ZYXEL
NETWORKS

User's Guide
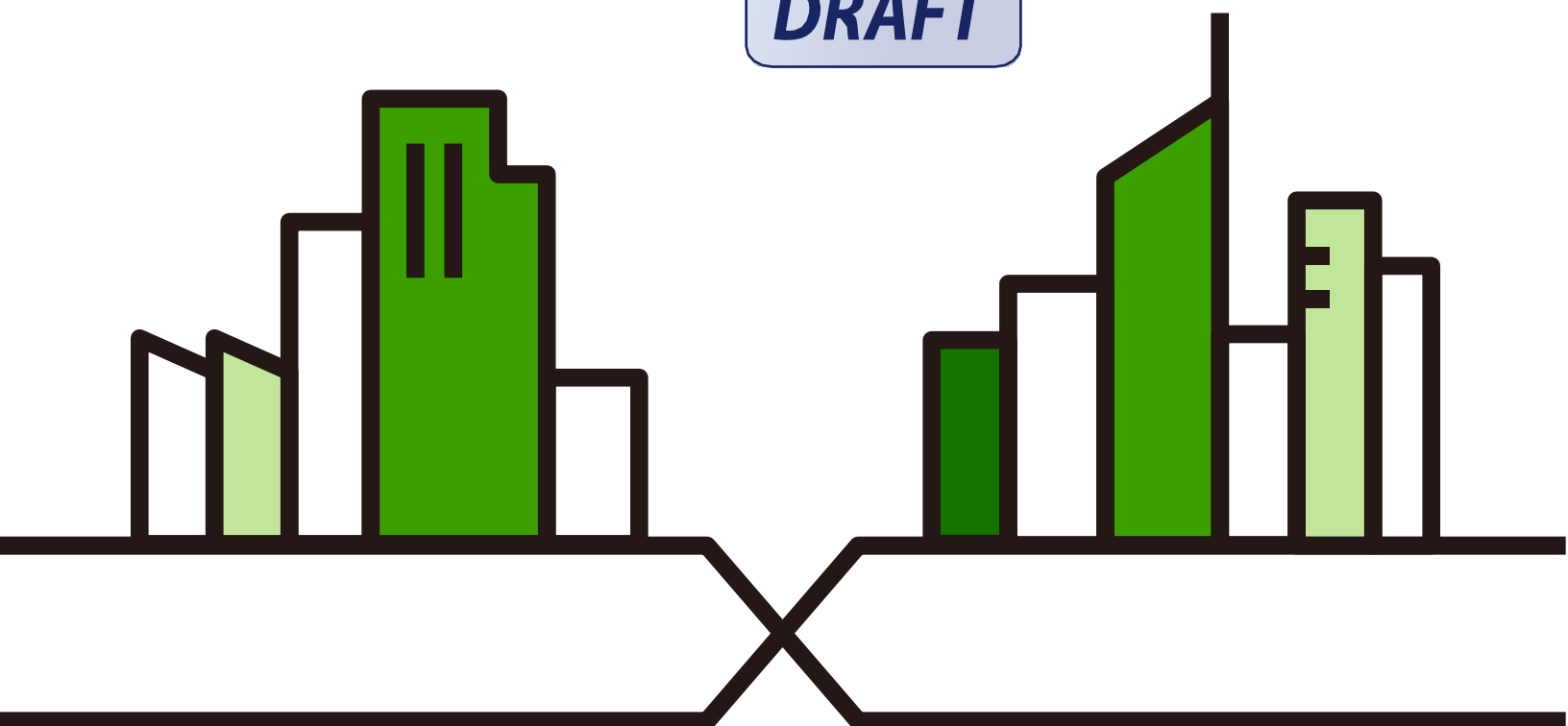
ZoneDAS Two

Active Fiber Distributed Antenna System

Default Login Details	
MGMT IP Address	https://192.168.0.1
Local IP Address	https://192.168.1.1
Login	admin
Password	12345678

Version 1.1 Edition 1, 12/2024
Firmware 200PACK2P06

DRAFT

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Every effort has been made to ensure that the information in this manual is accurate. However, screenshots and graphics in this manual may still differ slightly from what you see on screen due to differences between release versions and/or computer operating systems.

Each ZoneDAS Two unit, along with other Zyxel In-Building Solution devices, is customized for its operating region. As such, ZoneDAS Two components and devices designed for other regions may not work in your region and **will not be supported**. Please ensure that you purchase ZoneDAS Two **only** from your local authorized vendor.

Warnings and Notes

These are how warnings and notes are shown in this guide.

> **Warnings tell you about very important information, including things that could harm you or your device.**

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ZoneDAS may be referred to as the "ZoneDAS Two" in this guide.
- **Bold** font is used to identify product labels, screen names, field labels and field choices.
- A right angle bracket (>) within a navigation path denotes a mouse click. For example, **Setting** > **RU Settings** means you first click **Setting** in the navigation panel, then the **RU** sub menu.

Related Documentation

•Hardware Installation Guides (BU, RU, and EU)

The Hardware Installation Guides show how to install the BU (Base Unit), RU (Remote Unit), and EU (Expander Unit).

•More Information

In the event that a problem cannot be solved through the information in this manual, you should contact your exclusive distributor. If you cannot contact your distributor, then contact international customer support at ibs@zyxel.com.tw and/or ibs.tech@zyxel.com.tw.

Table of Content

CHAPTER 1
Introduction

1.1 Design Overview

ZoneDAS Two is compatible with all telecom operators, offering up to 800 MHz total bandwidth and supporting 5G 2X2 MIMO. With fiber transmission, it ensures faster, more reliable network coverage, ideal for enhancing connectivity in various environments.

Being modular, it offers unrivaled flexibility in band configuration, coverage, and upgradeability. 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 Two begins with signal source(s) from one or more operators. However, instead of having a passive combiner that merges signals and sends them to passive antennas, 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 Two 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!

A 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 fiber to its RUs, which are placed throughout the building to broadcast the signals. Each fiber cable can be up to 2.5 km long, and RU could get power over hybrid fiber for remote power feeding, or just use DC local power with POE adapter.

Figure 1 Basic ZoneDAS Architecture
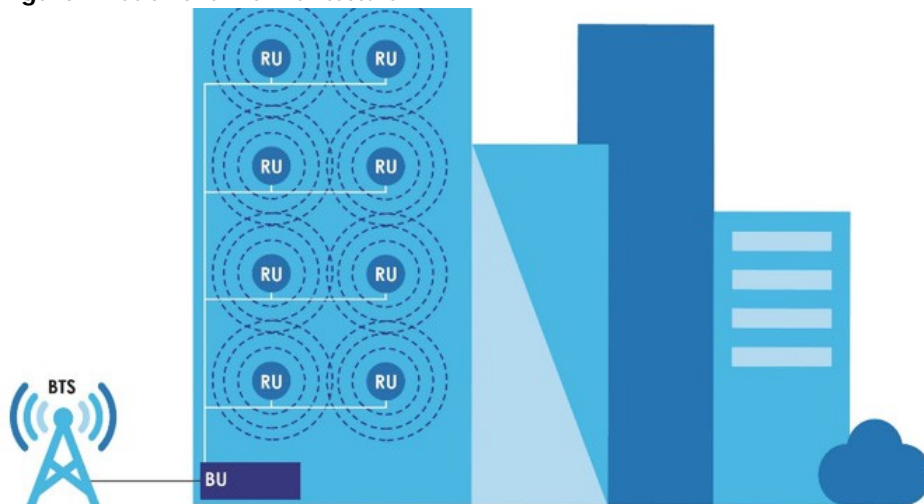
Like the combiner in passive DAS, the BU combines its input signals and sends the combined signal to each RU. Unlike in passive DAS, cable loss has been compensated for and signal quality is preserved for every RU. Each RU simply amplifies the signal to its specified strength and broadcasts it through its antenna(s), up to 4 of which it may fit onto each RU. The RU has powerful integrated amplifiers (giving up to 23 dBm per band) and uncompromising low noise figures (down to 6 dB) for optimizing the system footprint, thus lowering the overall TCO of the site solution. For RUs configured with external antennas, output signal pattern depends on the antennas installed. Strategic RU placement and configuration will ensure optimal coverage with strong cellular signal.

ZoneDAS Two is highly scalable and supports additional coverage through its companion device, the Expander (EU). An EU 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 Two" refers to the entire BU-RU system. ZoneDAS Two 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 upgradeability when new technologies arrive. Its ability to use fiber cables technologies facilitates quicker, easier multi-operator DAS deployment for neutral hosts and enterprises. 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 EU
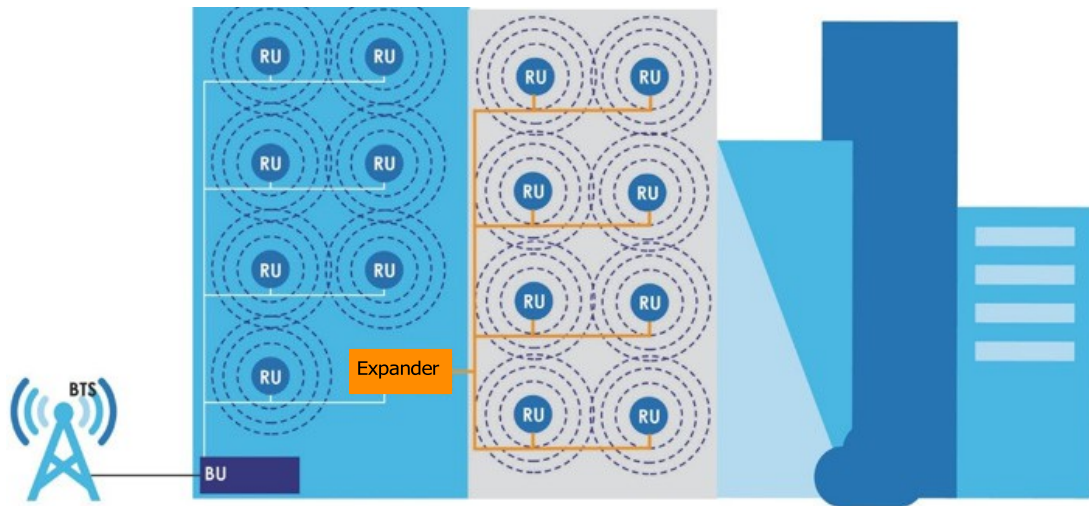
1.2 Coverage and Applications

ZoneDAS Two is ideal for medium sized buildings and installations. Its BU can connect up to a maximum of 8 RUs, each of which supplies cell phone signals for an area up to 2,500m^2, so a basic ZoneDAS Two setup can cover up to 20,000m^2. ZoneDAS Two is also highly extensible and can service larger areas when required, through EUs. Installing an EU adds capacity for 1~16 additional RUs, further increasing maximum coverage by 20,000m^2. With a full complement of 8 Expanders, one ZoneDAS Two can connect up to 128 RUs for a total coverage area of 320,000m^2. 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, EU, 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 you are sitting opposite to and looking at the front panel of the device.

1.3.1 Names and Terminologies

ZoneDAS Two 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
EU	Expander Unit

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
CH	Each RF module supports 4 channels through RF connectors
SD	Signal Distribution port / slot / module (for connecting EUs 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:

A ~ D	The character to identify the RF modules.
1 ~ 16	The character to identify other modules.

Finally, because ports and modules reside on devices, and because some of the most important ports and modules actually exist on different ZoneDAS Two 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.
EU5-RU2-RFA	The RF module that is installed onto the RF slot "A" on EU5-RU2.

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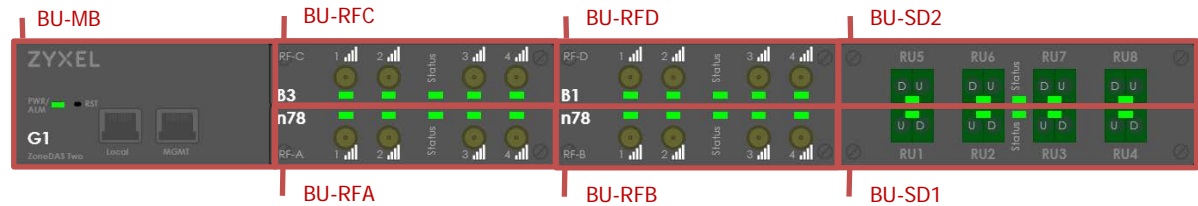
The following table describes the parts that are labelled in the figure above.

Table 1 BU System Part

SYSTEM PART	DESCRIPTION
BU-MB	The BU's Motherboard (BU-MB) is your gateway to controlling everything in ZoneDAS Two. To access the Web Configurator, connect a computer to the **MGMT/Local** port via an RJ-45 Ethernet cable.
BU-RF (A to D)	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 4 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), and so on. 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 EU. To connect an RU, simply pick an SD port (install a second SD module if the first is full) and connect a fiber cable from the RU's fiber port to the BU's SD port. To connect an EU, simply pick an SD port and connect a fiber cable from the EU's **To BU** port to the BU's SD port. For instructions on installing BU-SD modules, please see the Hardware Installation Guide.
Fan Module	The BU's fan module, accessible through the rear panel, 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.

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

1.3.2.1 LEDs (Lights)

Most ports/modules on the BU come with their own set of LED signal lights. These include the **Local/ 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.

Figure 4 BU LED Positions
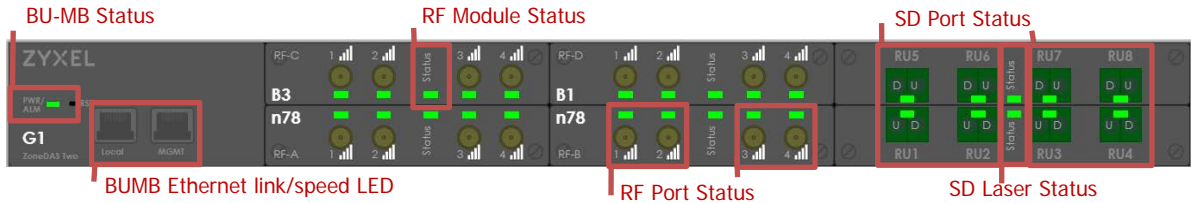
Table 2 Basic LED Behavior

BI-COLOR LED	BEHAVIOR	DESCRIPTION
	All Off	Power is off / RF service is off
	Green Blinking	Booting / Firmware upgrading
	Green	Power on / RF in service / Normal operation
	Red or Amber	Operational error / Hardware failure / Alert
	All Color Blinking	LED Testing

1.3.3 RU (Remote Unit)

Remote Units are important because they house the active antennas that actually broadcast the signals from the BU.

An RU has LEDs on the fiber connector, to indicate its RU-MB alarm/status. The Web uses four extra LEDs to show RF modules' alarm/status information.

Figure 5 BU With Remote Unit
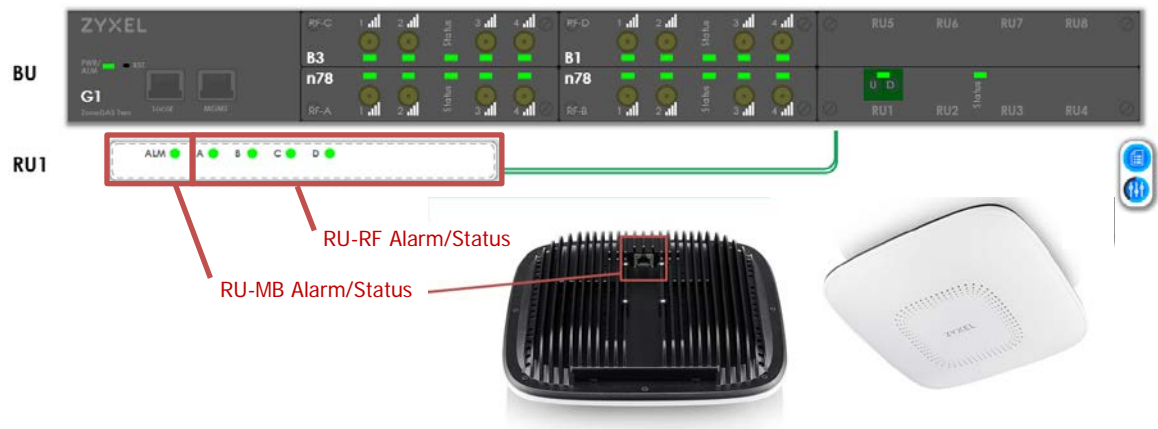
Table 3 RU System Parts

| 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.

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.

1.3.4 EU (Expander Unit)

The EU 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 EU would take that same SD port and turn it into 16 more! By nature of being a "mid-point station", it also provides another 2.5 km by fiber of reach between the BU and the RU. So, with an EU the RU can be up to 5 km away from the BU.

Figure 6 EU Connection Illustration
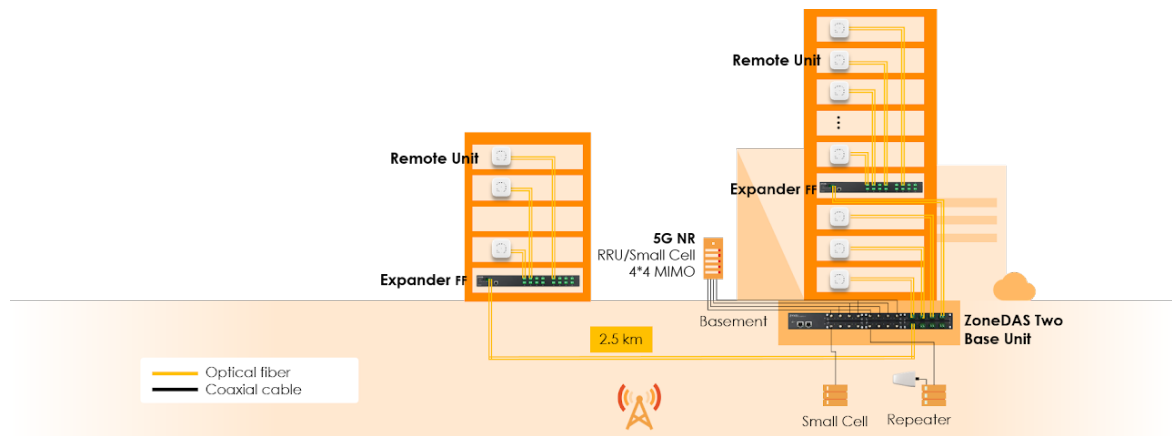
The EU has same ports and LEDs as the BU, except it has replaced the BU's RF modules with a single ToBU port. LED indicators and ports are located on its front panel, with near identical layout as the BU. The following figure shows its front panel and its different parts and ports.

Figure 7 EU Front Panel

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

Table 4 Expander System Components and Ports

| SYSTEM PART	DESCRIPTION
EU-MB	These are ports that access the EU's Motherboard (EU-MB). You may connect your computer to the **Local** port using an RJ-45 Ethernet cable and access the EU directly using its Web Configurator (https://192.168.1.1), to do firmware upgrade or check RU connections. Everything is controlled through the BU, which connects to the EU though the **To BU** Port.

EU-SD (ports labeled **RU1** to **RU16**)	As with the BU, each EU has 16 SD ports, each of which connects one RU. To connect an RU, simply pick an SD port and connect it to the RU's fiber port via a fiber cable. For instructions on properly installing EU-SD modules, please see the Hardware Installation Guide.

The EU looks like a BU and even has its own Web Configurator interface. But it cannot be controlled through the **Local** port like a BU. Instead, it must be connected to a BU (through its **To BU** port) and controlled through the BU's Web Configurator. All EU functions are unavailable from the EU itself; they must be accessed through the BU.

1.3.5 RPF (Remote Power Feeding Controller)

Remote Power Feeding Controller is a power supply device that provides remote power feeding to Remote Units. One device can support 16 DC power supply modules for 16 Remote Unit to solve the problem of no local power supply near RU.

Figure 8 RPF Connection Illustration
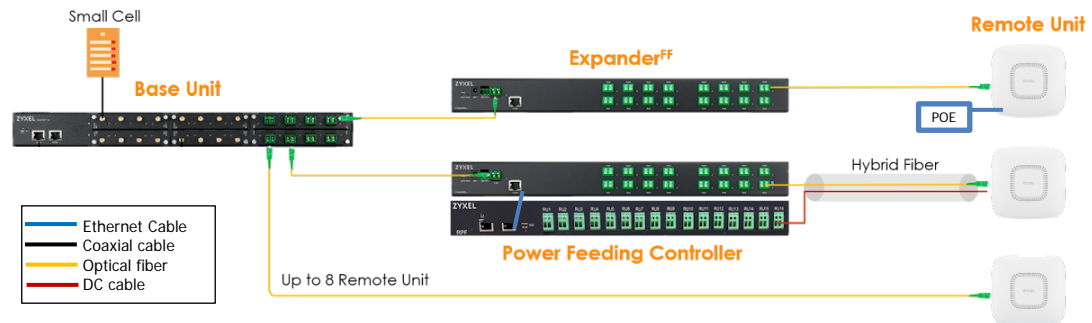
The RPF has the same ports and LEDs as the EU, and it would provide remote power feeding to connected RU automatically. But it also could be controlled by BU or EU by an Ethernet connection from **BU/EU local RJ45 port** to **RPF's any RJ45 port**. LED indicators and ports are located on its front panel, and LED would show the power status of each port.

Note. When RPF is controlled by BU/EU, the fiber port and power port must be paired with same labels (RU1~RU16). For example, if we want to connect a RU to this EU1 as EU1-RU1. The fiber cable from this RU must be connected to EU1's RU1 port, and the DC cable from this RU must be connected to this RPF's RU1 port. Then, EU1 could control this RU1's power on/off by RPF.

Figure 9 EU Front Panel

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

Table 5 Expander System Components and Ports

SYSTEM PART	DESCRIPTION
Ethernet Port	There are two Ethernet ports on the panel. One port could be connected to BU/EU's local Ethernet Port, and BU/EU would take control of this RPF. Another port is reserved as BU/EU's local Ethernet port, that you could connect your computer to this port using an RJ-45 Ethernet cable and access the BU/EU directly using its Web Configurator (https://192.168.1.1), to do firmware upgrade or check RU connections.

Power Port (ports labeled **RU1** to **RU16**)	A RPF has 16 power ports, each of which connects one RU to provide remote power feeding. To connect an RU, pick a fiber port from BU/EU and connect it to the RU's fiber port (ex: RUn) via a fiber cable, then take the power port which has same label "RUn" to the RU's power port via DC power cable.

1.3.6 The Reset Button

If ZoneDAS Two 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 labeled **RST** and is located inside a small pinhole on the front panel on the left.

Before pressing the **RST** 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 RST button for three (3) seconds**, then release. The system indicates that three seconds have passed by flashing the **ALM** LED. Simply release the **RST** 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 next.

2 To hard reset all variables back to factory defaults, press the **RST** button for ten (10) seconds. 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 Two 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 the Web Configurator will be discussed in later chapters.

In addition to the Web Configurator, ZoneDAS Two can be managed via SNMP (Simple Network Management Protocol) using an 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 Two is deployed, do the following regularly for effective management and optimal security.

- **ALWAYS change the "admin" 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 8.3 on page 63 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 Two 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 you through setting up ZoneDAS Two 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 Two'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 .

2.2 System Setup

There are two steps to setting up ZoneDAS Two 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 Two 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.

    1a   Make sure the BU can access source signals from its planned location.

    1b   Make sure that each RU will be within a 100-meter cabling distance from the BU.

2   Run fiber 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 fiber cables.

5   Connect each RF signal source to the BU.

    5a   Before connection, be sure that the RF signal is **always below +30dBm** (1W). The specified operational range for ZoneDAS Two is 0 ~ +24 dBm, while the recommended input signal range is 0 ~ +15 dBm.

Anything above 30dBm will permanently damage the BU!

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 **Local** port.

9   Open the browser on the computer and go to https://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 Two.

2   Set the System Time.

3   Ensure that RF inputs are within range (0 ~ 24 dBm).

4   Configure BU parameters.

5   Configure RU parameters.

6   Do System Calibration, and ensure that the system remains error free after System Calibration.

7   Fill in descriptive information such as Site Name and Site ID.

8   Configure network settings (Syslog Server etc.) for central management.

9   Save settings.

10   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 Two

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

Figure 10 Login Window

From here, simply enter the Username and Password. Default username is "admin" and the default Password is "12345678". Once logged in, the **Home** screen would appear. The following is a sample **Home** screen.

Figure 11 Home Screen
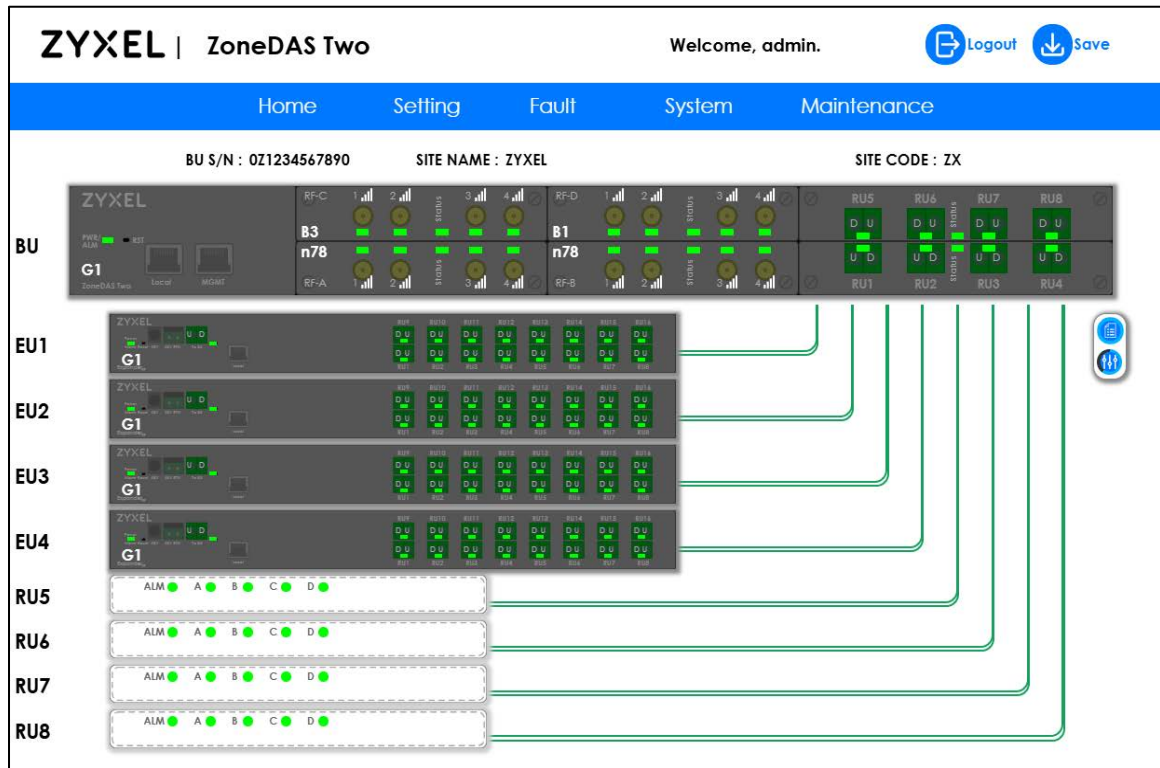
If you have any problems logging into the Web Configurator, please refer to Section 3.2 on page 29, where the process is explained in greater detail.

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 Settings** screen, as shown next:

Figure 12 Time Settings Screen

If the computer console has the correct local time for ZoneDAS Two, click **Set**. This will update the **System Time** and **Time Zone** (shown in orange, top center) — as well as the fields under **New Date**, **New Time**, and **Time Zone** — to those of the console.

If the computer console is not a suitable source for system time, then set the time and date manually: type in or select correct values for **New Date** and **New Time**, then click **Set**. But if you wish to set the time zone, do that first. Simply select the ZoneDAS Two unit's time zone from the **Time Zone** drop down menu.

Finally, you can connect ZoneDAS Two to an NTP Time Server to automatically set and maintain the system time for proper timestamps on your logs. That is not required at this point, but you may refer to 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 a repeater. Either way, the signal will come through a coaxial RF cable and the ZoneDAS Two will treat all signals 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. The wording "RF Input Signal" represents the total composite RF power of one BU-RF module. **ZoneDAS Two 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 is between 24 and 30 dBm in strength, the system will activate its Protection Mode and shut down all operation for that RF channel (and only that channel).

An 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 in the **Home** screen, at the BU. There, near each RF label, will be an RF signal strength mark, like this:

Figure 13 RF Input Signal Strength

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

If the strength of RF input for a module is higher than 15 dBm, the mark will show with orange to warn of sub-optimal performance. If the strength is lower than 0 dBm (for 5G, < -10 dBm), there will be an X mark to show "no signal". Otherwise, it will show a signal strength mark if RF input signal is detected.

Please ensure that all connected inputs are detected and working fine.

If not, please consult the signal source (BTS, femtocell, etc.) parameters 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 (for example Band 1, Band 3, Band 7, Band 41, and so forth).

2 Cellular technology used (choose **2G GSM**, **3G UMTS**, or **4G LTE**. This needs to be specified because it affects the system's internal parameter settings and tuning algorithms. 5G NR is fixed for 5G RF modules, not selectable.

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

Once the information is ready, simply enter it 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 Settings** screen, as shown next:

Figure 14 BU Settings Screen

The gray bar at the left of the table shows RF-A to RF-D channels, from top to bottom, and each RF module has 4 ports which are labeled CH1~CH4. These correspond to RF modules A, B, C and D. To the right of each module name is the band used by that module, as detected by the system. Entries under each column correspond to the status of that column's module/channel, as specified by the titles in gray on the left side. Here, please fill in the blanks for each connected channel, using the above- specified information. The system does feature error detection, so frequency values that do not fall within the detected Frequency Band will not be accepted as valid input.

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 .

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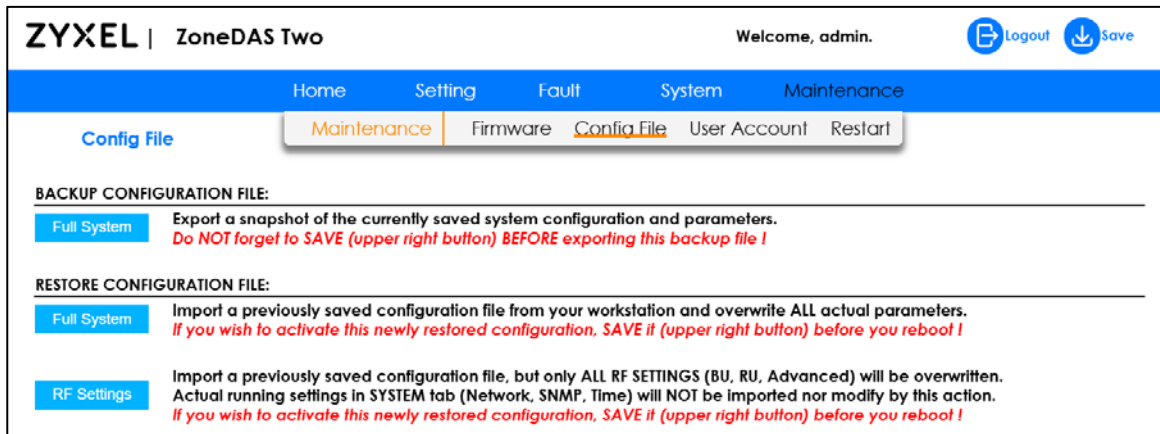
From there, click **Restore** and locate the target Config file from the browser's file manager. Double click on the file once it is found and ZoneDAS will begin the restoration process, which typically takes less than 10 seconds. When it is done, you will see the word "Success" displayed at the top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

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

Figure 16 ZoneDAS BU-RF Screen

The large graph at the bottom of the screen depicts RF activity for the selected RF module. In the above scenario, it is RF-A. To see RF activity for other RF ports, simply click one of the four blue buttons near the top center, marked **CH1**, **CH2**, **CH3**, and **CH4**.

The graph has 2 measurement curves: 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 timestamp. 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.

At this point, for all active RF channels, you 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 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 +23 dBm per RF band module. 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 will appear:

Figure 17 RU 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. Two identical columns still lie beneath each of these labels. The difference is, the gray bar at the left side of the table now lists all the RUs the system can connect to. As each RU has up to 4 RF modules, this table allows individual configuration of each RU-RF module's maximum output power.

Specifying output power for each RU-RF module is easy. Simply locate the module's place in the table, and enter a value that represents the RU-RF antenna's maximum RF output power (that is power under maximum load) under **DL Output Power**. The system will show the actual output power to the right. A max 17 dBm output would typically service an area equivalent to a 25 m x 25 m open-space zone, while 23 dBm would service an area-equivalent of 50 m x 50 m.

There is a **Personal Notes** section on the bottom left corner of this screen. This is to help you make configuration memos when testing for optimal maximum outputs and deciding on the number of licenses to buy. The section provides plenty of space for plain text — and only plain text. Be sure to click the **Store Personal Notes** button when text input is done.

As this is the initial installation, RU placement has already been determined. Simply configure all RUs using pre-planned values, noting that you can only change values for connected RUs. Once configuration is done, please press **Apply** (and **Save**).

2.3.8 System Calibration

To do system calibration, 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 **System Calibration**. The circle will light green to indicate that Service is now On.

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 Two can operate without the benefit of calibration, performance will be affected adversely. Calibration, therefore, is an important part of proper ZoneDAS Two installation.

Figure 18 System Calibration Button
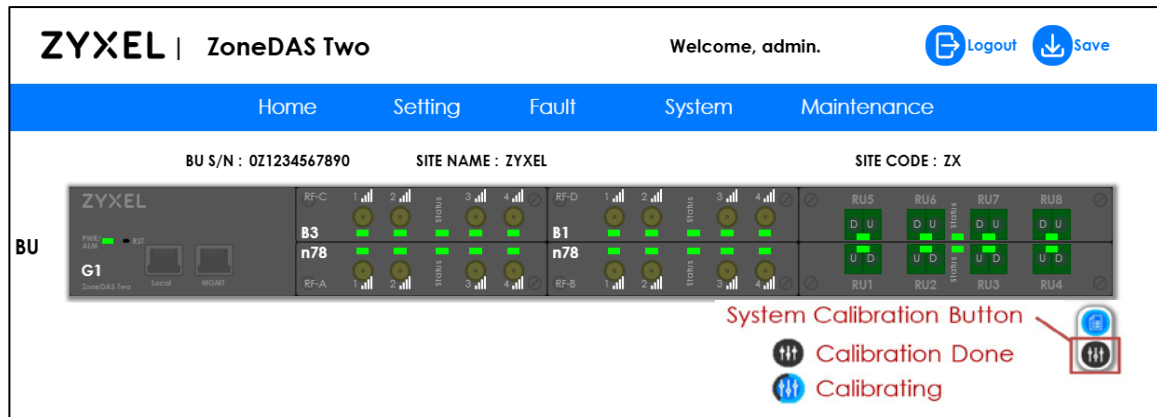
If RUs or EUs get unplugged and re-plugged into different ports, the on-screen lines connecting the BU to the RUs/EUs turn yellow to indicate they need calibration. System calibration would be activated automatically when lines need calibration, and you also could activate calibration manually. After calibration, 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.

2.3.9 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 step one.

To identify all the relevant parts, give names (and codes) to the BU, RF bands, 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 Two 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 helps 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**.

To give names to the RF bands, click **Setting** from the Navigation Panel and select **BU Settings**. Find **Description** on the right of the table, and fill in the description of each activated RF band. For example, the description may include the operator name for that signal and the frequency band for that channel.

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.

2.3.10 Set Central Management

If the 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 **System** on the Navigation Panel, wait for the menu to appear, and click on **Network**. This opens the **Network Settings** screen, as shown next:

Figure 19 ZoneDAS Network Settings Screen

There is an input box labelled **Syslog server**. Simply input the IP for the central syslog server, add a colon (:) and port number (default 514), then select **Enable** and click **Apply**, and Syslog Setup is complete! The system will automatically ping the IP and display a check mark after the IP address box if it succeeds. If it does not, it will display two exclamation marks (!!) instead.

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

Figure 20 ZoneDAS SNMP Screen

The SNMP screen has 3 sections for setting up remote management: **General Settings**, **Trap Destination**, and **SNMP v3 Settings**. ZoneDAS Two 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. For Trap Destinations, the system will automatically ping the IP and display a check mark after the IP address box if it succeeds, or display two exclamation marks (!!) instead if it does not. Once the correct parameters have been entered, click **Apply** and central management setup is complete.

Note: In accordance with SNMP requirements, please ensure that your Administrator password has at least 8 characters.

2.3.11 Save Settings

ZoneDAS Two 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 21 Save button

If Save is not clicked, all updated settings will exist only in

volatile memory and will disappear upon system reboot.

You will see a red circle around the **Save** button if there are settings left unsaved, like this:


Note: Once **Save** is selected, the current settings will transfer to the system's non-volatile memory for reloading upon reboot.

2.3.12 Backup Configuration

To backup the current configuration 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 Two will create a backup file in the default download folder, using its Serial Code and Date as part of the file name.

Figure 22 The Config File screen
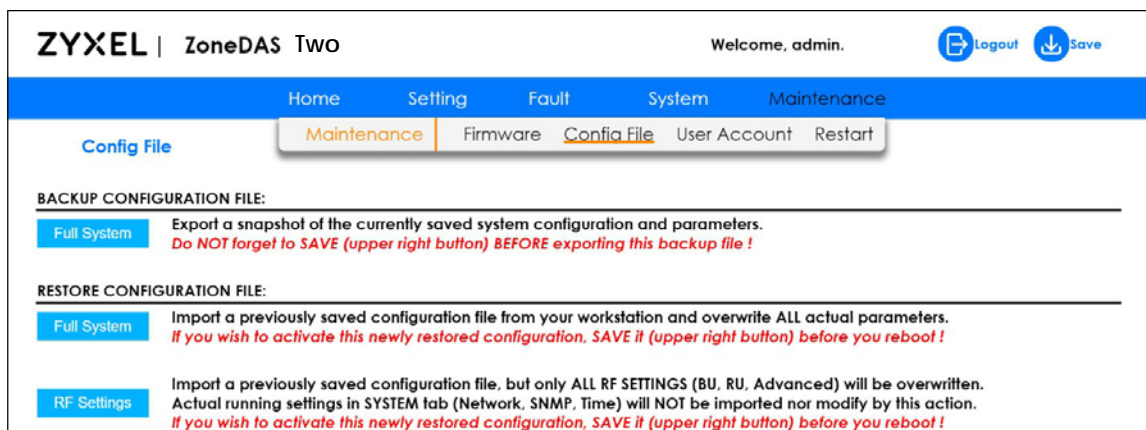
Once the backup config file has been created, be sure to keep a copy safe for future use. Setting up a system via loading a config file would be far quicker than doing it again from the beginning.

CHAPTER 3
The Web Configurator

3.1 Overview

This chapter, along with the five that follow, describes the ZoneDAS Two 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 Two via an Internet browser. The recommended screen resolution is 1024 by 768 pixels and the compatible browser are listed as below:

- Microsoft Edge 123.0 and later versions
- Mozilla Firefox 124.0 and later versions
- Google Chrome 124.0 and later versions
- Safari 17.0 and later versions

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 Two 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 192.168.1.2 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 Two BU's **Local** port.

4   Launch the web browser and go to https://192.168.1.1.

5 The **Login** screen should appear. To access the Web Configurator and manage ZoneDAS Two, type the default username: **admin** and password: **12345678** in the password screen and click **Login**.

Figure 23 Login Window

3.2.1 The Web Configurator Layout

The Web Configurator is arranged into these parts:

Figure 24 The Web Configurator Layout
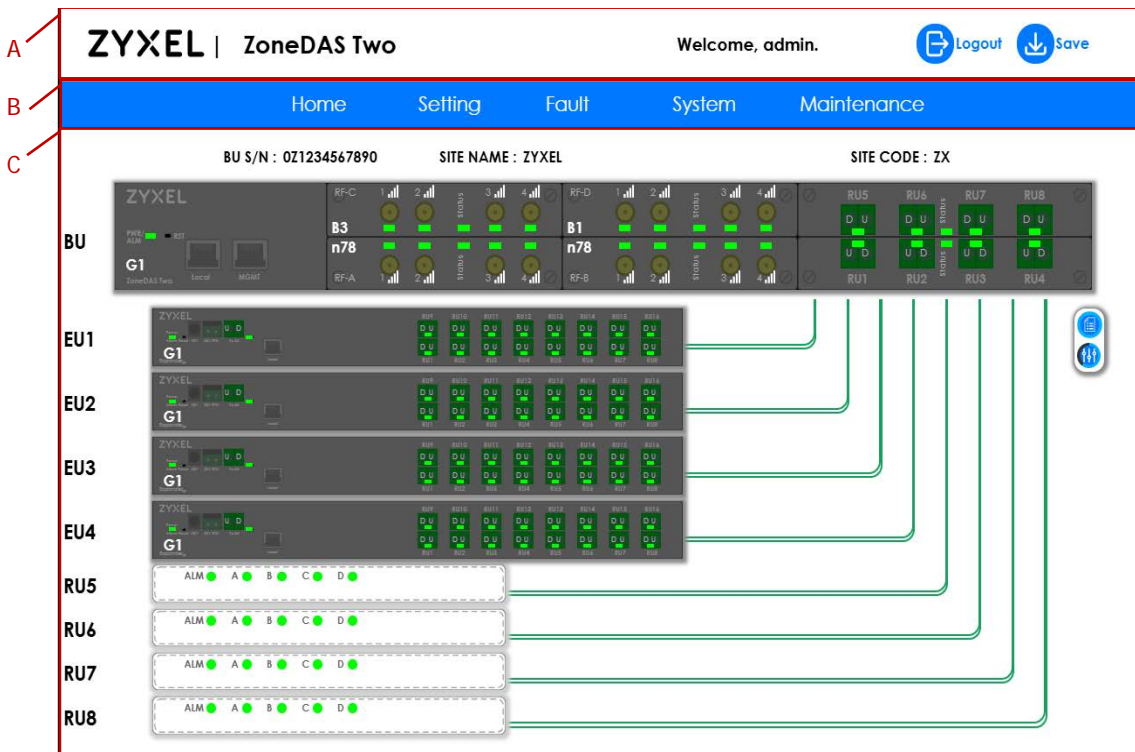
A - Title Bar
B - Navigation Panel
C - Main Window

The RUs and/or EUs 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-EU 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 25 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 Two 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 Two's features.

Figure 26 Navigation Panel

The following table describes all the sub-menus:

Table 7 Screens Summary

MENU	SCREEN	FUNCTION
Home	Home	This is the main Web Configurator screen. From here, you can view and monitor each ZoneDAS Two device and its connection status, including the BU and its connected EUs / RUs.
	BU	Use this screen to view/modify the BU's basic information.
	BU-RFA~RFD	Use this screen to view/modify each BU-RF's power, green power down, UL/DL gain offset and description, plus monitor status, UL/DL system gain, and input power.
	EU1~EU8	Use this screen to view/modify each EU's basic information.
	RU1~RU16	Use this screen to view/modify each RU's basic information, plus monitor each RU-RF's status, temperature, and input/output power.
Setting	BU Settings	Use this screen to configure each BU-RF's signal input 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, and TDD 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, and so on.
	Alarm Settings	Use this screen to modify each alarm type's severity level, SNMP alarm delay, and report as syslog, SNMP trap or email.
	System Log	Use this screen to view the ZoneDAS Two system log and to set up the system log server's IP.
System	Network	Use this screen to view and modify the system's Ethernet Interface settings (such as VPN/VLAN/Local/MGMT port), and network service's connection settings (such as SNMP/HTTPS/SSH/SFTP/Syslog/Email).
	SNMP	Use this screen to configure the system's SNMP (Simple Network Management Protocol) settings.
	Time Settings	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 usernames, passwords, and privilege levels.
	Restart	Select this to reboot the BU and all connected RUs (not including EUs). 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 EUs / 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). Check Section 1.3.2 on page 9 and Section 1.3.3 on page 11 for details on BU and RU LED signaling. To open the **Home** screen from anywhere in the Web Configurator, just click **Home** on the Navigation Panel (blue bar), as shown below.

Figure 27 BU Home Screen
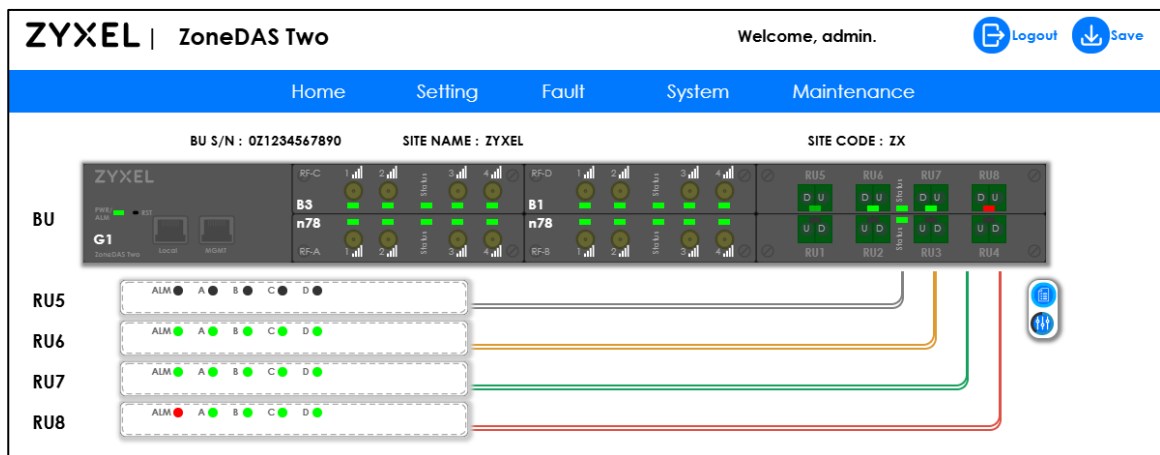
From the **Home** screen, if you move your mouse over an RF module, SD port, or a connected

RU/ Expander, the moused-over port or device will be encased in blue. This indicates that you can click on it to reach a dedicated screen for the port or device.

If you mouse over any of the lines connecting the RUs / EUs to the BU, the system will pop up basic information on the connection, such as Cable Loss, and states of the connection. The lines connecting each RU are also coded in different colors. These colors indicate the status of each connection, as follows:

• **Grey**: The device is plugged in but not ready.

• **Yellow**: The device needs calibration.

• **Green**: The device is "in service".

• **Red**: The device has alarm "Cable Error

Figure 28 EU Home Screen
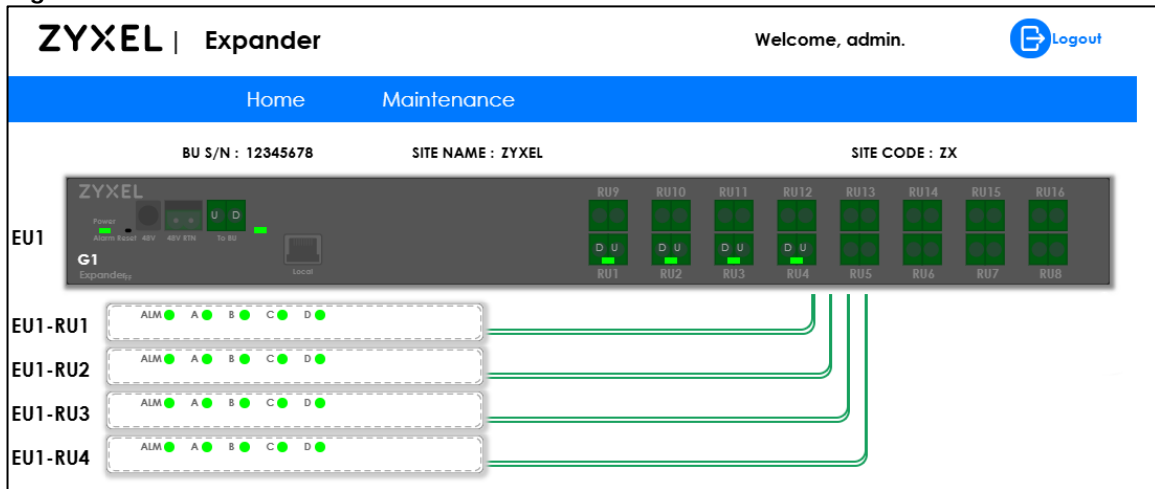
If you log into the EU directly, the **Home** screen shows a map similar to the BU's **Home** screen. The differences are as follows.

• This screen does not open RU screens to change RU settings and monitor power and status.

• This screen does not support triggering System Calibration.

The following table describes the EU **Home** screen.

Table 8 Home Screen: Legend

ITEM	DESCRIPTION
BU S/N	This shows the Base Unit's serial number.
Site Name	This shows the Site Name assigned to this ZoneDAS Two. The Site Name represents the 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 Two. 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.

System Report	Click the **System Report** icon to display a pop-up screen with device information, such as SN, HW version, FW version, cable loss, and band configuration, for all connected BU/EU/RU devices.

ZoneDAS Two System Report 12345678

2024-12-05 18:40:33

ID	SN	HW	FW	Cable Loss	Band
SYS					n78, n78, 3, 1 n78, n78, 3, 7
BU	S233K30100023 S233K30100024	9	200BUMB2P03		n78, n78, 3, 1 n78, n78, 3, 7
RU2	S233K11100078	2	200OPRU1P02	0.8/0.8 dB	7, n78a, 3, 1
RU3	S233K11100096	2	200OPRU1a03	0.8/0.8 dB	, n78a, 3, 1
RU4	S223K11100098	2	200OPRU1P02	0.8/0.8 dB	7, n78a, 3, 1
EU1	S233K29100012	3	200BUMB2P04	0.8/1.0 dB	
EU1-RU1	S223K29100055	4	200OPRU1a03	0.8/0.8 dB	n78a, n78a, 3, 7

[Supported Band Configurations]
B1/B8/B20/B3
B1/B8/N78/B3
B3/B3/N78/N78
B3/B8/N78/N78

System Calibration	Click on **System Calibration** to optimize system performance. During this process the system will detect the path loss of all RF pathways and adjust internal parameters accordingly. ZoneDAS Two can operate without the benefit of calibration, but performance will be adversely affected.

4.3 The BU Screen

Use the **BU** screen to show/modify a BU's basic information. Click anywhere on the **Home** screen's BU illustration to open the following screen.

Figure 29 BU Screen

The following table describes the labels on the BU screen.

**Table 9** BU Screen

LABEL	DESCRIPTION
Left Side Labels	
S/N	This entry shows the Base Unit's Serial Number.
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.
Location	Here you may enter a detailed description of the ZoneDAS Two BU's location, or upload a photo of this location.
Buttons	
LED Test	Click **LED Test** to activate a LED testing on this module for 1 minute. During this testing the LED will blink and toggle its color between green and red. You can also use this testing to quickly find where this module is placed.
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.

4.4 The BU-RF Screen

Use the **BU-RF** screen to monitor each BU-RF module's status and input power. Click anywhere on the **Home** screen's BU illustration to open the following screen. Alternatively, click on a BU-RF port to open the screen with the graph depicting that RF port's activities.

Figure 30 BU-RF Screen
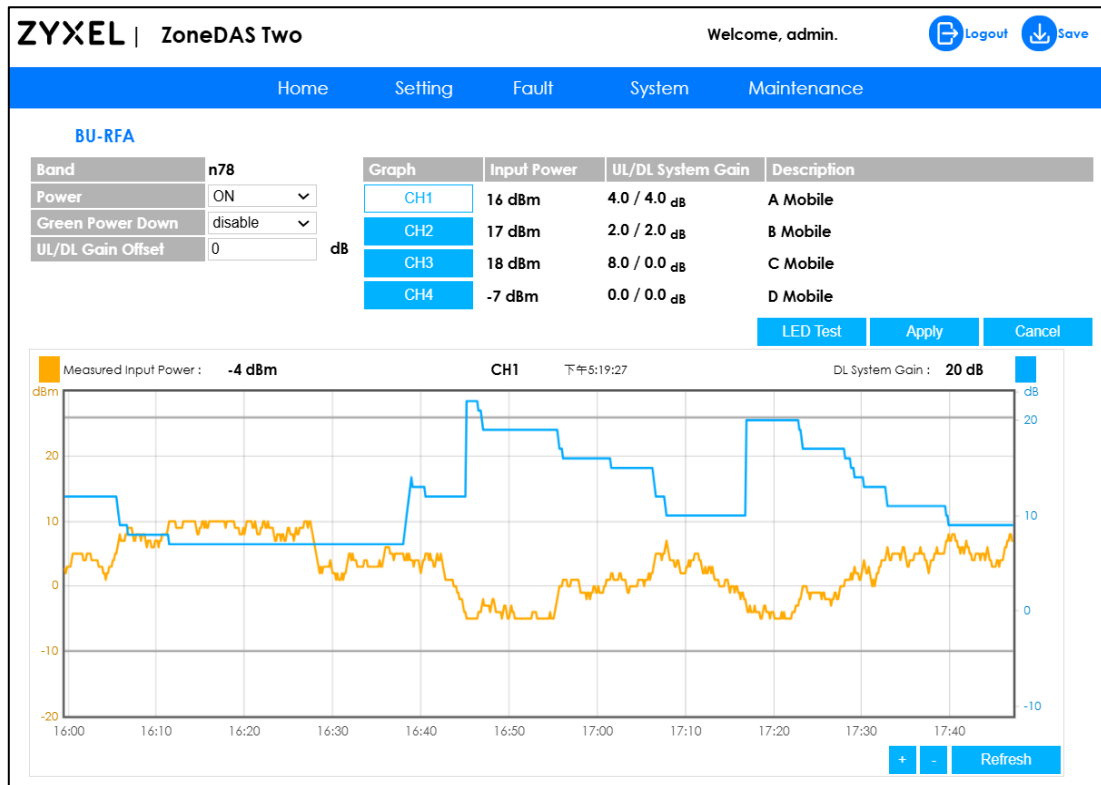
The following table describes the labels on the BU-RF screen.

Table 10 BU-RF Screen

LABEL	DESCRIPTION
Left Side Labels	
BU-RF Name • BU-RFA ~ BU-RFD	This blue text identifies the BU-RF this screen details. RF modules plugged directly into the BU are labeled BU-RFA~BU-RFD.
Band	This displays the RF signal's transmission frequency band.
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. **Turning OFF all installed BU-RFs will disable System Calibration!**
Green Power Down	Green Power Down, dictates whether a channel will go into Power-Saving Mode if there has been no input signal for a predefined time. The unit is hours, so simply input the number of hours the system should wait before switching the channel to Power-Saving Mode. When Power-Saving Mode is enabled and in effect for a channel, the Power LED for that channel's BU-RF module will repeatedly dim and brighten in the Web Configurator (not on the hardware) as indication. To disable Power-Saving Mode, simply select disable (factory default).
UL/DL Gain Offset	Use this to adjust the gain offset between UL/DL system gain.
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). Note that the BU's smart auto-levelling algorithm will automatically adjust system gain for each RF module to achieve its target value at full traffic load, as set in the RU settings table.
Input Power	Actual measured signal strength for the signal coming into the RF module.

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.
Description	The description or note related to this RF module or its signal. Often-used descriptions include the operator name for that signal and the frequency band for that channel.
Buttons	
LED Test	Click **LED Test** to activate a LED testing on this module for 1 minute. During this testing the LED will blink and toggle its color between green and red. You can also use this testing to quickly find where this module is placed.
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.
+	Click this to zoom in the graph, such that the time lapse between the vertical lines represents less and less time, right down to 10 seconds. This is equivalent to scrolling up on the mouse's scroll wheel while the pointer is placed over the graph.
-	Click this to zoom out the graph, such that the time lapse between the vertical lines represents more and more time, right up to 1 hour. This is equivalent to scrolling down on the mouse's scroll wheel while the pointer is placed over the graph.

4.5 The RU Screen

Use the **RU** screen to view the RU's status and its RF modules' output power and temperature. To reach this screen, choose an RU by clicking on its picture in the **Home** screen. To view the power/temperature graph for a particular RU-RF module, click on the blue button labelled RF-A, RF-B, RF-C, or RF-D. The module whose graph is currently being displayed will have its button shown in white instead of blue.

Figure 31 RU Screen

The following table describes the labels on the RU screen.

Table 11 RU Screen

LABEL	DESCRIPTION
RU Name	This blue text identifies the RU this screen details.
• RU1 ~ RU8	RUs plugged directly into the BU are labeled RU1~RU8.
• EU1-RU1 ~ EU8-RU16	RUs plugged into EUs are labeled EU1-RU1~ EU8-RU16, where the number after "EU" is the number assigned to the BU-SD slot that connects the EU.
Left Side Labels	
S/N	This entry shows the Remote Unit's Serial Number.
Up Time	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 EU ↔ RU connection. Cable loss increases with cable length and can be magnified by poor quality or damaged cable. Given proper cabling, ZoneDAS Two has effectively no BU ↔ EU cable loss.
Location	Enter a descriptive name for this RU's location, or upload a photo of this location.. For example 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.
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.
Band	This shows the frequency band currently used by the RU-RF.
Output/Input Power	This shows the current actual output/input power of this RU-RF module.
Calibration	Click here to trigger a single port's DL power calibration.
Description	This displays the description or note related to this RF module, which is configured in the **BU Setting** screen.
Buttons	
LED Test	Click **LED Test** to activate a LED testing on this module for 1 minute. During this testing the LED will blink and toggle its color between green and red. You can also use this testing to quickly find where this module is placed.
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.
+	Click this to zoom in the graph, such that the time lapse between the vertical lines represents less and less time, right down to 10 seconds. This is equivalent to scrolling up on the mouse's scroll wheel while the pointer is placed over the graph.
-	Click this to zoom out the graph, such that the time lapse between the vertical lines represents more and more time, right up to 1 hour. This is equivalent to scrolling down on the mouse's scroll wheel while the pointer is placed over the graph.
LED Test	Click **LED Test** to activate a LED testing on this module for 1 minute. During this testing the LED will blink and toggle its color between green and red. You can also use this testing to quickly find where this module is placed.

4.6 The EU Screen

Use the **EU** screen to show/modify an EU's basic information. Click anywhere on the **Home** screen's EU illustration to open the following screen.

Figure 32 EU Screen

The following table describes the labels on the EU screen.

Table 12 EU Screen

ITEM	DESCRIPTION
EU Name • EU1 ~ EU8	This blue text identifies the EU this screen details. EUs plugged directly into the BU are labeled EU1~EU8.
S/N	This entry shows the Expander Unit's Serial Number.
Up Time	This shows how long the EU has been operating for.
Cable Loss	This displays the amount of cable loss over the BU ↔ EU connection. Cable loss increases with cable length and can be magnified by poor quality or damaged cable.
Location	Here you may enter a detailed description of the ZoneDAS Two EU's location, or upload a photo of this location.
Buttons	
LED Test	Click **LED Test** to activate a LED testing on this module for 1 minute. During this testing the LED will blink and toggle its color between green and red. You can also use this testing to quickly find where this module is placed.
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.

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 Two will be up and running.

5.1.1 Available Functions

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

5.2 The BU Settings Screen

Use the **BU** screen to configure the BU's connection settings. This allows ZoneDAS Two 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 33 BU Settings Screen

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

Table 13 BU Settings Screen

LABEL	DESCRIPTION
DL Input Power	
Input	Enable/disable the signal input.
Power Level	Set the maximum possible power of the RF input signal from the base station (that is when it's under full load). If you don't know how to configure this value, you also could set it as **Auto** to detect the input power level automatically. You can also configure the behavior of the detect algorithm in the **Advanced Setting** screen. Note: You may need to set this to a fixed value if the input signal is unstable. An unstable signal may be more common if you get the RF signal through a repeater.
Alarm	Select this to generate a "no input signal" alarm when the input signal is missing.
Frequency Band	
Cellular	Select the mobile technology (as supported by the BTS) used by this RF channel, from 2G, 3G, and 4G. This setting is fixed as 5G for 5G modules.
DL/UL Center Frequency	Here, enter the "center frequency" of the frequency band used by this RF module for downlink transmission. For example, if we want the module to operate within a 20 MHz band from 1830 MHz to 1850 MHz, the "center frequency", or middle point between these figures, would be 1840. For uplink, the system will calculate the center frequency based on existing parameters and display it accordingly.
Bandwidth	Here, enter the "bandwidth" of this RF channel's frequency band. For example, if you want the module to operate from 1830 MHz to 1850 MHz, the "bandwidth" would be 20.
Description	Enter a description or note related to this input RF channel.
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 EU-enabled connections. Click **Setting** > **RU Settings** to see the following screen.

Figure 34 RU Settings Screen

The following table describes the labels on this screen.

Table 14 Settings > RU Settings

LABEL	DESCRIPTION
Left Side Labels	
RUx EUy-RUz	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. • EU1-RU1 ~ EU1-RU16 represent the 16 possible RUs connected to EU1's ports, from SD port 1 to SD port 16. The same applies to EU2, EU3, ... EU8.
Location	Enter a description of this RU's location.
Top Side Labels	
RF-A : Band X ~ RF-D : Band Z	**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. Bands X~Z represent the RF module's supported Band.
DL Output Power Signal Output / Maximum / Actual (dBm)	This is where you turn the signal output on/off and set the maximum output power for each RF module in each RU. Under **Max**, enter the output power cap for each RU-RF. Increasing this value expands coverage; lowering it reduces interference. **Actual** shows the current actual output power from this RU.
Buttons and Check boxes	
GSM ETSI compliant	Click this check box to limit output power to +13 dBm for RUs using GSM Band 8.
Apply all power values	Click this button 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.
Store Personal Notes	The **Personal Notes** section helps you make configuration memos when testing for optimal maximum outputs. These notes must be in plain text, and you must click the **Store Personal Notes** button (then the **Save** button) to actually save the notes.

5.4 The Advanced Settings Screen

Use the **Advanced Settings** screen to configure Auto Levelling and TDD settings for the BU. These settings represent internal parameters that the system uses for signal optimization. They are not meant for manual adjustment and it is recommended to select **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.

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

Figure 35 Advanced Settings Screen

5.4.1 Auto Levelling Settings

Auto-Levelling is an intelligent algorithm that ZoneDAS Two uses to adapt to widely varying, unpredictable input signal strengths.

Note: Through Auto-Levelling, ZoneDAS Two is able to maintain a stable and optimal output signal pattern despite changes to input signal strengths from Base Transceiver Stations.

The default settings of this smart algorithm have been determined during extensive field-operations and traffic loading scenarios and have been functionally adapted in technology and modulation schemes.

5.4.2 5G Baseband Synchronization Settings

Timing and synchronization are important and interrelated requirements for 5G wireless network performance. This Settings is used to configured the parameters to sync the phase and frequency of 5G baseband radio frames.

- TDD frame structure
  Duplex telecommunication means two-way transmission over a communication channel. Time Division Duplex (TDD) accomplishes this using different time slots for uplink and downlink signals over the same frequency. Enter the number of DL/UL slot of this TDD structure, which is chosen by all operators in the country or state.

- SSB ARFCN
  The Synchronization Signal/PBCH block (SSB) is used for synchronization, and the Absolute Radio Frequency Channel Number (ARFCN) is used to identify the frequency that SSB is used.
  You could keep this field empty and BU would search it automatically, or you could specify it here manually.

- 5G RF Testing
  This setting supported for RF testing, and disabled as default.

<div align="right">

CHAPTER 6
FAULT

</div>

6.1 Overview

The **Fault** screen allows you to monitor and control all alarm-related functionalities. 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 on page 47).
- Use the **Past Alarms** screen to view, filter, and search for past alarms (Section 6.3 on page 48).
- Use the **Alarm Settings** screen to modify the severity classification of alarms (Section 6.4 on page 49).
- Use the **System Log** screen to access and view the ZoneDAS System Log (Section 6.5 on page 52).

6.2 The Active Alarms Screen

An alarm is how ZoneDAS Two 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, while 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 36 Active Alarms Screen

The following table describes the labels on this screen.

Table 15 Active Alarms Screen

INDEX	DESCRIPTION
Index	This is the index number for the active alarm.
Condition	This allows you to filter active alarms by condition. Enter the condition you want to search for. See Section 6.4.2 on page 51 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 Two then searches for all alarms of that severity or higher. See Section 6.4.1 on page 51 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, 2025, you would type "2025-01-22". If you want to see all alarms between 7 pm and 8 pm, you would type "19:" If you follow that with 26, for "19:26", you would see all alarms from 7:26 pm.
Source	Enter the name of the system partition for which you wish to locate active alarms. Refer to Table 1 on page 9 and Table 4 on page 12 to learn more about the various system partitions on ZoneDAS Two.
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.
Clear ALL	Click the **Clear ALL** button to clear all removable alarms, meaning those with a **Clear** button to the right of the alarm.
Refresh	Click **Refresh** button to search the system again for new or remaining alarms.

Note: ZoneDAS Two can store up to 2000 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 37 Past Alarms Screen

The following table describes the labels on this screen.

Table 16 Past Alarms Screen

INDEX	DESCRIPTION
Index	This is the index number for the past alarm.
Condition	This allows you to filter past alarms by condition. Enter the condition you want to search for. See Section 6.4.2 on page 51 for more information on the various alarm conditions.
Severity	This allows you to filter past alarms by severity. Select the severity level of the active alarm you want to search for. ZoneDAS Two then searches for all alarms of that severity or higher. See Section 6.4.1 on page 51 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 for January 22, 2025, you would type "2025-01-22". If you want to see all alarms between 7 pm and 8 pm, you would type "19:" If you follow that with 26, for "19:26", you would see all alarms from 7:26 pm.
Source	Enter the name of the system partition for which you wish to locate past alarms. Refer to Table 1 on page 9 and Table 4 on page 12 to learn more about the various system partitions on ZoneDAS Two.
Clear ALL	Click the **Clear ALL** button on the top right to clear the log of all past alarms.
Refresh	Click **Refresh** button to show all remaining past alarms.

Note: ZoneDAS Two can store up to 2000 past alarm entries. Once it reaches the limit, each new entry overwrites the oldest one.

6.4 The Alarm Settings Screen

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

Figure 38 Alarm Settings Screen

The following table describes the labels on this screen.

Table 17 Alarm Settings Screen

INDEX	DESCRIPTION
Index	This is the index number of the alarm.
Condition	This column contains a simplified description of each alarm. See Section 6.4.2 on page 51 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 Section 6.4.1 on page 51 for more information on alarm/event severity types.
Syslog	Select the check box to log an alarm in the syslog. Clear the check box to not log the alarm in the syslog.
SNMP-Trap	Select the check box to send alarms of this type through the SNMP trap. Clear the check box to stop the system from sending SNMP traps for alarms of this type.
SNMP-Delay	If SNMP-Trap is selected 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 Two on-site.
Email	Select the check box to send alarms of this type through the email. Clear the check box to stop the system from sending email for alarms of this type.
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 Two Alarms are categorized into the following:

Table 18 Alarm Severity Levels

SEVERITY	DESCRIPTION
Event	An Event is simply 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 Two device (such as a service, a port, a power supply, and so on) has stopped functioning and needs attention.
Major	A major alarm indicates that a device is completely down or in danger of going down. This type of problem must be addressed immediately. Major alarms are emphasized using orange text.
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. Critical alarms are emphasized with red text.

Note: These represent the factory default Alarm Severity Levels. You can modify any alarm's severity level as appropriate for your scenario.

6.4.2 List of Alarms/Events/Conditions

The following table describes all the alarms, events, and conditions that ZoneDAS Two may provide.

Table 19 Alarms and Events

| ALARM / EVENT	DESCRIPTION
(201)alarm_clear	An alarm has been manually cleared.
(202)login_fail	There was a system login failure.
(203)fw_upgrade_notify	ZoneDAS has entered a firmware update process.
(204)vpn_connection_failed	Cannot connect to Virtual Private Network (VPN). Please check VPN settings.
(301)hw_error	There is a hardware monitoring failure.

(302)overheat	ZoneDAS detects a temperature threshold violation in the BU or an RU-RF module. If the latter is the case, the system will shut down the entire RU. This is Step 3 in the 3-step temperature control system.
(303)fan_error	ZoneDAS detects a fan speed threshold violation in the BU.
(304)unknown_device	The BU can connect to and communicate with this device, but cannot identify the device. This is likely because the device is from a separate product line.
(305)fan_missing	A fan module has been removed.
(306)pull_out	A BU-RF or BU-SD or RU module has been removed.
(307)start_service	A module is ready to start service.
(308)overheat_prevention	An RU-RF module is getting too hot and the system has reduced its power output to prevent overheating. This is Step 1 in the 3-step temperature control system.
(309)awaiting_full_cooldown	An RU-RF module has overheated despite overheat prevention and the system has shut down the module for cool down. This is Step 2 in the 3-step temperature control system.
(401)connection_timeout	The device has been identified but cannot properly connect.
(402)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**.
(403)out_of_manegement	The module is out of service and is not responding to the BU. Here, "module" refers to anything that can be plugged/unplugged while the system is on (that is BU-RF, BU-SD, EU, RU). This includes instances when a module was plugged in before a reboot but missing after.
(404)wrong_cable_connection	The cable is connected to wrong device.
(501)frequency_lock_failure	The BU or RU's RF module cannot detect or lock onto the operator's frequency. This may mean that the setup frequency is incorrect.
(502)storage_failure	A module cannot access its non-volatile memory.
(503)band_mismatch	The configured RF input frequency value does not fall within range of the RF module's frequency band. In other words, the RU-RF module does not match its corresponding BU-RF module, as positioned on module slot A, B, C or D.
(504)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.
(506)no_input_signal	An existing RF signal going into an BU-RF module has gone missing or is too weak to be detected and processed (that is dropped below -5 dBm for > 20 seconds).
(507)dl_freq_not_set	If the BU tries to start Service while the downlink frequency for any installed RF module (A, B, C or D) has not yet been specified, the system will raise this alarm. Once a valid frequency has been entered, the alarm will automatically clear.
(508)cable_error	During System Calibration, if an RF pathway fails to calibrate while going through one of the four twisted pairs in the Ethernet cable between the BU and RU/EU or between EU and RU, the system will raise this alarm, identifying both the destination device and the particular twisted pair (A,B,C, or D).
(509)unsupported_band_config	The plugged band configuration is not supported. Please check with system report which band configurations are supported, and change your band configuration.
(512)power_calibration_fail	There is an error when running system power calibration, and this RU could not finish the calibration. In this situation, the RU would load old setting or default setting.
(513)output_power_unreachable	After power calibration, RU-RF's output power can't reach the configured power level.

6.5 The System Log Screen

ZoneDAS Two 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 Two will send all its system log entries. To see the **System Log** screen, click **Fault** > **System Log** to open the following screen.

Figure 39 System Log Screen
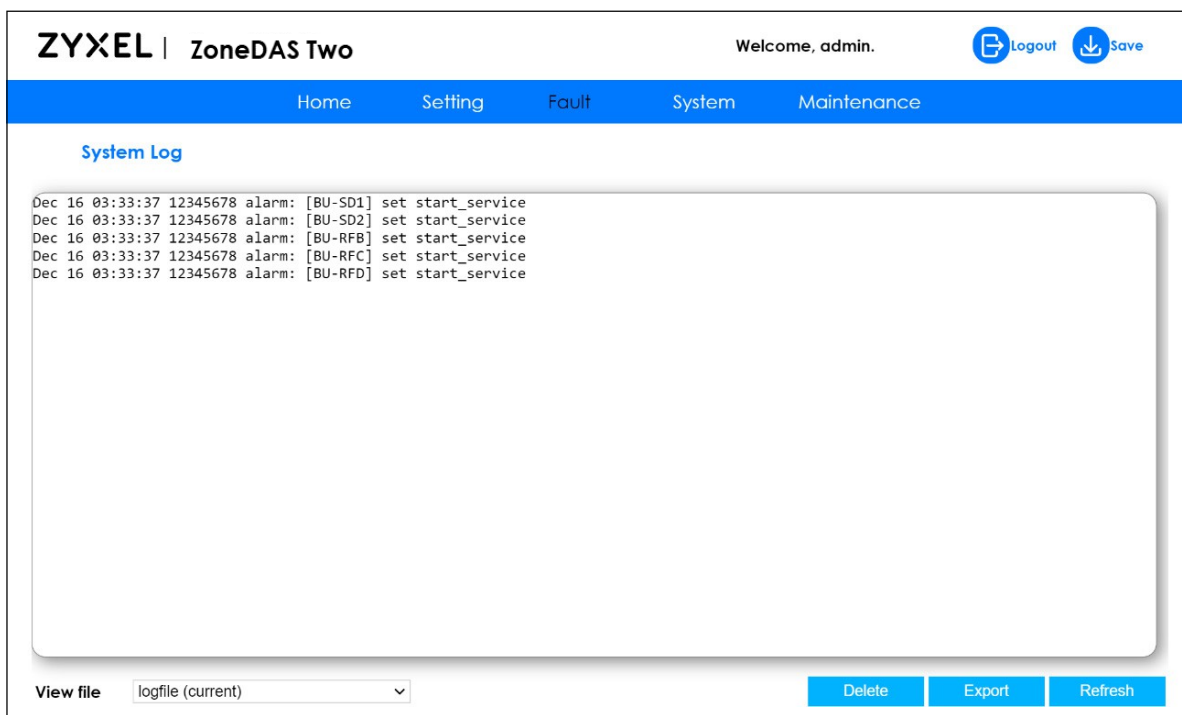
The following table describes the labels on this screen.

Table 20 Fault > System Log

INDEX	DESCRIPTION
View file	ZoneDAS Two supports a current log file and up to 99 history log files, with each file containing up to 1MB of log data. Choose the file "logfile (current)" or "logfile.1" ~ "logfile.99" to display its contents on screen.
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 compress all log files to a zipped file. A window will pop up for you 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 Two. They let you control how ZoneDAS Two can be accessed, including options for VPN and SNMP. They also allow you 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 Two (Section 7.2 on page 54).
- Use the **SNMP** screen to configure SNMP options and settings for central management (Section 7.3 on page 56).
- Use the **Time Settings** screen to configure time and date settings, including time zones and Daylight- Saving Time (Section 7.4 on page 59).

7.2 The Network Screen

The **Network** screen is where you can configure ZoneDAS Two to enable further computer access to the Web Configurator. Use **Network Settings** to set up direct connections for CAT7 cable direct access through the **Local/MGMT** port and Virtual LAN (VLAN) connections. **VPN Settings** offers access controls for connection through Virtual Private Network.

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

Figure 40 Network Screen

The following table describes the labels on this screen.

Table 21 Network Screen

INDEX	DESCRIPTION
Network Settings	
MAC Address	This is the MAC Address of the ZoneDAS Two BU **MGMT** port.
MGMT Interface	Check DHCP to enable having the **MGMT** port acquire an IP from a **DHCP** server automatically. The MGMT port is reserved for remote management, you cannot disable it.
MGMT IP/mask	This is where you can input an alternative IP and subnet mask for accessing ZoneDAS Two from a local console.
Local MAC	This is the MAC Address of the ZoneDAS BU Local port.
Local Interface	Check this box to **Enable** ZoneDAS control through the **MGMT** port. Uncheck to disable. The Local port is reserved for local maintenance.
Local IP/mask	This is where you can input an alternative IP and subnet mask for accessing ZoneDAS from a local console.
Default Gateway	This is where you can set a new default gateway for the ZoneDAS Two BU.
VLAN Interface	Click and check the box to enable VLAN access to this ZoneDAS Two BU.
VLAN ID	This is where you can set the BU's VLAN ID.
VLAN IP/mask	This is where you can input the IP and subnet mask for accessing the ZoneDAS Two through VLAN.
SNMP port	The port to use for connecting via the SNMP protocol.
HTTPS port	The port to use used for connecting via the HTTPS protocol.
SSH/SFTP port	The port to use for connecting via the SSH/SFTP protocol.
Syslog IP:port	The IP and port to use for connecting to the Syslog server.
VPN Settings	

OpenVPN	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.
Password	Enter the login password for the OpenSSL VPN secure connection.
Import .opvn File	Click the **Upload** button to import a .opvn file into the ZoneDAS Two for use in establishing the OpenVPN connection. Once a file has been uploaded, the box beside the **Upload** button will say "Exist".
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 Two do not match those of the OpenVPN server. **Inconsistent Compression** shows when the LZO compression schemes used by ZoneDAS Two 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. If connection failed, you also could export the log file to find out the root cause.
Assigned IP	Enter the IP address and port number of the computer on which OpenVPN is installed. The system will automatically ping the IP and display a check mark after the IP address box if it succeeds. If it does not, it will display two exclamation marks (!!) instead.
Email Settnigs	
SMTP Server	Click and check the box to enable sending Email from this ZoneDAS Two BU. For network security, SSL/TLS is required and it could not be disabled.
Server Address	The IP and port to use for connecting to the SMTP server.
Username	The username to use for SMTP authorization.
Password	The password to use for SMTP authorization.
Mail From	The address that indicates the sender of the message.
Mail To	The address for the main recipients of this email. You could enter multiple address which separated by comma (,).
Send Alarm	Click and check the box to enable sending alarm notification via Email. Click the Test button to send a testing alarm notification for verification.
System Report	Select the time and day to enable sending scheduled system report via Email. Click the Test button to send a testing system report for verification.
Buttons	
Apply and Save	This is equivalent to clicking **Apply** on this screen then clicking **Save** button on the title bar.
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.

7.3 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. ZoneDAS Two 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 41 SNMP Management Model
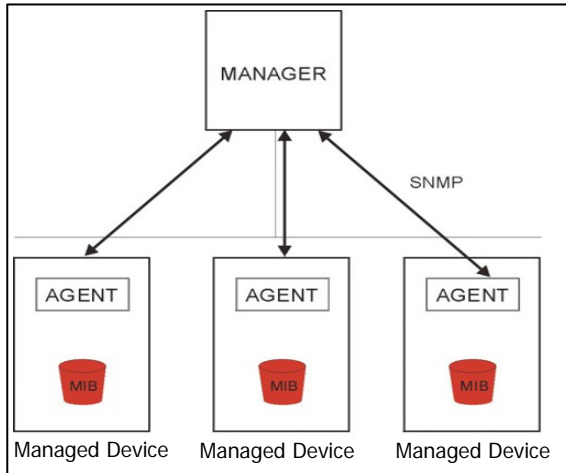
An SNMP managed network consists of two main types of components: agents and a manager.

An agent is a management software module that resides in a managed device (that is 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 Two 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 42 SNMP Screen

The following table describes the labels on this screen.

Table 22 SNMP Screen

INDEX	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.
SNMPv2 Settings	
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.
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.
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 more secure 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.
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. The system will automatically ping the IP and display a check mark after the IP address box if it succeeds. If it does not, it will display two exclamation marks (!!) instead.
Port	Enter the port number to which the BU sends SNMP requests.
Buttons	
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.

7.4 The Time Settings Screen

The **Time Settings** 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 Settings**.

Figure 43 Time Settings Screen

The following table describes the labels on this screen.

Table 23 Time Settings Screen

INDEX	DESCRIPTION
Current Date, Time (all in orange)	This field displays the date (including day of week), and time used by ZoneDAS Two, in large, orange numbers.
Set Time Automatically	
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).

Enable	Select this check box to have the ZoneDAS Two synchronize its system time with a predefined NTP (Network Time Protocol) server. To make this work, ZoneDAS Two must have direct Internet access through its **MGMT** port. Typically, this means a CAT7 cable must be plugged from the **MGMT** port directly into an Internet access point.
NTP Server Address	Enter the IP address or URL of the above-mentioned time server. The ZoneDAS Two will automatically ping the IP and display a check mark after the IP address box if it succeeds. If it does not, it will display two exclamation marks (!!) instead. If you keep this setting empty, it will sync the time from a Google NTP server.
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.
Change Date and Time	
Date	Enter the desired system date in this field, in YEAR, MONTH, DATE format.
Time	Enter the desired system time in this field, in 24-hour format.
Set	Click **Set** to have the system use the above-shown date and time.

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 EUs/RUs (Section 8.2 on page 61).
- 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 on page 63).
- Use the **User Account** screen to manage user accounts and privileges (Section 8.4 on page 64).
- Use the **Restart** screen to reboot ZoneDAS Two BU and connected RUs (Section 8.5 on page 67).

8.2 The Firmware Screen

ZoneDAS Two upgrades its firmware in 2 steps. First the firmware is uploaded into ZoneDAS Two 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 through your Zyxel distributor. After a successful upload, the firmware can be installed. After firmware installation, all upgraded devices will reboot.

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

Figure 44 Firmware Screen

The following table describes the labels on the **Firmware** screen.

Table 24 Firmware Screen

LABEL	DESCRIPTION
Unit Name	The first column lists all units that support firmware upgrade in this column, such as MB, RF, EU, SD, RU, LE, EXP. **G1/G2:** ZoneDAS Two could combine two groups as one, this name is used to identify the group. **MB**: BU/EU mother board. **EXP**: An EU trunk unit connected to the BU. **LE**: Line extender unit between the BU and EU, the BU and RU, or the EU and RU. The units under EUx are hidden in a folder by default. Click + to expand the folder to show them, or click − to collapse this folder to hide them.
Serial Number	This displays the device's serial number.
Running Firmware	This displays the firmware version each ZoneDAS Two device is using right now. When the unit is under upgrading, this field displays **Scheduled to upgrade**, **Ready to upgrade**, **Upgrading**, or **xx%**. Click the heading row to display a popup where you can select **Auto**, **All**, or **None**, that you could select multiple units for firmware upgrade. **Auto**: Select those units where the running firmware version is not the same as standby firmware version. **All**: Select all units. **None**: De-select all units. To force upgrade some units, you can select the unit manually by selecting the check box to the right of the unit's firmware version.
Standby Firmware	Firmware versions listed under this label have been uploaded into ZoneDAS Two memory but have not yet been installed. This field shows **FW already running, no need for upgrade** If the running firmware version is the same as standby firmware version.
Package Version	ZoneDAS Two firmware is released as a package that includes all modules' firmware. This field displays the package version.
Buttons	
Upload	Click **Upload** to upload a firmware file into the ZoneDAS Two BU's memory. ZoneDAS Two will automatically decode the firmware package and upgrade each system part accordingly.
Schedule	Once an appropriate firmware file has been uploaded into the ZoneDAS Two BU, you may click **Schedule** to set a future time for the system to automatically install (activate) the firmware. Note: Use this 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.

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

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

Figure 45 Network Temporarily Disconnected
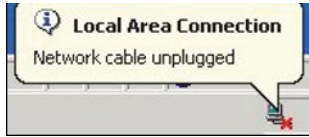
After two minutes, log in again and check your new firmware version in the **Maintenance** > **Firmware** screen.

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. On ZoneDAS Two, configuration files 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 are plain ASCII and use the ".txt" extension. Use the **Config File** screen to save and restore your configuration file(s).

Note: Once your BU is properly configured and functioning smoothly, we highly recommend 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.

Figure 46 Config File Screen
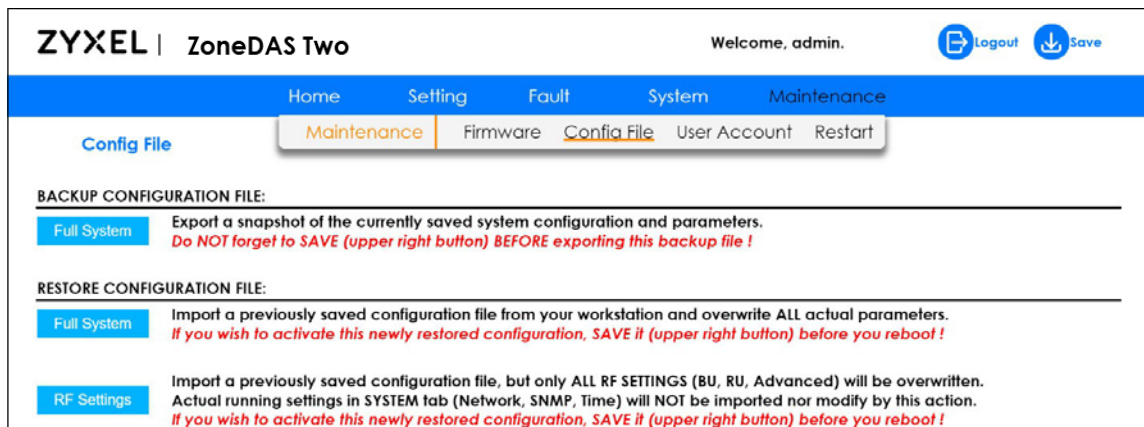
Click **Maintenance** > **Config File** to open the following screen.

The following table describes the labels on this screen.

Table 25 Config File Screen

LABEL	DESCRIPTION
Backup Full System	Click **Full System** (under **Backup Configuration File**) to save the current configuration on your computer. The system will create a configuration file, give it a name, and save it to the console's default download directory.

Restore Full System	Click **Full System** (under **Restore Configuration File**) 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 of the screen) to commit all values to permanent memory.
Restore RF Settings	Click **RF Settings** (under **Restore Configuration File**) to replace all RF settings (that is those in the **BU Settings**, **RU Settings**, and **Advanced Settings** screens) with settings stored in a configuration file. The browser will pop up a file window for the user to select the desired config file. Once selected, the system will apply all the RF settings stored within the configuration file. If you are 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 the Web Configurator. Settings include username, password, and privileges. Click **Maintenance** > **User Account** to open this screen.

Figure 47 User Account Screen

The following table describes the labels on this screen.

Table 26 User Account Screen

LABEL	DESCRIPTION
Administrator	
Password	Specify the password for the **admin** account. Typed characters are displayed as dots (•) in all password fields. Password requirements are listed below, under **Account Information** > **Password**.
Confirm Password	To ensure that the Administrator's password has not been mistyped, please enter the exact same password a second time.
Apply	Click **Apply** to save administrator password 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.
Additional User Accounts	
User Name	Enter a descriptive name for the user account. The username may have 3~31 characters. Specifically, it can include 0~9, a~z, and @%+/!#$^.(){}[]~-_. Note: NO CAPITAL LETTERS allowed!

Password	Specify the password for this account. The password must have 8~31 characters. Specifically, it can include 0~9, a~z, A~Z, and @%+/!#$^.(){}[]~-_;:,*= A strong password must be at least 8 characters long, which should contain different types of characters, including: •Uppercase letters (A~Z) • Lowercase letters (a~z) •Numbers (0~9) • Non-alphanumeric characters, such as @%+/!#$^.(){}[]~-_;:,*=
Confirm Password	Enter the exact same password again, for verification.
Privilege Level	Select the privilege level for the user. There are four types of privilege levels. • **End-User** – A user of this level can access most screens but cannot make 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 additional user account setting 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 additional user account changes made since last clicking **Apply**.
List of Accounts	
Index	This is the index number assigned to each user account. ZoneDAS Two supports up to 7 user accounts.
User Name	This is the name of the user assigned to this account.
Privileges	This is the privilege level granted to this account.
Action	Click the **Edit** icon to edit this user account. Click the **Delete** icon to remove this user account.

With regard to user privileges, please note that each menu option has four kinds of access privileges:
Read/Write, **Read Only**, **Write Only**, and **Hidden**. They differ as follows:

Read/Write:A user with this level of access privilege can access the page, view all settings on the page, make any changes, and apply them via the **Apply** button.

Read Only:A user with this level of access privilege can access the page and view all settings but cannot make any changes. The **Apply** button and all user-adjustable fields and are greyed out.

Write Only:This access privilege level only applies to screens that have no information to read, such as **Save** and **Restart**.

Hidden:A user with this level of access privilege for a page cannot even see the page. It simply would not appear as a menu option. If all menu options within a menu category are hidden for a user, then the entire category would be hidden.

The following table details exact privileges given to End-Users, Technicians, Super-Users, and Administrators.

Table 29   User Privileges

MENU CATEGORY	MENU OPTION	ADMINISTRATOR	SUPER-USER	TECHNICIAN	END-USER
Home	Home	Read/Write	Read/Write	Read/Write	Read Only
	BU	Read/Write	Read/Write	Read/Write	Read Only

	RF	Read/Write	Read/Write	Read/Write	Read Only
	EU	Read/Write	Read/Write	Read/Write	Read Only
	RU	Read/Write	Read/Write	Read/Write	Read Only
Settings	BU Settings	Read/Write	Read/Write	Read/Write	Read Only
	RU Settings	Read/Write	Read/Write	Read/Write	Read Only
	Advanced Settings	Read/Write	Read/Write	Read Only	Hidden
Fault	Active Alarms	Read/Write	Read/Write	Read Only	Read Only
	Past Alarms	Read/Write	Read/Write	Read Only	Read Only
	Alarm Settings	Read/Write	Read/Write	Read Only	Hidden
	System Log	Read/Write	Read/Write	Read/Write	Read Only
System	Network	Read/Write	Read/Write	Read/Write	Hidden
	SNMP	Read/Write	Read/Write	Read/Write	Hidden
	Time Settings	Read/Write	Read/Write	Read/Write	Hidden
Maintenance	Firmware	Read/Write	Read/Write	Read/Write	
	Config File	Read/Write	Read/Write	Read/Write	Hidden
	User Account	Read/Write	Read Only	Hidden	Hidden
	Restart	Write Only	Write Only	Write Only	Hidden
	Save	Write Only	Write Only	Write Only	Hidden

8.5 The Restart Screen

Use **Restart** to reboot the ZoneDAS Two BU and connected 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 Two will restart.

Figure 48 Restart Window

Restarting this device may take about **60 seconds**.
Do you want to restart this device?

Remember to SAVE (with the upper right button) BEFORE restarting this device!

Ok   Cancel
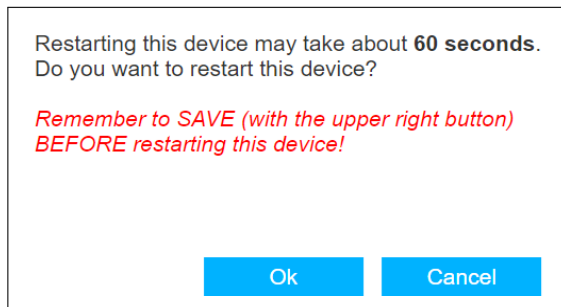
Copyright

Copyright © 2024 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and

Statement United States of

The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

• This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operations.

• Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
• This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES Statement

CAN ICES (A) / NMB (A)

European Union

The following information applies if you use the product within the European Union.

CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT stack other devices or equipment on the device.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- DO NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- DO NOT use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Keep the air filters clean, in order to ensure sufficient airflow.
- Connect the frame ground before you connect any other cables or wiring and disconnect all cables or wiring before disconnecting the frame ground.
- Earthing connection has to be installed by service personnel.
- The length of exposed (bare) power wire should not exceed 12 mm.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:

  - Install the power supply before connecting the power cable to the power supply.

  - Unplug the power cable before removing the power supply.

  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.

- The following warning statements apply, where the disconnect device is not incorporated in the equipment or where the plug on the power supply cord is intended to serve as the disconnect device,

  - For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device shall be incorporated external to the equipment;

  - For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and shall be easily accessible.
- CLASS 1 LASER PRODUCT
- APPAREIL À LASER DE CLASS 1
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

IMPORTANT SAFETY INSTRUCTIONS

1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before servicing this device.

2 Do not open the device. Opening or removing covers can expose you to dangerous high voltage points or other risks. Please contact your vendor for further information.

3 Warning! Use the fan module handles when pulling out or pushing in the fan module. Be careful not to put fingers or objects inside the fan module.

4 Caution! The RJ-45 jacks are not used for telephone line connection.

5 Caution! To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

6 Caution! Use a UL listed or CSA Certified DC power source to connect to the DC power input.

1 Avertissement : Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil

2 Ne pas ouvrir l'appareil. L'ouverture ou le retrait des couvercles peut vous exposer à des points comportant des tensions élevées ou à d'autres risques. Veuillez contacter votre vendeur pour plus d'informations.

3 Avertissement : Utiliser les poignées du châssis pour retirer ou insérer le module de ventilation Faites attention à vos doigts et à tout objet quand vous manipulez le ventilateur

4 Attention : Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.

5 ATTENTION – Pour réduire les risques d'incendie, utiliser uniquement des conducteurs de télécommunications 26 AWG au de section supérleure.

6 Attention: Utilisez une source d'alimentation CC répertoriée UL ou certifiée CSA pour la connexion au bloc d'alimentation CC.

Environment Statement

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el

momento de desechar el

producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.
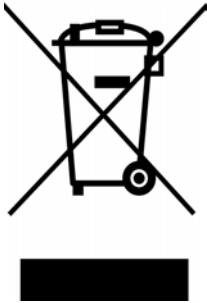
About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Table 29   Explanation of the Symbols

SYMBOL	EXPLANATION
∿	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
⎓	Direct current (DC): DC if the unidirectional flow or movement of electric charge carriers.
⏚	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
▣	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: https://service-provider.zyxel.com/global/en/gpl-oss-software-notice.