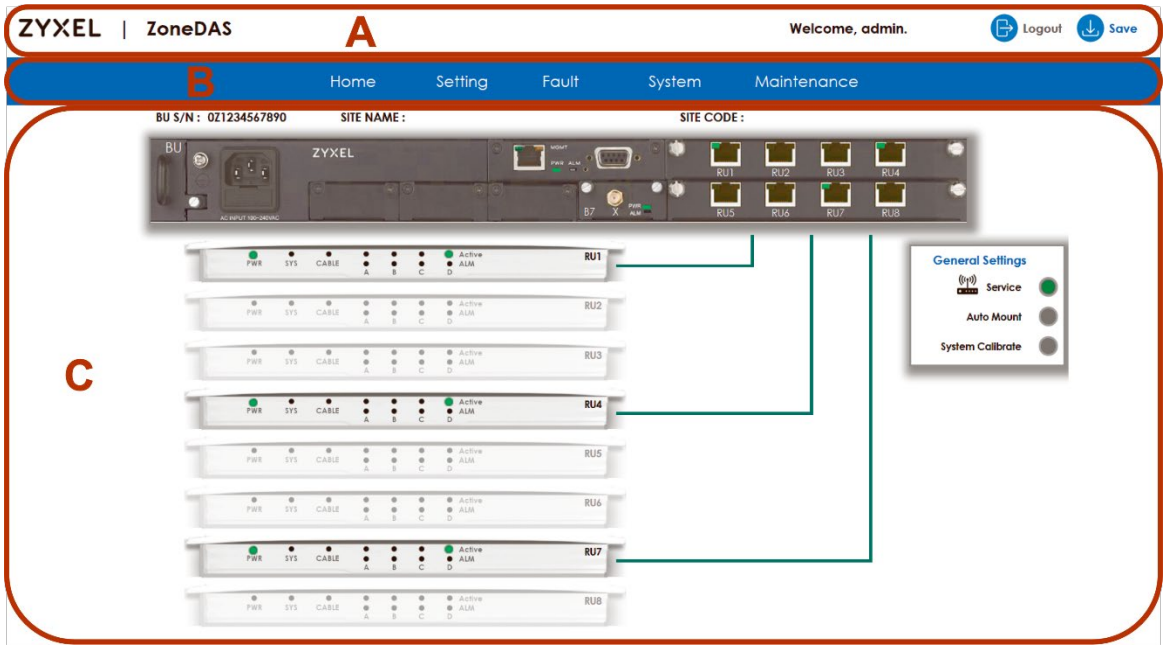
Figure 21 Login screen



3.2.1 The Web Configurator Layout

The Web Configurator is arranged into these parts:

Figure 22 The Web Configurator Layout



A - Title Bar

B - Navigation Panel

C - Main Window

The RUs and/or Extenders shown below the BU are arranged in order of SD port connection, top to bottom. The top RU is the one connected to the first SD port, labeled "RU1", and the bottom RU is the one connected to the last SD port, labeled "RU8". Lines illustrating the BU-RU and/or BU-Extender connections are for illustration only and stop at the BU, but the physical cables do extend to the ports.

See Section 4.2 The Home Screen to learn more about the different colors illustrating the cable connections, plus the Web Configurator's Home Screen.

3.2.2 Title Bar

The title bar allows certain functions, such as the two below, to be available from anywhere in the Web Configurator.

Figure 23 Title Bar functions

The icons provide the following functions:

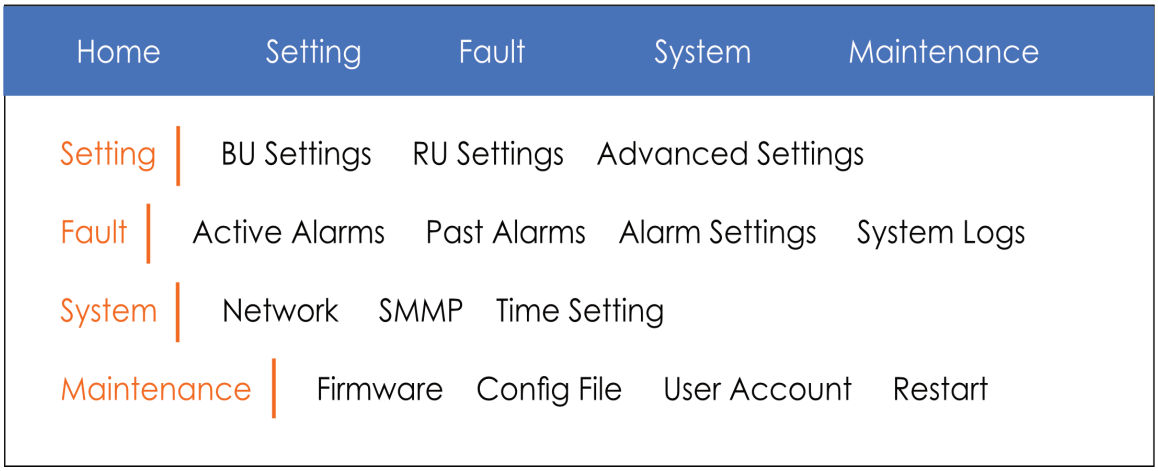
Table 6 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
Save	Click this button to save your configuration in the BU's non-volatile memory. Non-volatile memory retains the configuration of your ZoneDAS even after reboot.
Logout	Click this button to log out of the Web Configurator.

3.2.3 Navigation Panel

Use the sub-menus on the Navigation Panel to configure ZoneDAS's features.

Figure 24 Navigation Panel



The following table describes the sub-menus:

Table 7 Navigation Panel

MENU	SCREEN	FUNCTION
Home	Home	This is the main Web Configurator screen. From here, you can view and monitor each ZoneDAS device and its connection status, including the BU and its connected Extenders / RUs.
	BU	Use this screen to view/modify the BU's basic information, plus monitor each BU-RF's status, downlink system gain, and input power.
	RU1~RU8	Use this screen to view/modify each RU's basic information, plus monitor each RU-RF's status, temperature, and output power.
Setting	BU Settings	Use this screen to configure each BU-RF's connection settings.
	RU Settings	Use this screen to configure each RU-RF's signal output settings.
	Advanced Settings	Use this screen to configure the system's auto leveling settings.
Fault	Active Alarms	Use this screen to view and clear the system's current alarms.
	Past Alarms	Use this screen to view a history of all system alarms. Filters are available by category, severity, etc.
	Alarm Settings	Use this screen to modify each alarm type's severity level, SNMP activation mode, and SNMP alarm delay.
	System Log	Use this screen to view the ZoneDAS system log and to set up the system log server's IP.
System	Network	Use this screen to view and modify the system's VLAN, VPN, and Main Interface (MGMT port) settings.
	SNMP	Use this screen to configure the system's SNMP (Simple Network Management Protocol) settings.
	Time Setting	Use this screen to configure the system's time and date settings.
Maintenance	Firmware	Use this screen to upload and install new firmware for the system's various components.
	Config File	Use this screen to backup or restore system configurations.
	User Account	Use this screen to create and manage up to 8 user accounts via configuring user names, passwords, and privilege levels.
	Restart	Select this to reboot the BU and all connected RUs (not including Extenders). This option may be suitable if and when the system becomes unstable.

CHAPTER 4
Home

4.1 Overview

The **Home** screen is, as the name implies, the starting point from which everything is done in the Web Configurator. As such, it is the screen that appears first after login. Use the **Home** screen to monitor and configure the BU (Base Unit) and its connected Extenders / RUs (Remote Units).

4.1.1 Available Functions

- View each system part's connection status, perform a system-wide calibration, and activate/deactivate service (Section 4.2).
- Access the **BU** screen to monitor the BU's RF modules (Section 4.3).
- Access the **RU** screen to monitor the RU and its RF modules (Section 4.4).

4.2 The Home Screen

The **Home** screen's primary function is to show a map of the system's connections. The LED lights on its illustrated devices are designed to match the physical lights on the actual devices (albeit with some communication delays). The exception is when an RU is configured for LED OFF, in which case the system turns off only the physical LEDs. Check Section 1.3.2 and 1.3.3 for details on BU and RU LED signaling. To open the **Home** screen from anywhere in Web Configurator, just click **Home** on the Navigation Panel (blue bar), as shown below.

Figure 25 ZoneDAS Home Screen

From the **Home** screen, if you move your mouse over an RF module, SD port or its connected RU, the moused-over port or device will be encased in blue. This indicates that you can click on it to reach an expanded screen for the port or device.

If you mouse over any of the lines connecting the RUs / Extenders to the BU, the system will pop up basic information on the connection, such as Cable Loss, Upper Limit (Maximum Allowed Cable Loss), and estimated cable length. The lines are also coded in different colors. These colors indicate the status of each connection, as follows:

Grey: The device is plugged in but not Mounted
Yellow: The device is Mounted but not Calibrated
Green: The device is Calibrated
Red: The device has failed to Calibrate

The following table will explain the different connection statuses mentioned above.

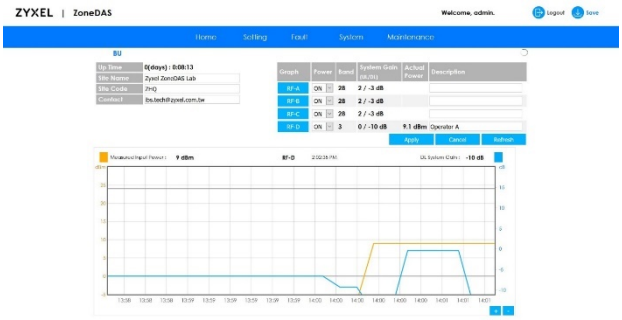
Table 8 Home Screen: Legend

STATUS	DESCRIPTION
BU S/N	This shows the Base Unit's serial number.
Site Name	This shows the Site Name assigned to this ZoneDAS. The Site Name represents system's location and is used for remote management. It may be configured from the BU screen.
Site Code	This shows the Site Code assigned to this ZoneDAS. The Site Code is a shortened, systemized version of the Site Name and is used for remote management. It may also be configured from the BU screen.
General Settings	
Mount	Click the **Mount** button for ZoneDAS to activate the connection to this Extender or RU. Mounting creates a record for the SD port connection. It associates the port with the unique characteristics particular to that combination of cable and RU/Extender. This record stores the connection's calibration information and saves the user from a system-wide calibration whenever an RU is temporarily unplugged (for example, to hard reset by powering off). Once mounted, if you plug in a different RU/Extender into the same port, ZoneDAS will detect the difference and display a Mount button beside the newly connected device. Click it for ZoneDAS to activate the connection to the new RU or Extender. As ZoneDAS only remembers one device per SD port, this will also overwrite the previous record with data from the newly plugged in RU/Extender.
Service **Service**	Turn **Service** on (Green) for the BU to provide RF signals to all connected RUs and Extenders. The BU will only send RF signals to mounted RUs and Extenders (except when Auto Mount is on). Once you have mounted all the RUs and Extenders, click the **Service** light for the BU to start sending RF signals to every device.
Auto Mount **Auto Mount**	Turn **Auto Mount** on (Green) for the BU to automatically activate every SD port connection as they are plugged in. This is useful when you just want to get ZoneDAS working without bothering with creating connection records and doing calibrations. Such a scenario is possible if the RUs are so close together that no RU is stretched closed to its capacity. However, this option is not recommended for normal operations, and proper mounting will enable the system to notify you when an RU is plugged into the wrong port after unplugging and save you from performing a new system calibration.
System Calibrate **System Calibrate**	Click on **System Calibrate** to optimize system performance. During this process the system will detect the path loss of all RF pathways and adjust internal parameters accordingly. ZoneDAS *can* operate without the benefit of calibration, but performance will be adversely affected. Simply turning on **Service** applies a **System Calibration**. However, if RUs or Extenders get unplugged and re-plugged into different ports without turning **Service** off, manual calibration is recommended. Choose an appropriate time for this, as **ZoneDAS must go off-line to perform System Calibration**.

4.3 The BU Screen

Use the **BU** screen to monitor the BU-RF modules' status and input power. Click anywhere on the **Home** screen's BU illustration to open the following screen. Alternatively, click on an RF port to do the same thing and have the bottom graph showing that particular RF port's activities.

Figure 26 BU Screen



The following table describes the labels on the BU screen.

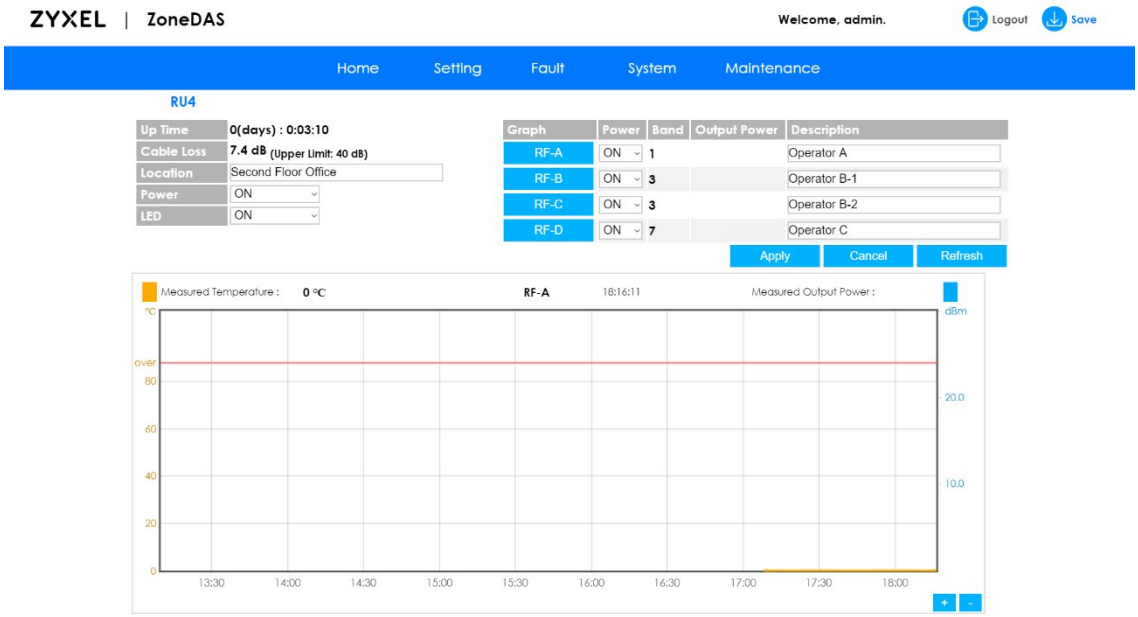
Table 9 BU Screen

LABEL	DESCRIPTION
Left Side Labels	
Up Time	This shows how long the BU has been operating for.
Site Name	Here you may name the system's location, for remote management.
Site Code	Here you may create a code for the Site Name.
Contact	Here you may enter the contact info for your supplier or repair facility.
Right Side Labels	
Graph	Click on an RF module name to have the graph below show the input power curve for the module's signal source (shown in yellow) and the corresponding downlink system gain (shown in blue).
Power	Use this to control the ON/OFF status of each BU-RF module. It is possible to power on a slot without filling it with a module, and vice versa.
Band	This displays the RF signal's transmission frequency band.
System Gain (UL/DL)	System Gain represents the ZoneDAS system's overall gain (BU and RU) and is calculated as follows: • UL (Uplink) Gain = BU-RF port's output power - RU-RF port's input power. • DL (Downlink) Gain = RU-RF output power - BU-RF port's input power.
Actual Power	This is the actual measured signal strength for the signal coming into the RF module.
Description	Enter a description or note related to this RU-RF module or its signal. Often-used descriptions include the operator name for that signal and the frequency band for that channel.
Buttons	
Apply	Click **Apply** to save your changes to the BU's run-time memory. The memory is volatile and loses changes when it's turned off or loses power, so use the **Save** button on the Title Bar to save your changes to the non-volatile memory once configuration is complete.
Cancel	Click **Cancel** to lose all changes made after last clicking **Apply**. The screen will refresh from the BU's run-time memory.
Refresh	Click **Refresh** to update the information on this screen.

4.4 The RU Screen

Use the **RU** screen to view the RU's status and its RF modules' output power and temperature. Choose an RU by clicking on its picture in the **Home** screen, and the following screen will appear.

Figure 27 Home > RU



The following table describes the labels on the RU screen.

Table 10 Home > RU

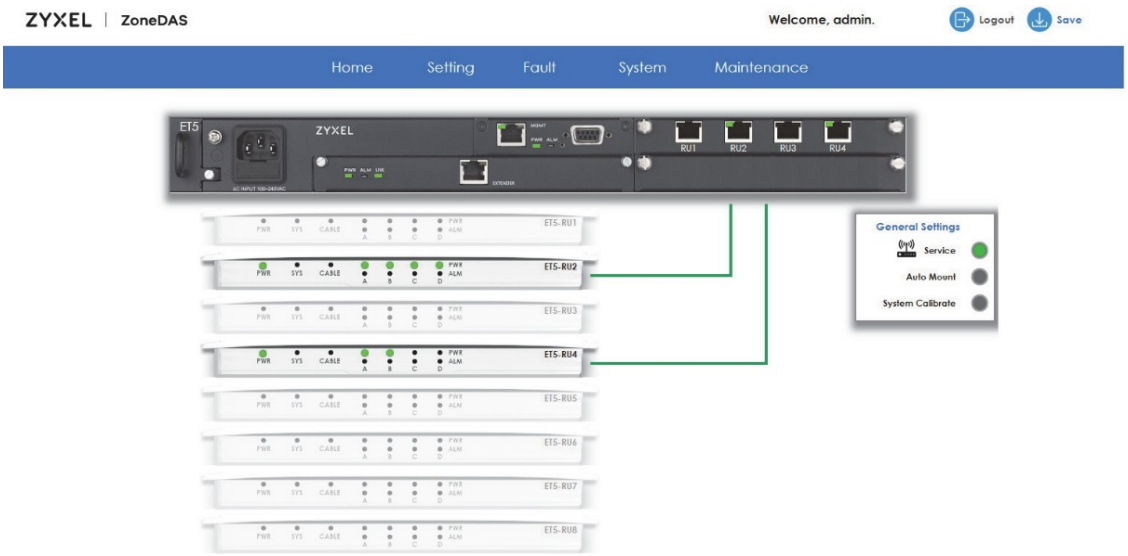
LABEL	DESCRIPTION
RU Name • RU1 ~ RU8 • ET1-RU1 ~ ET8-RU8	This identifies the RU on screen and is displayed in blue. RUs plugged directly into the BU are labeled RU1~RU8. RUs plugged into Extenders are labeled ET1-RU1~ ET8-RU8, where the number after "ET" is the number assigned to the BU-SD slot that connects the Extender.
Left Side Labels	
Up Time	This field displays how long the RU has been running since its last reboot or power-on.
Cable Loss	This displays the amount of cable loss over the BU↔RU or Extender↔RU connection. Cable loss increases with cable length and can be magnified by poor quality or damaged cable. Given proper cabling, ZoneDAS has effectively no BU↔Extender cable loss.
Location	Enter a descriptive name for this RU's location. e.g. Grand Lobby, 2nd Floor East Wing, Central Courtyard
Power	Select **ON** to power on the RU. Select **OFF** and the system will cut its power supply to the RU.
LED	Select **Turn ON** to activate the LED signal lights that are physically on the RU. Select **Turn OFF** to deactivate all physical signal lighting on this RU. In this mode, the physical LEDs will remain off even during alarm states, but the virtual LEDs in the Web Configurator will stay on and provide information.
Right Side Labels	
Graph	Here the system displays each RF module installed in this RU. Select a module (RF-A to RF-D) to display a graph showing its temperature and output power through time. The labeled axis for temperature is on the left; the labeled axis for output power is on the right.

LABEL	DESCRIPTION
Power	This shows the power status of each RU-RF module/slot. Select **ON** or **OFF** to turn that module ON or OFF. The system does this by supplying or cutting power to the RF module's slot. It is therefore possible to turn power on even for empty slots.
Band	This shows the frequency band currently used by the RU-RF.
Output Power	This shows the current actual output power of this RU-RF module.
Description	Enter a description or note related to this RU-RF module.
Buttons	
Apply	Click **Apply** to save your changes to the BU's run-time memory. The memory is volatile and loses changes when it's turned off or loses power, so use the **Save** button on the Title Bar to save your changes to the non-volatile memory once configuration is complete.
Cancel	Click **Cancel** to lose all changes made after last clicking **Apply**. The screen will refresh from the BU's run-time memory.
Refresh	Click **Refresh** to update the information on this screen.

4.5 The Extender Screen

If you have connected one or more Extenders to ZoneDAS, it will show up on the **Home** screen (Section 4.2). There you will see all your connected Extenders, alongside all the RUs that are directly connected to the BU. Click on an Extender to access the **Extender Screen**. It allows you to access all the RUs connected to that Extender, and it looks like this:

Figure 28 Home > Extender



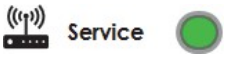
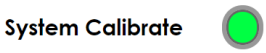
The Extender screen looks a lot like the **Home** screen, as it is basically the same screen. The difference is that it replaces the BU with the Extender—and the BU's RUs with the Extender's RUs. It also behaves in the same way, so you can access the **RU Screen** for an RU simply by clicking on that RU (or the SD port it's connected to).

In effect, the Extender is a subsidiary BU. From the **Extender Screen**, you may access the RUs connected to that Extender—and only those RUs. To go back to the **Home** screen, where you will see the BU and other Extenders/RUs, simply click **Home** from the Navigation Panel.

Note: You cannot connect an Extender to another Extender (cascading Extenders is not supported).

The General Settings box on the right looks and works just like it does in the **Home** screen. As such, anything you do there is universal and applies to the entire ZoneDAS system. The following table describes all the labels on the Extender screen.

Table 11 Extender Screen

STATUS	DESCRIPTION
Mount	Click the **Mount** button for the Extender to activate this RU connection. See Section 4.2 The Home Screen for more on Mounting. The Extender, like the BU, will only remember one device per SD port. Once a new device has been mounted, the Extender will clear all stored parameters for the previously connected device.
General Settings	
Service  	Turn **Service** on (Green) for the system to provide RF signals to all connected RUs. The Extender, like the BU, will only send RF signals to mounted RUs. Once you have mounted all the RUs, click the round **Service** button to start sending them RF signals.
Auto Mount 	Turn **Auto Mount** on (Green) for the system to automatically activate every SD port connection, system wide. See Section 4.2 The Home Screen for more on the Auto Mount feature.
System Calibrate  	Click on **System Calibrate** to optimize system performance. During this process the system will detect the path loss of all RF pathways and adjust internal parameters accordingly. ZoneDAS *can* operate without the benefit of calibration, but performance will be adversely affected. Simply turning on **Service** applies a **System Calibration**. However, if RUs or Extenders get unplugged and re-plugged into different ports without turning **Service** off, manual calibration is recommended. Choose an appropriate time for this, as **ZoneDAS must go off-line to perform System Calibration**.

CHAPTER 5 SETTING

5.1 Overview

The **Setting** menu is used to configure the BU and its connected RUs. Once you have set up all the parameters in both the **BU Settings** and **RU Settings** screens, your ZoneDAS will be up and running.

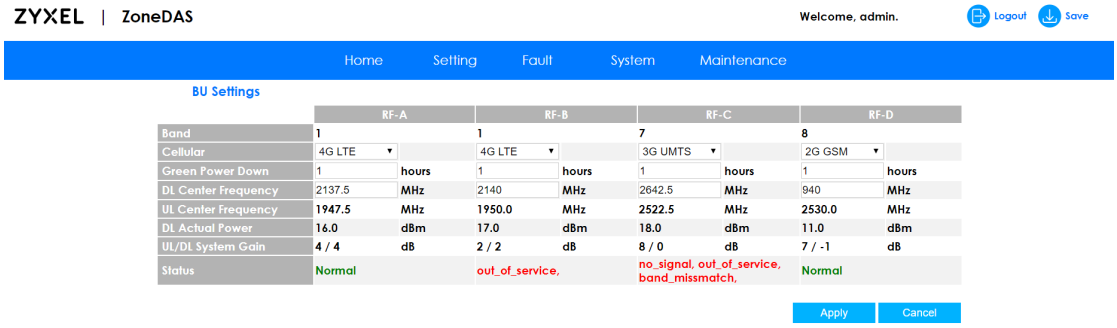
5.1.1 Available Functions

- Use the **BU Settings** screen to configure the BU's connection settings (Section 5.2).
- Use the **RU Settings** screen to configure the RU's connection settings (Section 5.3).
- Use the **Advanced Settings** screen to configure the system's Auto Leveling settings (Section 5.4).

5.2 The BU Settings Screen

Use the **BU** screen to configure the BU's connection settings and allow ZoneDAS to properly transmit/ receive information to and/from the operator's BTS (Base Transceiver Station). Click **Setting > BU Settings** to open the following screen.

Figure 29 Setting > BU Settings



	RF-A		RF-B		RF-C		RF-D	
Band	1		1		7		8	
Cellular	4G LTE		4G LTE		3G UMTS		2G GSM	
Green Power Down	1	hours	1	hours	1	hours	1	hours
DL Center Frequency	2137.5	MHz	2140	MHz	2642.5	MHz	940	MHz
UL Center Frequency	1947.5	MHz	1950.0	MHz	2522.5	MHz	2530.0	MHz
DL Actual Power	16.0	dBm	17.0	dBm	18.0	dBm	11.0	dBm
UL/DL System Gain	4 / 4	dB	2 / 2	dB	8 / 0	dB	7 / -1	dB
Status	Normal		out_of_service,		no_signal, out_of_service, band_missmatch,		Normal	

Apply Cancel

The following table describes the labels on the BU Settings screen.

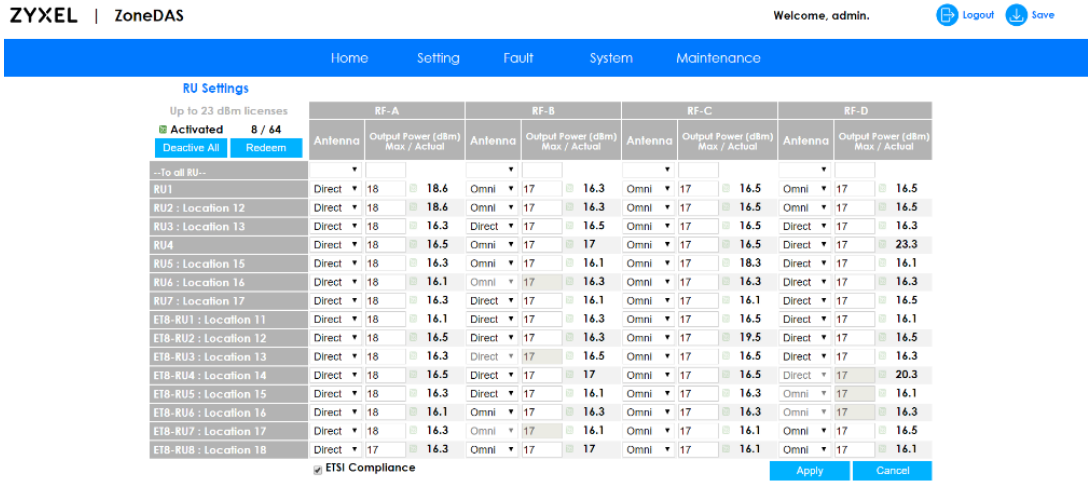
Table 12 Setting > BU Settings

LABEL	DESCRIPTION
Left Column Labels	
Band	This field displays the frequency band used by the RF module, as detected by the BU.
Cellular	Select the mobile technology (as supported by the BTS) used by this RF module for connection. Choose from 2G/3G/4G. If the information cannot be obtained, then choose Auto.
Green Power Down	This is the power saving mode offered by ZoneDAS. It enables an RF channel to "go to sleep" if the channel has received no input signal for a time. The default of 0 indicates that the function is disabled. To enable the function, enter a positive integer. This will be the number of hours the system would wait under no signal conditions before switching the channel to power-saving mode. If a signal appears while a channel is under Green Power Down, the system will power the channel back up again.
DL Center Frequency	Enter the "center frequency" of the frequency band used by this RF module for downlink transmission. For example, if we want the module to use operate within a 20 MHz band from 1830 MHz to 1850 MHz, the middle point between these figures is 1840, and that would be the "center frequency" one should enter.
UL Center Frequency	Here the system displays the center frequency of the frequency band used by this RF module for uplink transmission. The system calculates this value based on all the other parameters it has obtained, so the user does not need to enter it directly.
DL Actual Power	This displays the maximum signal strength that has actually been received by the RF module from the operator's BTS (Base Transceiver Station).
UL/DL System Gain	UL/DL System Gain is the overall ZoneDAS gain (BU and RU), and is calculated as follows: • UL (Uplink) System Gain = BU-RF port's output power - RU-RF's input power. • DL (Downlink) System Gain = RU-RF port's output power - BU-RF's input power.
Status	This row shows the current connection status for each of the four RF modules. • Normal: Indicates that the inserted RF module is working normally. • Alarm: Indicates an alarm is on. Instead of displaying "Alarm", the system will directly display the alarm code. The user may go to the **Fault > Active Alarms** to see more details about the problem.
Buttons	
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to lose all changes made after last clicking **Apply**. The screen will refresh from the BU's run-time memory.

5.3 The RU Settings Screen

Use the **RU Settings** screen to display and configure antenna or power settings for each and every connected RU, including both direct and via-Extender connections. Click **Setting > RU Settings** to see the following screen layout.

Figure 30 Setting > RU Settings



The following table describes the labels on this screen.

Table 13 Setting > RU Setting

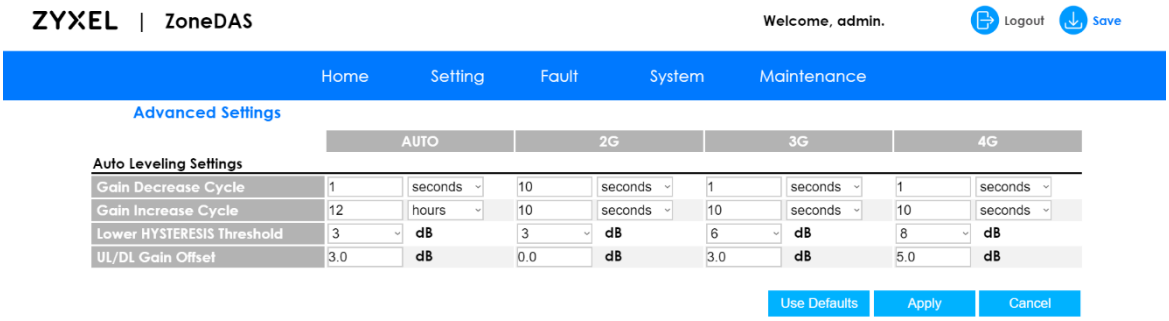
LABEL	DESCRIPTION
Left Column Labels	
--To all RU--	When a selection is made to a drop-down list to the right of this label, that selection will be applied to all drop-down lists under it. This means the selection will be applied to all RUs.
RUx : Location ## ETy-RUz : Location ##	All connected RUs are identified by a simple code: • RU1 ~ RU8 represent the 8 possible RUs connected directly to the BU, from SD port 1 to SD port 8. • ET1 ~ ET8 represent the 8 possible Extenders connected directly to the BU, from SD port 1 to SD port 8. • ET1-RU1 ~ ET1-RU8 represent the 8 possible RUs connected to ET1's ports, from SD port 1 to SD port 8. "Location" simply refers to the user-input description of where each RU is located.
Upper Row Labels	
RF-A to RF-D	**RF-A** to **RF-D** represent the 4 RF modules in the BU. An RF module is used to connect the BU to the operator's BTS.
Antenna	Choose an antenna type for this RU-RF to use: **Omni** for surround coverage or **Direct** for directional coverage.
Output Power (dBm) Max / Actual	This is where the user sets the maximum output power each RF module in each RU. Under **Max**, enter the greatest allowed output power from each RU-RF. Increasing this value expands coverage, while lowering it reduces interference. **Actual** shows the current actual output power from this RU.
ETSI Compliance	Select this to limit output power to 13 dBm for RUs using GSM Band 8.
Buttons	
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to lose all changes made after last clicking **Apply**. The screen will refresh from the BU's run-time memory.

5.4 The Advanced Settings Screen

Use the **Advanced Settings** screen to configure Auto Levelling for the BU. "Auto-Levelling" is an intelligent algorithm that ZoneDAS uses to adapt to widely varying, unpredictable input signal strengths. **Through Auto-Levelling, ZoneDAS is able to maintain a stable and optimal output signal pattern despite changes to input signal strengths from Base Transceiver Stations**. Default settings of this smart algorithm have been determined during extensive field-operations and are adapted in function of technology and modulation schemes.

Click **Setting > Advanced Settings** to open the following screen.

Figure 31 Setting > Advanced Settings



Advanced Settings represent internal parameters that the system uses for signal optimization. They are not meant for manual adjustment and it is recommended that the user simply choose **Use Defaults** for all values. If for any reason you wish to adjust these values, please consult Zyxel using the Customer Support contact information behind the front page of this Guide.

CHAPTER 6
FAULT

6.1 Overview

The **Fault** screen allows the user to monitor and control all alarm-related functionality. These include the monitoring of current and past alarms, the configuration of security level for each alarm, and the System Log, which records all events and alarms.

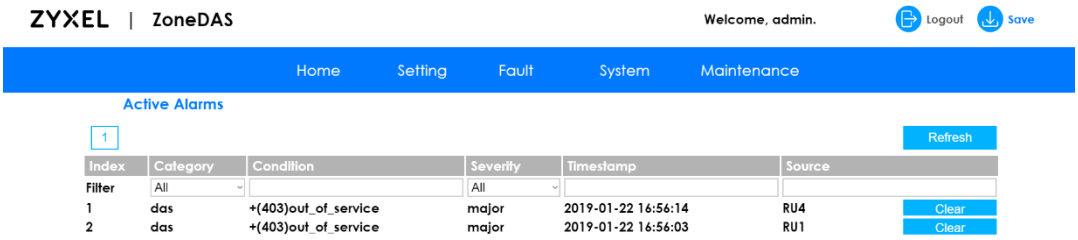
6.1.1 Available Functions

- Use the **Active Alarms** screen to view, filter, and search for active alarms (Section 6.2).
- Use the **Past Alarm** screen to view, filter, and search for past alarms (Section 6.3).
- Use the **Alarm Settings** screen to modify the severity classification of alarms (Section 6.4).
- Use the **System Log** screen to access and view the ZoneDAS System Log (Section 6.5).

6.2 The Active Alarms Screen

An alarm is how ZoneDAS notifies that something noteworthy has happened or gone wrong (for example, the connection between a BU and an RU has been lost). An alarm about something that is still in effect is called an active alarm, which an alarm that has been cleared is called a past alarm. The **Active Alarms Screen** shows all the active alarms that currently exist. Click **Fault > Active Alarms** to access it, which looks like the following.

Figure 32 Fault > Active Alarms



The following table describes the labels on this screen.

Table 14 Fault > Active Alarms

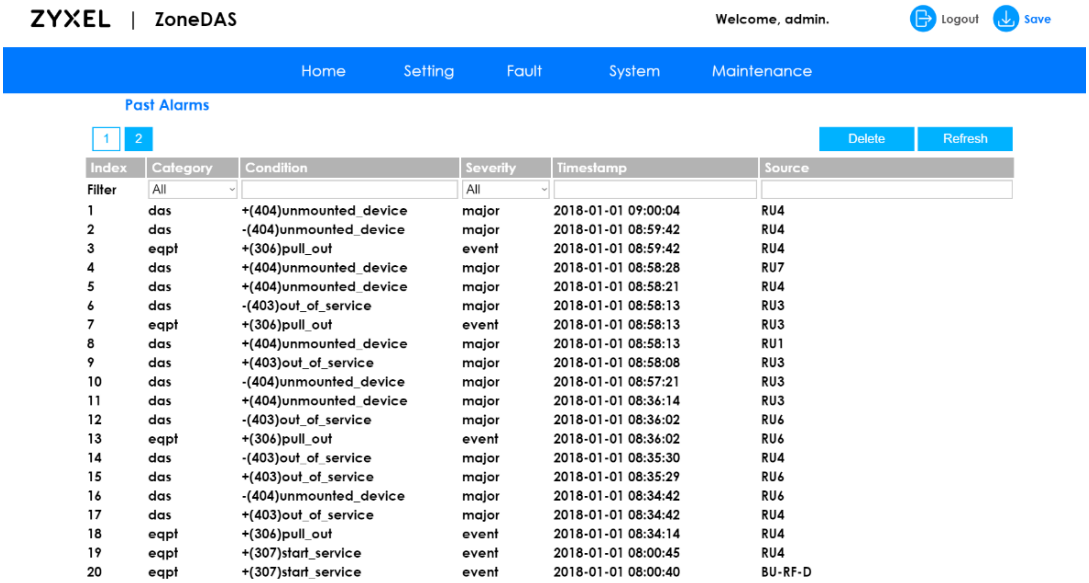
LABEL	DESCRIPTION
Index	This is the index number for the active alarm.
Category	Select the system partition for which you wish to display active alarms. • **mgmt** - include alarms from the BU-MB. • **eqpt**- include *hardware* alarms from the BU-SD, BU-RF, RU-RF, RU-MB. • **das** - include *software* alarms from the BU-SD, BU-RF, RU-RF, RU-MB. • **All** - include all alarms from the entire ZoneDAS system.
Condition	This allows you to filter active alarms by condition. Enter the condition you want to search for. See List of Alarm Conditions for more information on the various alarm conditions.
Severity	This allows you to filter active alarms by severity. Select the severity level of the active alarm you want to search for. ZoneDAS then searches for all alarms of that severity or higher. See Alarm Severity Levels for more information on event severity.
Timestamp	This allows you to filter active alarms by time and date. Enter the day and time to filter alarms by time of occurrence. For example, if you want to show active alarms for January 22, 2019, you would type "2019-01-22". If you want to see all alarms between 7pm and 8pm, you would type "19:" If you follow that with 26, for "19:26", you would see all alarms from 7:26pm.
Source	Enter the name of the system partition for which you wish to locate active alarms. Refer to Table 1: BU System Parts and Table 3: RU System Parts to learn more about the various system partitions on ZoneDAS.
Clear	Click the **Clear** button at the right end of an alarm listing to remove it. If the **Clear** button is missing, it means the alarm cannot be removed.
Refresh	Click **Refresh** button to search the system again for new or remaining alarms.

Note: ZoneDAS can store up to 4096 active alarm entries. Once it reaches the limit, each new entry overwrites the oldest one.

6.3 The Past Alarms Screen

Use the **Past Alarms** screen to view all the alarms that are no longer active. Click **Fault > Past Alarms** to open the following screen.

Figure 33 Fault > Past Alarms



Index	Category	Condition	Severity	Timestamp	Source
Filter	All		All		
1	das	+(404)unmounted_device	major	2018-01-01 09:00:04	RU4
2	das	-(404)unmounted_device	major	2018-01-01 08:59:42	RU4
3	eqpt	+(306)pull_out	event	2018-01-01 08:59:42	RU4
4	das	+(404)unmounted_device	major	2018-01-01 08:58:28	RU7
5	das	+(404)unmounted_device	major	2018-01-01 08:58:21	RU4
6	das	-(403)out_of_service	major	2018-01-01 08:58:13	RU3
7	eqpt	+(306)pull_out	event	2018-01-01 08:58:13	RU3
8	das	+(404)unmounted_device	major	2018-01-01 08:58:13	RU1
9	das	+(403)out_of_service	major	2018-01-01 08:58:08	RU3
10	das	-(404)unmounted_device	major	2018-01-01 08:57:21	RU3
11	das	+(404)unmounted_device	major	2018-01-01 08:36:14	RU3
12	das	-(403)out_of_service	major	2018-01-01 08:36:02	RU6
13	eqpt	+(306)pull_out	event	2018-01-01 08:36:02	RU6
14	das	-(403)out_of_service	major	2018-01-01 08:35:30	RU4
15	das	+(403)out_of_service	major	2018-01-01 08:35:29	RU6
16	das	-(404)unmounted_device	major	2018-01-01 08:34:42	RU6
17	das	+(403)out_of_service	major	2018-01-01 08:34:42	RU4
18	eqpt	+(306)pull_out	event	2018-01-01 08:34:14	RU4
19	eqpt	+(307)start_service	event	2018-01-01 08:00:45	RU4
20	eqpt	+(307)start_service	event	2018-01-01 08:00:40	BU-RF-D

The following table describes the labels on this screen.

Table 15 Fault > Past Alarms

LABEL	DESCRIPTION
Index	This is the index number for the past alarm.
Category	Select the system partition for which you wish to display past alarms. • mgmt - include alarms from the BU-MB. • eqpt- include *hardware* alarms from the BU-SD, BU-RF, RU-RF, RU-MB. • das - include *software* alarms from the BU-SD, BU-RF, RU-RF, RU-MB. • All - include all alarms from the entire ZoneDAS system.
Condition	This allows you to filter past alarms by condition. Enter the condition you want to search for. See List of Alarm Conditions for more information on the various alarm conditions.
Severity	This allows you to filter past alarms by severity. Select the severity level of the past alarm you want to search for. ZoneDAS then searches for all alarms of that severity or higher. See Alarm Severity Levels for more information on event severity.
Timestamp	This allows you to filter past alarms by time and date. Enter the day and time to filter alarms by time of occurrence. For example, if you want to show past alarms from January 22, 2019, you would type "2019-01-22". If you want to see past alarms that have occurred between 6pm and 7pm every day, you would type "18:" If you follow that with 18, for "18:18", you would see all alarms from 6:18pm.
Source	Enter the name of the system partition for which you wish to locate active alarms. Refer to Table 1: BU System Parts and Table 3: RU System Parts to learn more about the various system partitions on ZoneDAS.
Delete	Click the **Delete** button at the top right end to clear the log of all past alarms.
Refresh	Click the **Refresh** button to show all remaining past alarms.

Note: ZoneDAS can store up to 4096 past alarm entries. Once it reaches the limit, each new entry will overwrite the oldest one.

6.4 The Alarm Settings Screen

The **Alarm Settings** screen allows the user to view the alarm definition table and modify alarm severity classifications. It gives a listing of all alarms, ordered by category, and lets the user configure each alarm's various parameters. To access this screen, click **Fault > Alarm Settings**.

Figure 34 Fault > Alarm Settings

The following table describes the labels on this screen.

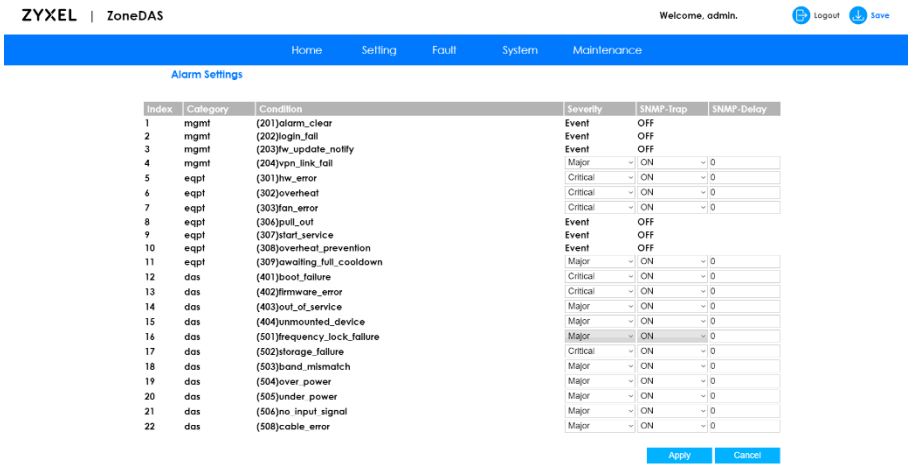


Table 16 Fault > Alarm Settings

LABEL	DESCRIPTION
Index	This is the index number of the alarm.
Category	This column shows the categorization of each alarm. • **DAS** – refers to software alarms from BU-RF, BU-SD, RU-RF, and RU-MB. • **Equipment** – refers to hardware alarms from BU-RF, BU-SD, RU-RF, and RU-MB. • **Management** – refers to alarms from the BU-MB
Condition	This column contains a simplified description of each alarm. See List of Alarm Conditions for more information on the various types of alarms.
Severity	This is where the user can set the severity classification for all instances of this alarm. See Alarm Severity Levels for more information on alarm/event severity types.
SNMP-Trap	Select ON from this drop-down list to send alarms of this type through the SNMP trap. Select OFF to stop the system from sending SNMP traps for alarms of this type.
SNMP-Delay	If SNMP-Trap is set to ON for an alarm, the SNMP-Delay tells the system how long to wait (in minutes) before a trap is actually sent for this alarm. This is useful for preventing false alarms, such as when a cable is unplugged and immediately re-plugged. This is also useful for preventing central management from receiving a deluge of alarms while a technician is doing work with ZoneDAS on-site.
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to remove all changes made since last clicking **Apply** and reconfigure the screen afresh.

6.4.1 Alarm Severity Levels

ZoneDAS Alarms are categorized into the following:

Table 17 Alarm Severity Levels

SEVERITY	DESCRIPTION
Event	An Event is a notification message and requires no action.
Warning	An alarm of this type may require action. This severity type can also be used to indicate a condition that should be noted (logged) but does not require direct action.
Minor	An alarm of this type indicates that a ZoneDAS device (a service, a port, a power supply, etc.) has stopped functioning and needs attention.
Major	A major alarm indicates that device is completely down or in danger of going down. This type of problem must be addressed immediately.
Critical	A critical alarm is one that has destabilized numerous devices on the network. All available staff should stop what they are doing and focus on fixing the problem.

Note: These represent the factory default Alarm Severity Levels. You can modify the severity of any alarm based on what is you feel is appropriate for your scenario.

6.4.2 List of Alarm Conditions

The following table describes all the alarms, conditions, and notifications that may occur within ZoneDAS.

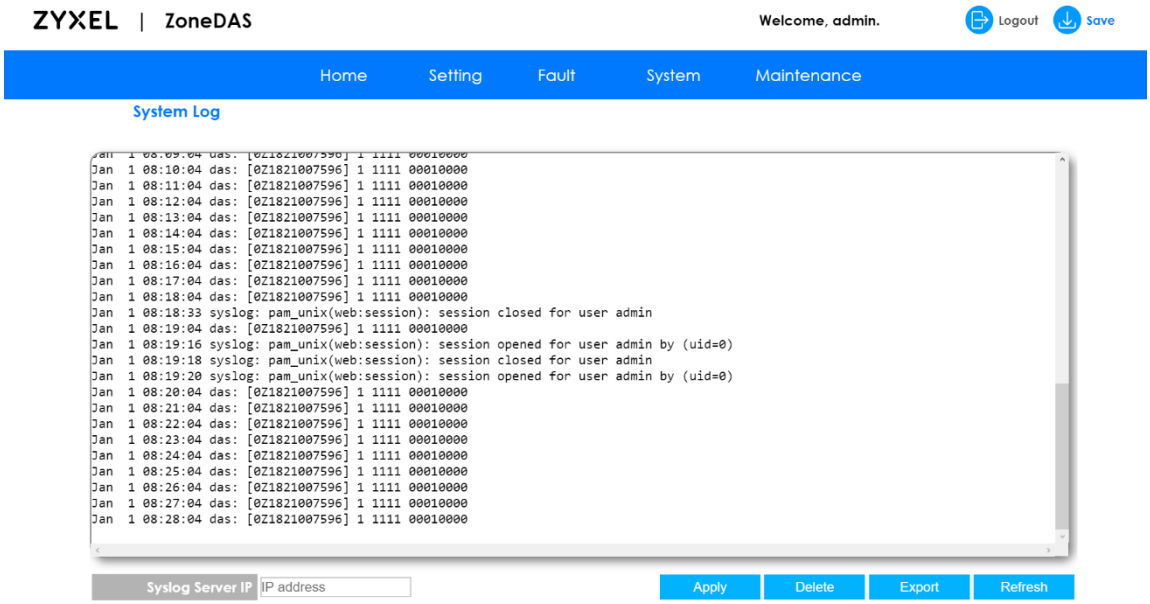
Table 18 Alarm Conditions

ALARM CONDITION	DESCRIPTION
DAS	
band_mismatch	The frequency band in the RF module does not match the configured frequency band.
boot_failure	A module failure has been detected during boot. The module has been identified along with the error, under **Source**. If multiple modules fail, then multiple **boot_failure** entries will appear, each with different descriptions under **Source**.
firmware_error	This error indicates that a particular module's firmware needs an update or has an error. The module's name is listed under **Source**.
frequency_lock_failure	The RF module cannot detect or lock the operator's frequency band. This may mean that the setup frequency is incorrect or that no signal is detected from the BTS.
gain_changed	This means the system's uplink/downlink system gain has changed.
no_input_signal	A BU-RF module cannot detect a signal from its signal source.
out_of_service	The module is out of service and is not responding to the BU.
over_power	If the alarm source is the BU, this means the input power has exceeded 26 dBm. If it is an RU, this means the output power has exceeded 26 dBm. In either case, the device is under threat of damage from an exceedingly strong signal.
power_calibration_failure	A calibration process has failed.
storage_failure	A module cannot access its non-volatile memory.
unmounted_device	The system detects an unmounted Extender or RU. Please mount all connected devices.
Equipment	
awaiting_full_cooldown	An RU-RF module has overheated despite overheat prevention and the system has shut down the module for cooldown.
bu_fan_error	ZoneDAS detects a fan speed threshold violation in the BU.
bu_overheat	ZoneDAS detects a temperature threshold violation in the BU.
extender alarm	A connected Extender has raised an alarm for either itself or one of its connected RUs.
overheat_prevention	An RU-RF module is getting too hot and the system has reduced its power output to prevent overheating.
hw_monitor_fail	There is a hardware monitoring failure.
pull_out	A BU-RF or BU-SD module has been removed.
ru_fan_error	ZoneDAS detects a fan speed threshold violation in the RU.
rf_module_overheat	Too much of the RU has overheated and the system has shut down the entire RU.
start_service	A module is ready to start service.
Management	
alarm_cear	An alarm has been manually cleared.
fw_upgrade_notify	ZoneDAS has entered a firmware update process.
login_fail	There was a system login failure.
out_of_memory	The BU or Extender is close to using up its system memory.
vpn_link_fail	Cannot connect to Virtual Private Network (VPN). Please check VPN settings.

6.5 The System Log Screen

ZoneDAS keeps a comprehensive log of all system activities, notifications, warnings and alarms. The log is invaluable for troubleshooting and can be accessed both locally and remotely via the **System Log screen**. There you can see the log directly and optionally specify a remote Syslog Server where ZoneDAS will send all its system log entries. To see the **System Log screen**, click **Fault > System Logs** to open the following screen.

Figure 35 Fault > System Logs



The following table describes the labels on this screen.

Table 19 Fault > System Log

LABEL	DESCRIPTION
Syslog Server IP	Enter the IP address of the Syslog Server that will remotely store this system log. To specify the port for the Syslog Server, simply follow the **IP address with a colon and the port number**. File format used for sent files is IETF (RFC 5424). Secure Socket Layers (SSL) is not supported at this point. But one can have ZoneDAS reach its Syslog Server through OpenVPN to secure all messages. ZoneDAS currently supports UDP and not TCP.
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the Title Bar to save your changes to the non-volatile memory when you are done configuring.
Delete	Click **Delete** to delete all entries in the system log.
Export	Click **Export** to save the system log to a text file. A window will pop up for the user to name the text file, then the file will be saved to the system's default download directory.
Refresh	Click **Refresh** to renew this screen.

CHAPTER 7
System

7.1 Overview

This chapter describes the screen and options that can be found under the Web Configurator's System menu. The System menu, as the name implies, is the doorway to general system configurations in ZoneDAS. They let the user control how ZoneDAS can be accessed, including options for VPN and SNMP. They also allow the user to set a very important system parameter: time.

7.1.1 Available Functions

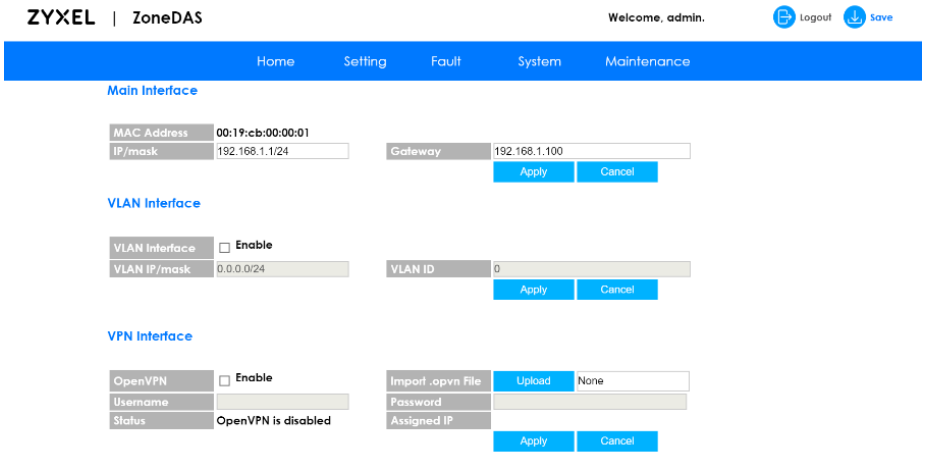
- Use the **Network** screen to configure the 3 main ways to access ZoneDAS (Section 7.2).
- Use the **SNMP** screen to configure SNMP options and setting for central management (Section 7.3).
- Use the **Time Setting** screen to configure time and date settings, including time zones and Daylight-Saving Time (Section 7.4).

7.2 The Network Screen

The **Network** screen is where the user can configure the 3 main ways to access Web Configurator in ZoneDAS: Main, VLAN, and VPN. The Main Interface refers to the default method, where the user connects a CAT5 cable directly from the ZoneDAS MGMT port to the user's computer console. The VLAN Interface refers to accessing ZoneDAS through Virtual LAN. The VPN Interface refers to accessing ZoneDAS through a Virtual Private Network. These two latter options represent the ZoneDAS system's remote access options.

To access the Network screen, simply click **System > Network**, as per below.

Figure 36 System > Network



The following table describes the labels on this screen.

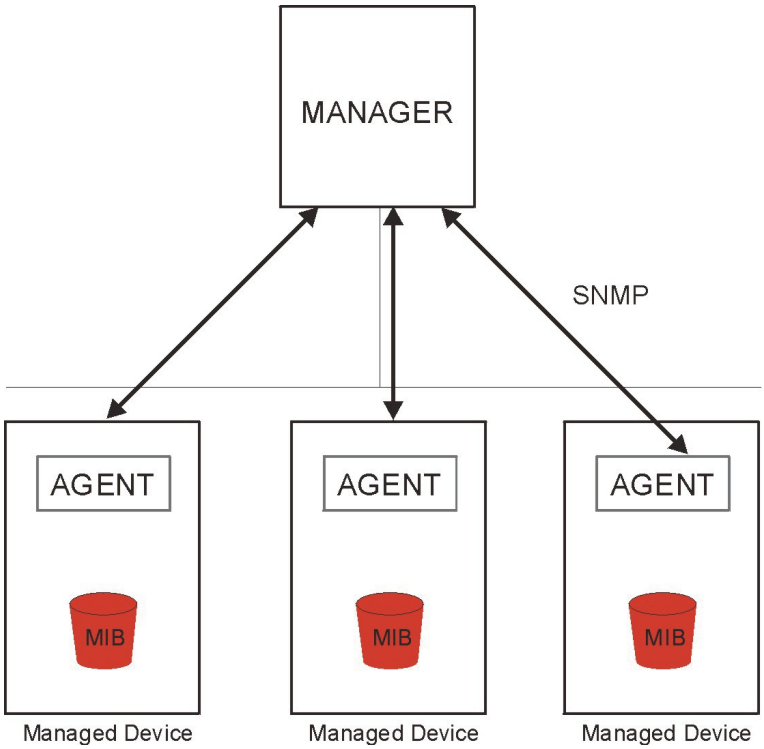
Table 20 System > BU Information

LABEL	DESCRIPTION
Main Interface	
MAC Address	This is the MAC Address of the ZoneDAS BU.
IP/mask	This is where the user can input an alternative IP and subnet mask for accessing ZoneDAS from the console's browser.
Gateway	This is where the user can set a new Gateway.
Apply	Click **Apply** to save that section's changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to remove all changes made since last clicking **Apply** and reconfigure the screen afresh.
VLAN Interface	
Enable	Click and check the box to enable VLAN access to this ZoneDAS BU.
VLAN IP/mask	This is where the user can input the IP and subnet mask for accessing ZoneDAS through VLAN.
VLAN ID	This is where the user can set the VLAN ID.
VPN Interface	
Enable	Select **Enable** to use *OpenSSL VPN* for a secure connection to the BU.
Username	Enter a descriptive login name for the OpenSSL VPN secure connection to the BU.
Status	This displays the VPN connection status. When the VPN connection is up, this field shows the IP address assigned by the OpenVPN server. When the VPN connection is down, one of the following shows: • **Authorization Fail** shows when authorization cannot be given for the OpenSSL VPN connection. This may be due to incorrect credentials or too many concurrent sessions. • **Inconsistent cipher** shows when the ciphers used by ZoneDAS does not match that of the OpenVPN server. • **Inconsistent Compression** shows when the LZO compression schemes used by ZoneDAS and the OpenVPN server do not match. • **Linking in progress** shows when an OpenSSL VPN secure connection is being established. • **Linking failed** shows when there's a failure to establish an OpenSSL VPN secure connection.
Import .opvn File	Click **Upload** to import an .opvn file into ZoneDAS for use in establishing the OpenVPN connection. Once a file has been uploaded, the box beside the **Upload** button will say "Exist".
Password	Enter the login password for the OpenSSL VPN secure connection.
Assigned IP	Enter the IP address and port of the computer on which OpenVPN is installed.

7.3 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. ZoneDAS supports SNMP agent functionality, allowing a manager station to manage and monitor the BU through a network. The BU supports SNMP version two (SNMPv2c) and version three (SNMPv3). The following figure illustrates an SNMP management operation.

Figure 37 SNMP Management Model



An SNMP managed network consists of two main types of components: agents and a manager.

An agent is a management software module that resides in a managed device (i.e. the BU). The agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include number of packets received, node port status, etc. A Management Information Base (MIB) is a collection of managed objects. SNMP facilitates communication between a manager and its agents for the purpose of accessing these objects.

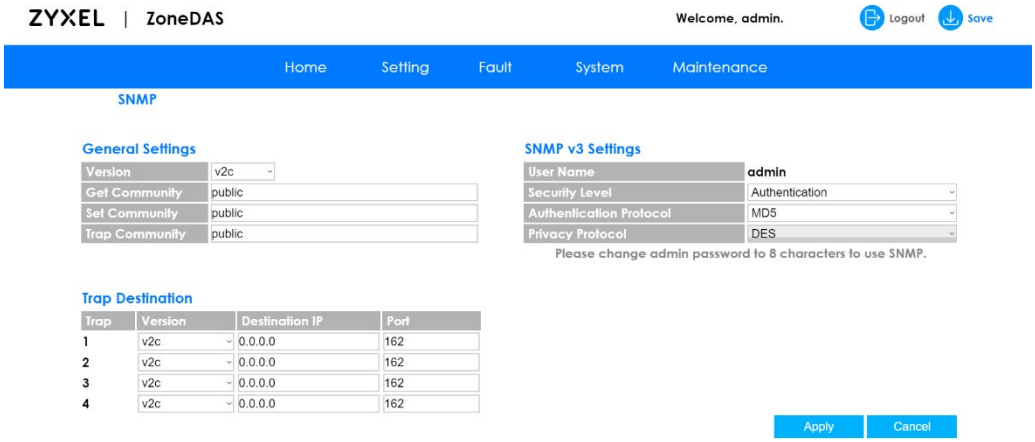
SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.

- Trap - Used by the agent to inform the manager about events.

To setup ZoneDAS for SNMP operation, it is necessary to configure its SNMP parameters and settings. To access these options, click **System > SNMP** to open the following screen:

Figure 38 System > SNMP



The following table describes the labels on the SNMP screen.

Table 21 System > SNMP

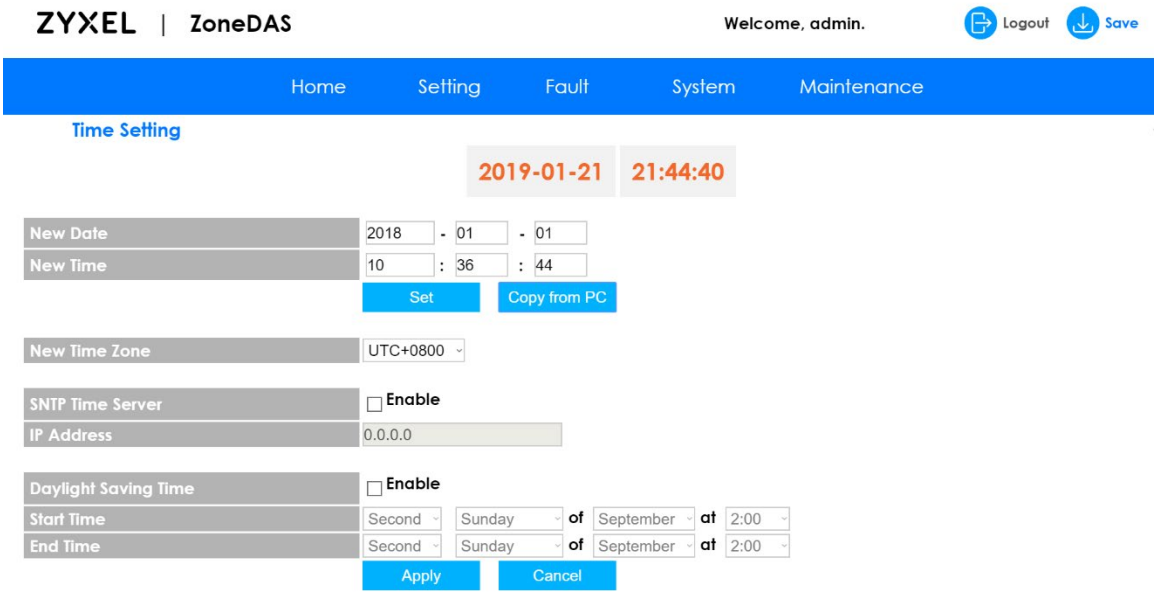
LABEL	DESCRIPTION
General Settings	
Version	Select the SNMP version the BU will use for sending traps to the SNMP manager. Choose from v2c, v3, or v2c+v3.
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests.
Trap Community	Enter the **Trap Community**, which is the password sent with each trap to the SNMP manager.
Trap Destination	
Trap	This is the index number for the entry.
Version	Select an SNMP version supported by the BTS.
Destination IP	Type the IP address of the station to which you wish to send your SNMP traps.
Port	Enter the port number to which the BU sends SNMP requests.
SNMPv3 Settings	
User Name	This field displays the username under which the BU is logged on.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this BU. Choose: • **None** -to use the username as the password string to send to the SNMP manager. This is equivalent to Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • **Authentication** - to implement an authentication algorithm for SNMP messages sent by this BU. • **Authentication + Privacy** - to implement authentication and encryption for SNMP messages sent by this BU. This is the highest security level. Note: The settings on the SNMP manager must be set at the same or higher security level relative to the security level settings on the BU.

LABEL	DESCRIPTION
Authentication Protocol	Select whether you wish to implement password authentication for SNMP communication with the managed device. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower. If you select **MD5** or **SHA**, enter a password between 8 and 100 ASCII characters for SNMP user authentication.
Privacy Protocol	Select whether you want to implement encryption for SNMP communication with the managed device. • **DES** - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • **AES** - Advanced Encryption Standard superseded DES as the data encryption standard and also uses a secret key. AES applies a 128-bit key to each 128-bit block of data. If you select **DES** or **AES**, enter the password of between 8 and 100 ASCII characters for encrypting SNMP packets.
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** remove all changes made since last clicking **Apply** and reconfigure the screen afresh.

7.4 The Time Setting Screen

The **Time Setting Screen** is used to configure the system's time related settings, including, date, time zone, and Daylight Saving Time settings. To access this screen, click **System > Time Setting**.

Figure 39 System > Time Setting



The following table describes the labels on this screen.

Table 22 System > Time Setting

LABEL	DESCRIPTION
Current Date (in orange)	This field displays the date used by ZoneDAS, in large, orange numbers.
Current Time (in orange)	To the right of the Current Date, this field displays the time that ZoneDAS uses, in large, orange numbers. This display uses the 24-hour format.
New Date	Enter the desired system date in this field.
New Time	Enter the desired system time in this field, in 24-hour format.
Set	Click **Set** once the desired system date and time have been entered.
Copy from PC	Set the ZoneDAS system time using the connected console's date, time, and time zone settings.
New Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and the Coordinated Universal Time (UTC), which is effectively the same as the Greenwich Mean Time (GMT).
SNTP Time Server	Select this check box to have ZoneDAS synchronize its system time with a predefined SNTP (Simple Network Time Protocol) server. To make this work, ZoneDAS must have direct Internet access through its MGMT port. Typically, this means the CAT5 cable from MGMT must plug directly into an Internet access point.
IP Address	Enter the IP address of the above-mentioned time server.
Daylight Saving Time	Daylight Saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Click **Enable** to have the system use Daylight Savings Time.
Start Time	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Saving Time**. The **at** field uses the 24 hour format. Here are a couple of examples: In most parts of the United States, Daylight Saving Time starts on the second Sunday of March. Each time zone in the United States goes into Daylight Saving Time at 2 A.M. local time. Therefore, in the United States you would select **Second**, **Sunday**, **March** and select **2:00** in the **at** field. In the European Union, Daylight Saving Time starts on the last Sunday of March. All time zones in the European Union start using Daylight Savings Time at the same moment (1:00 A.M. GMT or UTC). Therefore, in the European Union you would select **Last**, **Sunday**, **March**. The time you select in the **at** field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Time	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Saving Time**. The **at** field uses the 24 hour format. Here are a couple of examples: In the United States, Daylight Savings Time ends on the first Sunday of November. Each time zone in the United States stops using Daylight Savings Time at 2 A.M. local time, so in the United States you would select **First**, **Sunday**, **November** and select **2:00** in the **at** field. In the European Union, Daylight Savings Time ends on the last Sunday of October. All time zones in the European Union stop using Daylight Savings Time at the same moment (1 A.M. GMT or UTC). Therefore, in the European Union you would select **Last**, **Sunday**, **October**. The time you'd select in the **at** field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to remove all changes made since last clicking **Apply** and reconfigure the screen afresh.

CHAPTER 8
Maintenance

8.1 Overview

This chapter provides information on the **Maintenance** screens. Use the **Maintenance** menu to upload firmware, handle configuration files, and manage user accounts.

8.1.1 Available Functions

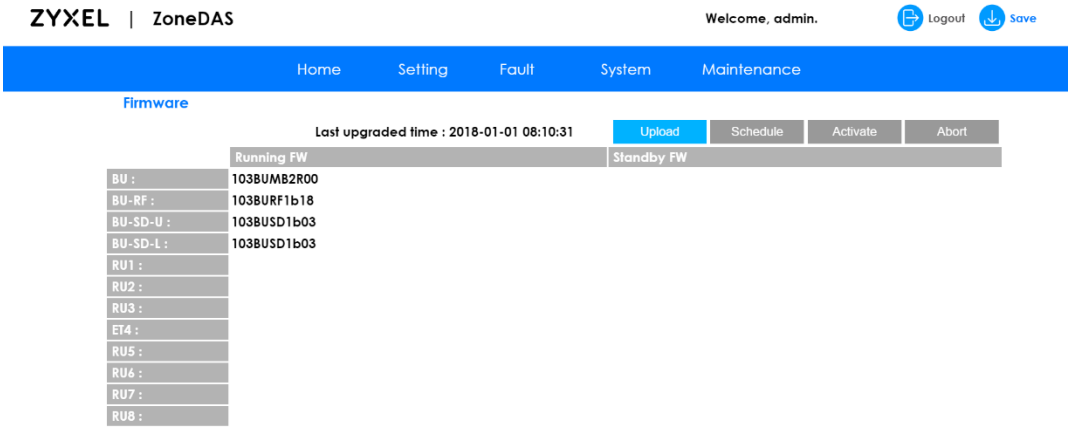
- Use the **Firmware** screen to upload firmware to the BU and all connected RUs (Section 8.2).
- Use the **Config File** screen to save your configuration as a file, download configuration files from the BU to your computer, or upload configuration files from your computer to the BU (Section 8.3).
- Use the **User Account** screen to manage user accounts and privileges (Section 8.4).
- Use the **Restart** screen to reboot ZoneDAS (BU and RUs) (Section 8.5).

8.2 The Firmware Screen

ZoneDAS upgrades its firmware in 2 steps. First the firmware is uploaded into ZoneDAS through a computer console. Then the firmware is actually applied. This 2-step process prevents complications that may arise through broken connections or computer failure. Firmware files come in unified packages and are available at www.zyxel.com. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the firmware can be installed. After firmware installation, the system will reboot.

Click **Maintenance > Firmware** to open this screen.

Figure 40 Maintenance > Firmware



The following table describes the labels on the Firmware screen.

Table 23 Maintenance > Firmware

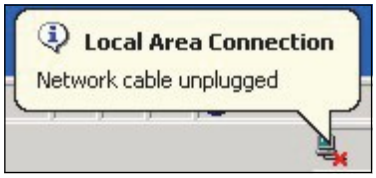
LABEL	DESCRIPTION
Upload	Click **Upload** to upload a firmware file into the ZoneDAS BU's memory. ZoneDAS will automatically decode the firmware package and upgrade each system part accordingly.
Schedule	Once an appropriate firmware file has been uploaded into the ZoneDAS BU, the user may click **Schedule** to set a future time for the system to automatically install (activate) the firmware. This may be used to take advantage of night hours for system upgrades, as the ***upgrade process often requires the system to stop service and reboot***.
Activate	Click **Activate** to install an uploaded firmware right away.
Abort	Click **Abort** to prevent an uploaded firmware from Activation.
Running Firmware	Firmware listed under this label are the ones that are installed and running on ZoneDAS right now.
Standby Firmware	Firmware listed under this label have been uploaded into ZoneDAS memory but have not yet been installed.
BU	Firmware listed in this row are for the Base Unit only.
BU-RF	Firmware listed in this row are for the Base Unit's RF modules only.
BU-SD-U BU-SD-L	Firmware listed in this row are for the Base Unit's SD modules only. U refers to the upper module (the one on top), while L refers to the lower module (on bottom).
RUx	Firmware listed in this row are for Remote Units only.
ETx	Firmware listed in this row are for Extenders only. At present, Extender firmware can only be installed by accessing the Extender's Web Configurator. This will change.

Note: Do not turn off or reboot ZoneDAS while any firmware upload or activation is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into ZoneDAS again.

After a firmware upgrade, ZoneDAS will restart automatically and temporarily disconnect from the network. In some operating systems, you may see the following message on your desktop.

Figure 41 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Maintenance > Firmware** screen.

If the upload was not successful, you would see an error message.

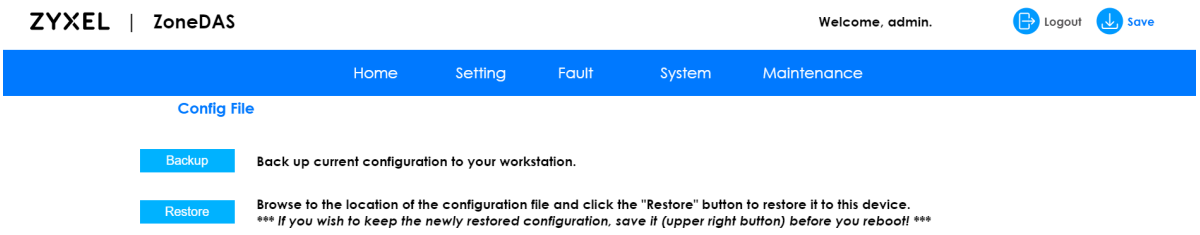
8.3 The Config File Screen

A configuration file stores a BU's settings. As such, a configuration file can be applied to the BU (without reboot), backed up to computers, and restored at any time. They can even be modified with plain text editors before being used for restoration. Configuration files use the ".txt" extension. Use **Config File screen** to perform all these functions (except, of course, the text editing).

Once your BU is properly configured and functioning smoothly, we highly recommend that you back up your configuration in a configuration file before making further changes. The configuration backup file will be useful if and when you need to reload your previous settings.

Click **Maintenance > Config File** to open the following screen.

Figure 42 Maintenance > Config File



The following table describes the labels on this screen.

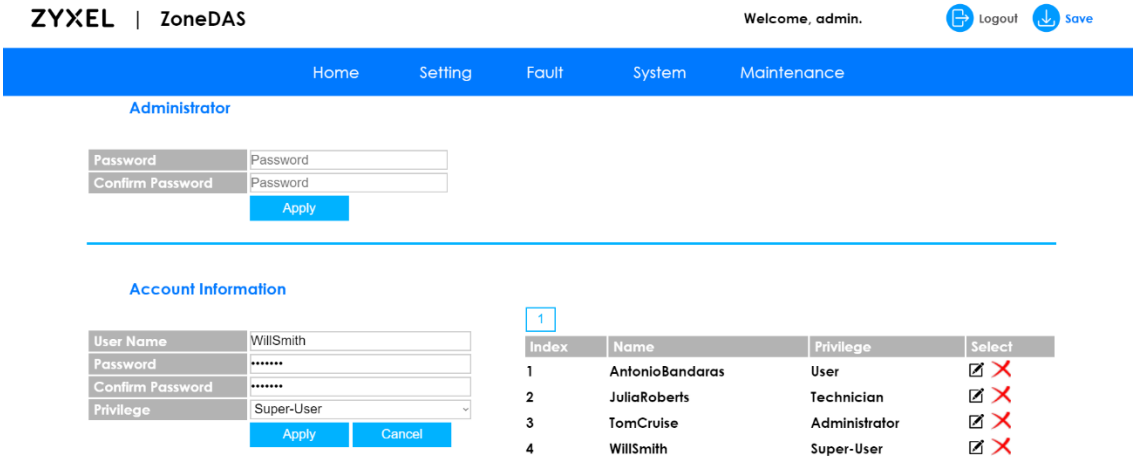
Table 24 Maintenance > Config File

LABEL	CONFIGURATION
Backup	Click **Backup** to save the current configuration to your computer. The system will create a configuration file, give it a name, and save it to the console's default download directory.
Restore	Click **Restore** to replace all current settings with those stored in a configuration file. The browser will pop up a file window for the user to select the file desired. Once selected, the system will apply all settings stored within the configuration file. If the user is satisfied that the newly loaded configuration is safe for use, click the **Save** button (on the very top right) to commit all values to permanent memory.

8.4 The User Account Screen

Use the **User Account** screen to manage administrator accounts for Web Configurator. Settings include user name, password, and privileges. Click **Maintenance > User Account** to open this screen.

Figure 43 Maintenance > User Account



The following table describes the labels on this screen.

Table 25 Maintenance > User Account

LABEL	DESCRIPTION
Administrator	
Password	Specify the password for this account. The characters are displayed as dots (•) in this field.
Confirm Password	To ensure that the Administrator's password has not been mistyped, please enter the exact same password a second time.
Account Information	
User Name	Enter a descriptive name for the user account. The user name must have 1~31 alphanumeric characters. Specifically, it can include 0~9, a~z, A~Z, and @%+/!#$^.(){}[]~-_
Password	Specify the password for this account. The password must also have 1~31 alphanumeric characters. Specifically, it can include 0~9, a~z, A~Z, and @%+/!#$^.(){}[]~-_
Confirm Password	Enter the exact same password again, for verification.
Privilege	Select the privilege level for the user. There are four types of privilege levels. • **User** – A user of this level can access most screens but cannot make any changes. • **Technician** – A user of this level is like a regular **User** but can change some basic settings and restore configuration files. • **Super-User** – A user of this level can access and configure all screens except for User Account settings. • **Administrator** – A user of this level can access and configure all screens.
Apply	Click **Apply** to save all changes to the BU's run-time memory. The BU, by default, does not keep each session's changes, so use the **Save** button on the title bar to save changes to the non-volatile memory when configuration is complete.
Cancel	Click **Cancel** to undo all changes made since last clicking **Apply**.
List of Accounts	
Index	This is the index number assigned to each user account. ZoneDAS supports up to 8 user accounts.
Name	This is the name of the user assigned to this account.
Privilege	This is the privilege level granted to this account.
Select	Click the icon to edit this user account. Click the icon to remove this user account.

8.5 The Restart Screen

Use System Restart to reboot the ZoneDAS BU and RUs. This may be a good way to resolve system instability. Click **Maintenance > Restart** and a window such as the following will pop-up. Click **OK** from there and ZoneDAS will restart.

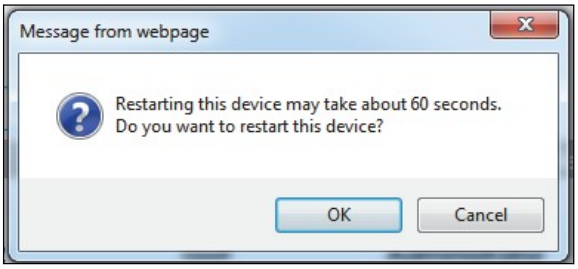



Figure 44 Maintenance > Restart