FREEWAVE

SET-UP GUIDE

Elements™ ES1000 with FreeWave Zentry™ powered by zero trust

FW_ES1000_SetUp_Guide
Revision Sep 2025

This guide provides the steps to establish remote connections to your edge devices from anywhere in the world through your ES1000 and the FreeWave portal.

STOP!

Before going further, please contact
support@freewave.com
to create a FreeWave Zentry account.

The FreeWave Support is available to guide you through the instructions below and ensure you get the most out of Zentry and the ES1000.

Table of Contents

The FreeWave ES1000 goes beyond traditional cellular gateways and standard network devices. Built on FreeWave's Zentry zero-trust security platform and managed through the Zentry Console, the ES1000 enables virtually instant access and management your edge devices on an advanced security fabric.

YOU WILL NEED

1. A FreeWave Zentry account
2. A computer with a web browser, internet connectivity and an available USB-C port
3. A USB-C cord
4. Power

KIT CONTENTS

1. ES1000 unit
2. Claim token code
3. Power supply
4. Antennas
5. 24V cable

Purpose Of This Guide

This guide provides the steps to establish remote connections to your edge devices from anywhere in the world through your ES1000 and the FreeWave portal.

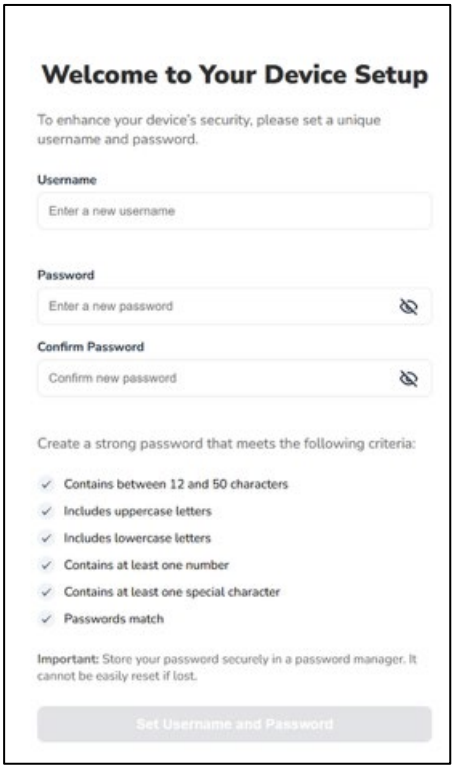
Configuring Your ES1000

1. Connect your ES1000 to a computer using a USB-C cable (not provided).
2. Navigate to http://192.168.137.2 using your web browser.

NOTE: this address uses http, not https. Secure protocol will be available soon.

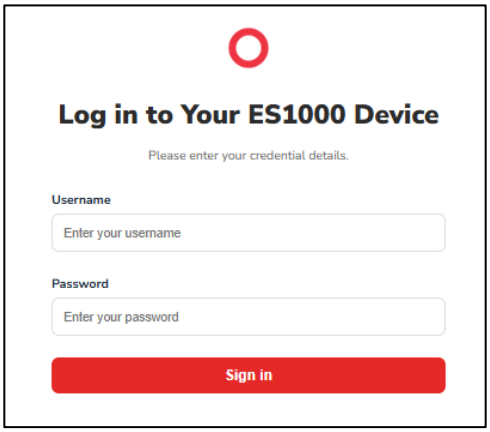
Create a Username and Password

You will be prompted to create a username and password. Password requirements are indicated in the setup screen.



NOTE: This password is non-recoverable. Please store it in secure place before proceeding.

Login using the username and password created above.



Out-Of-The-Box Configuration

Your ES1000 default configuration utilizes the pre-activated, universal LTE cellular interface as the WAN interface to connect to the internet. The LAN (local area network) is configured to use the Ethernet ports in bridged mode).

Note: Wi-Fi is disabled by default for security purposes.

To Make Network Configuration Changes

The below sections outline some of the many configurations available on the ES1000 that will suit your use cases.

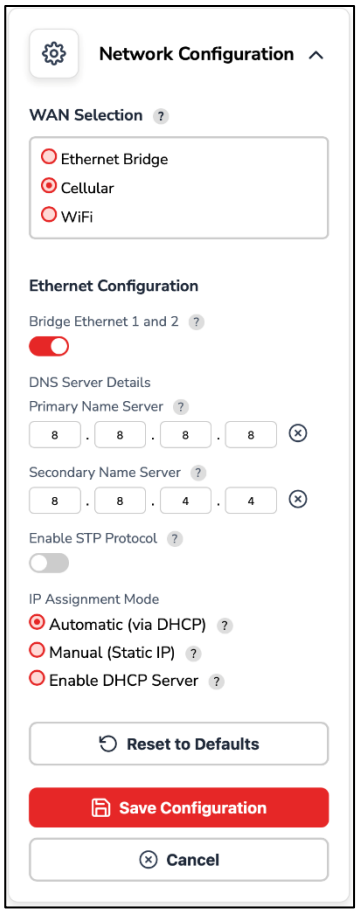
Important Note: Like all networking devices, the ES1000 is highly configurable to serve a broad spectrum of complex use cases. If you are at all unsure how to manage networking devices to serve your networking needs, please contact FreeWave Support for assistance.

To Configure WAN and LAN Interfaces

Many WAN and LAN interface configuration combinations are possible. This section describes default settings to manage Ethernet ports, how to bridge or utilize separate capabilities for Ethernet ports 1 and 2 (with cellular WAN).

Note: Ethernet ports 1 and 2 support different link modes

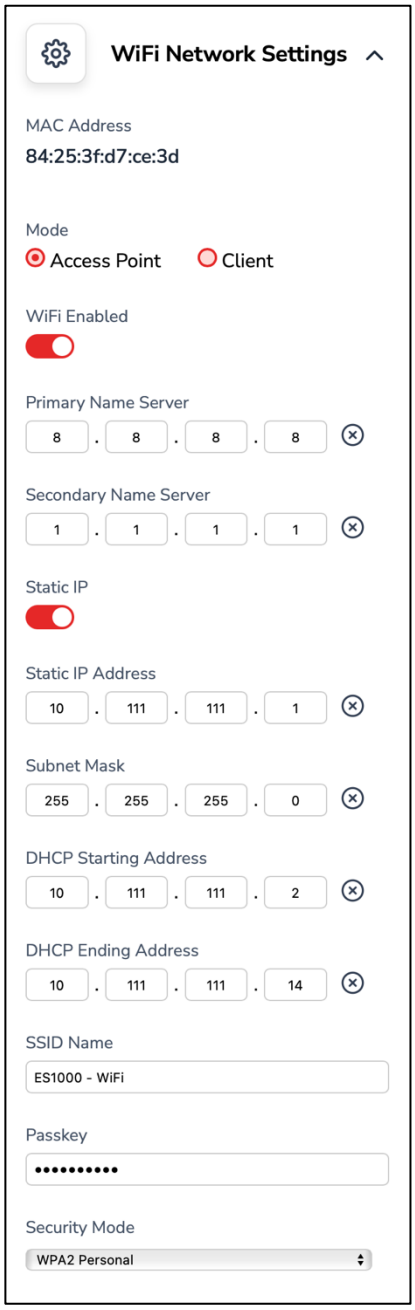
Ethernet Port #1	Ethernet Port #2
Supported Link Modes:	Supported Link Modes:
10baseT/Half 10baseT/Full 100baseT/Half 100baseT/Full 1000baseT/Full	10baseT/Full 100baseT/Full 1000baseT/Full



1. Click Network from main menu
2. Click the gear symbol next to Network Configuration to expand detailed menu shown.
3. Select the WAN interface you would like to use. In this example we will be selecting the Cellular interface.
4. Click the toggle underneath Ethernet Configuration to Bridge Ethernet 1 and 2
    a. For Primary Name Server use 8.8.8.8
    b. For Secondary Name Server use 8.8.4.4
5. Set primary name server.
6. Select Automatic (via DHCP).
7. Click “Save Configuration” to change the WAN interface.

To Configure Your ES1000 as a Cellular Gateway

This section describes how to create a Wi-Fi access point (like a cellular mobile hotspot) so you can connect devices to your ES1000 via Wi-Fi using cellular for internet connectivity.



1. From the main menu, select the Wi-Fi Connections tile.
2. Click on the gear next to Wi-Fi Network Settings
3. Select Access Point in the “Mode” setting
    a. Enable Wi-Fi.
    b. Enter the primary and secondary name servers you would like to use.
        i. If you are unsure, use 8.8.8.8 (Google) and 1.1.1.1 (Cloudflare).
    c. Enable Static IP.
    d. Enter Static IP address, subnet mask, DHCP starting and ending address information.
        i. If you are unsure, use information as indicated on the right.
    e. Enter the SSID you want the ES1000 to broadcast.
    f. Select Security Mode appropriate for your application.
    g. Enter a password you want to connect the above established SSID.
4. Save the Wi-Fi configuration.

From the Console screen, you should see “Connected” on the Cellular tile and “Interface Up” on the Wi-Fi tile.

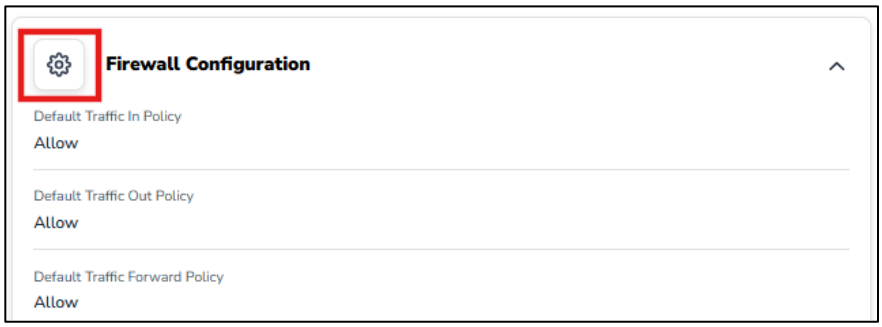
Your ES1000 is now set up as a Wi-Fi access point using cellular as a WAN interface.

To Configure NAT/Firewall Settings

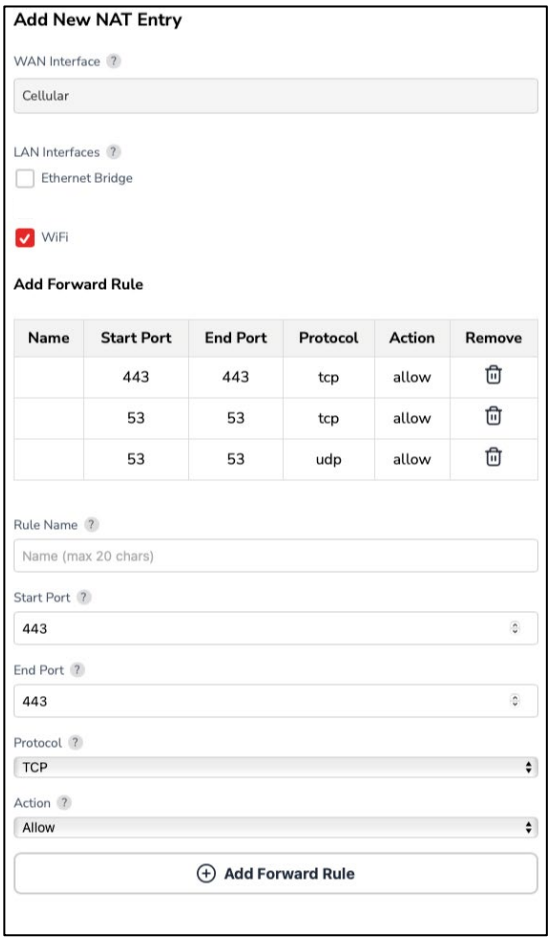
These settings allow devices connected to the ES1000 via Wi-Fi to get internet connection over the cellular interface.

We will be setting up your NAT for port forwarding for ports 443 TCP, 53 TCP, and 53 UDP.

1. From the main menu, navigate to the Firewall/NAT settings tile.
2. Click the gear symbol next to Firewall Configuration.



3. Click the Add NAT Entry button.
4. Choose Cellular as your WAN Interface.
5. Select WiFi under LAN Interfaces.
6. Type in 443 for Start Port.
7. Type in 443 for End Port.
8. Select TCP from Protocol dropdown menu.
9. Click Add Forward Rule button, repeat process for ports 53 TCP and 53 UDP.
10. Once finished, click Add NAT Entry.
11. Click Save Configuration button at bottom of page.



Configuring FreeWave Zentry: Creating a Zero-Trust Network

To create a remote connection to the ES1000, or anything connected to the same subnet as the ES1000, you will need to configure at least one other device to create a point-to-point connection. Most use a laptop for the initial proof-of-concept as it affords ease of setup and configuration.

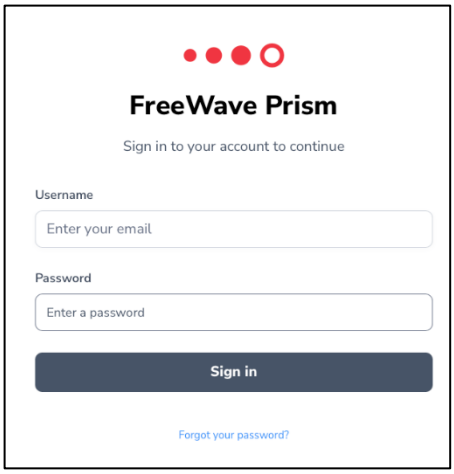
Once you have the zero-trust client installed on your computer you will create an identity for your device. Once completed, you will create a "function" so you can manage devices connected to the ES1000 in the field.

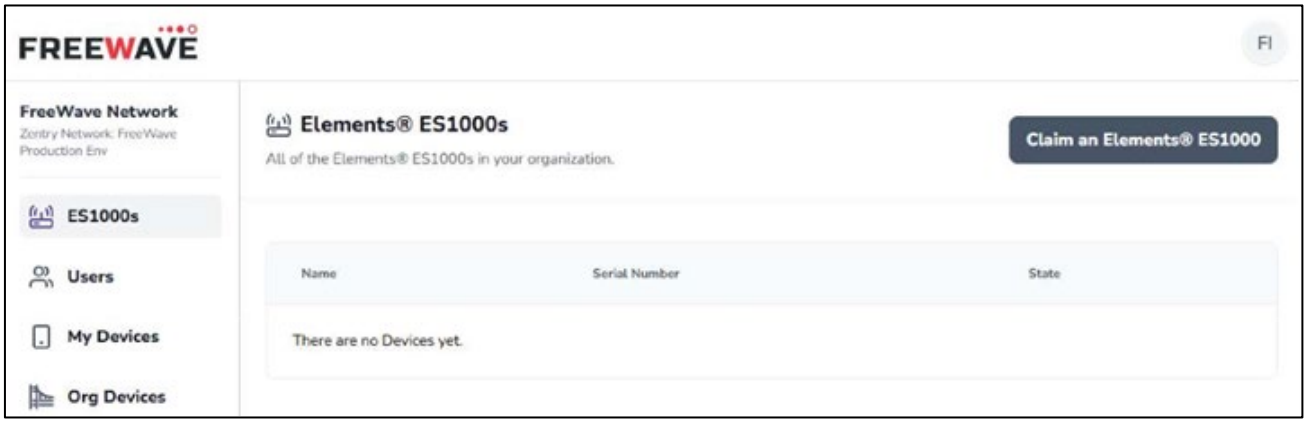
Important Note:

To complete setup, please contact support@freewave.com to create a Zentry account.

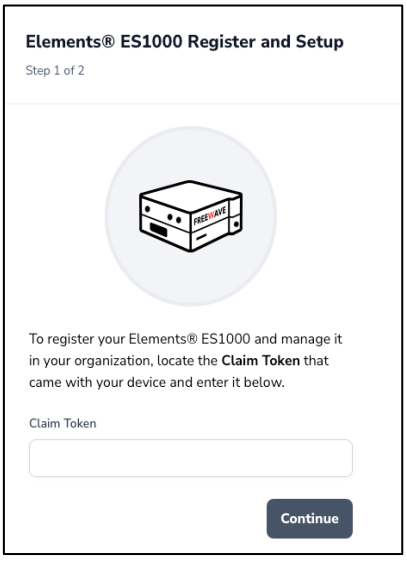
To Claim your ES1000

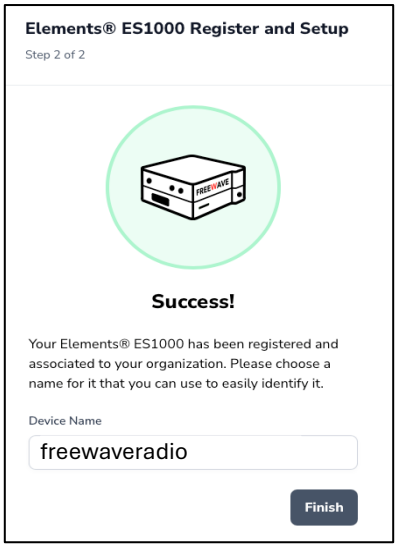
1. Navigate to https://www.zentry.freewave.com/ using your web browser.
2. Login with your username and password that you created during your initial account setup with the FreeWave support team.
3. Click on ES1000s on left side of Console menu.
4. Click Claim an Elements ES1000 on top right hand side of page.





5. Type in Claim Token code (find it on the QR code on the side of the ES1000 unit).
6. Once successful, create a unique name for your device and click Finish (e.g. freewaveradio).
   Note: this device name is the DNS used to securely access the ES1000.

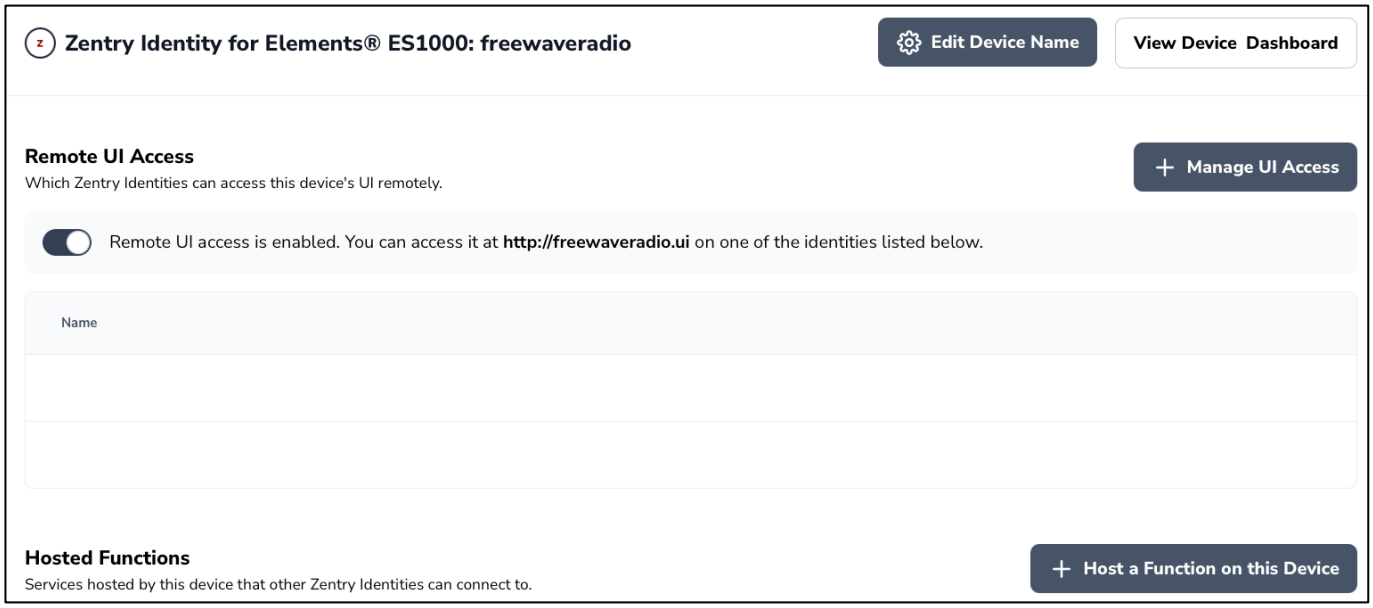




Allow Remote UI Access to ES1000

1. Click View Zentry Identity button on top right of page.

2. Toggle Remote UI Access button at top of page.
3. Click + Manage UI Access button top right of page.
4. Select Add / Remove button to allow appropriate access to devices.
   NOTE: If no devices show up here, ensure you have added other devices like your laptop to your organization on Zentry portal.
5. Click + Host a Function on this Device button



6. Choose a proper name for your function.
7. Under “Additional Ports” type in any ports you’d like to allow access to on your device to host this function (Ex: 1880 for NodeRed). Separate multiple ports with a comma.
8. Fill in the Forward Host box with the IP of your device connected to ES1000 Ethernet port that you’d like to access.
9. Toggle other common ports as you’d like at bottom of page.
10. Click Save New Function button in top right.

Install the Zentry client on your Computer

- For Windows please download the zero-trust client from the link below.
  - Windows Client
  - Click the .exe labeled Ziti.Desktop.Edge.Client-2.6.4.exe to download a lightweight desktop application which will connect your device to the zero-trust fabric.
- For MacOS/iOS please download the zero trust client from the App Store from one of the links below.
  - MacOS
  - iOS
- For Linux operating systems please contact support@freewave.com.

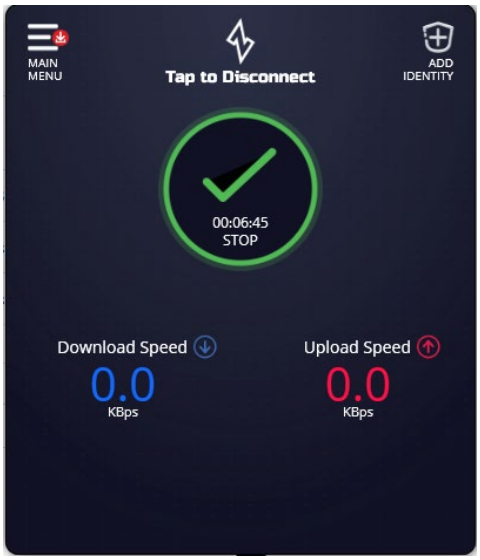
Create a Zero-Trust Identity for your Computer

NOTE: the ES1000 comes configured with an identity and is connected to the zero-trust fabric. You will use the Claim Token code to bring your ES1000 into your organization on the Zentry Console.

1. Go to the FreeWave Zentry Console at: https://www.zentry.freewave.com/.
2. Click "My Devices"
   a. Choose "+Add Device" (this will be your laptop or whatever device you are planning on using to connect to the ES1000 via Zentry).
   b. Name the device (we suggest something easily identifiable e.g. Ron's laptop).
   c. Click Create Identity button.
   d. Download the identity and save the JWT file to your device.

Windows

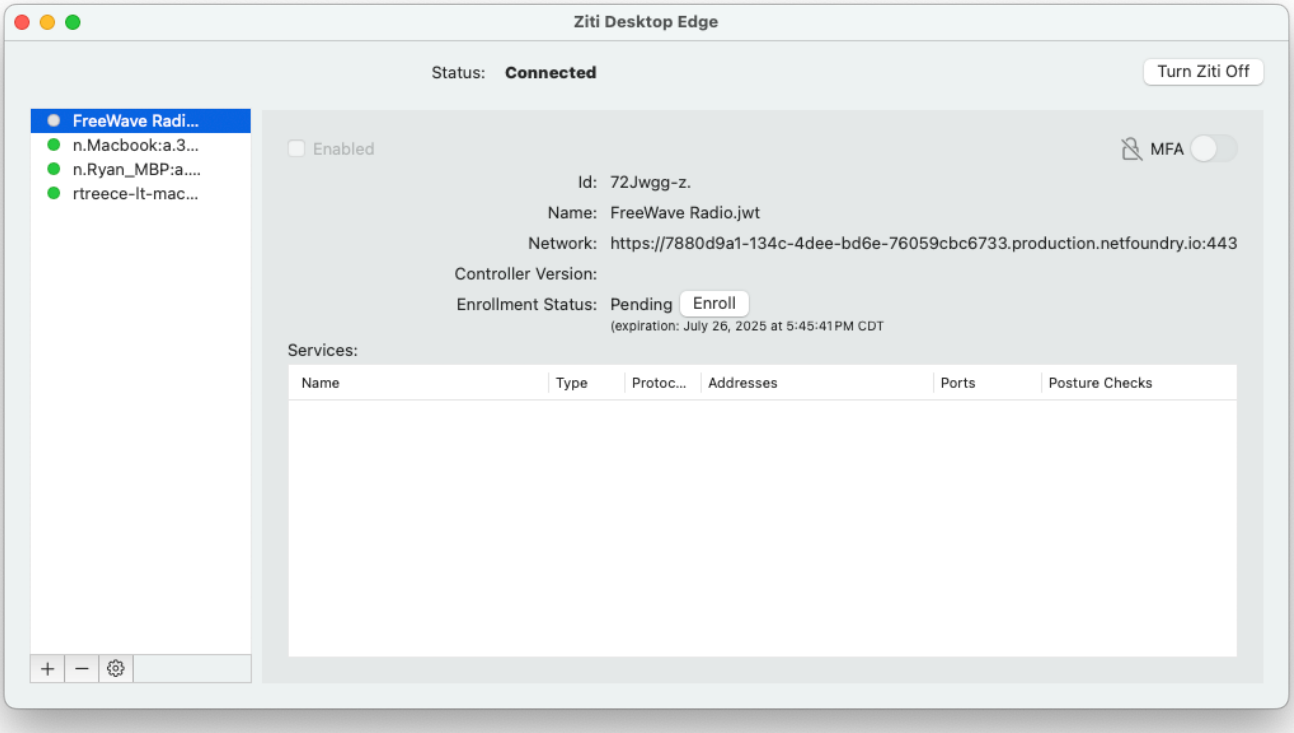
1. Open the zero-trust application previously installed. You will load the identity file into the application.
    a. In the Ziti application, click on “Add Identity” on the top right
    b. Choose “with JWT” from pull down menu that appears.
    c. Select and upload previously saved JWT file.
    d. Click circle icon in center of application to connect and ensure green check is showing representing that the device is online.



MacOS

1. Open the zero-trust application previously installed. You will load the identity file into the application.
    a. In the Ziti application. In the upper right corner click on “Add Identity”, then choose “JWT”.
    b. Click on the “+” sign in the bottom left corner and choose the proper JWT file you downloaded.
    c. In “Enrollment Status” click Enroll.
    d. Select “Turn Ziti On” on top right corner and make sure status shows connected.

You should now see the identity “Enabled” in the zero trust client application.



Verify Remote Connection

1. Open a Chrome or Firefox web browser window and navigate to https://zentry.freewave.com and login with your credentials you setup with support.
2. Click ES1000 button on left of page, click the name of your ES1000 you'd like to test connection to.
3. Click View Zentry Identity in top right of screen.
4. Copy the exact http:// URL listed under Remote UI Access
5. Paste URL into your browser of choice which will bring up the ES1000 login page.
   NOTE: Make sure the URL is http and not https! If you cannot see the login page you may need to wait a brief period before the security schema syncs.

Congratulations!

You have successfully created a zero trust network from your device to the ES1000.

For more complex configurations please refer to the user manual and/or reach out to support@freewave.com

Export Compliance

FreeWave Technologies, Inc. products may be subject to control by the Export Administration Regulations (EAR) and/or the International Traffic in Arms Regulations (ITAR). Export, re-export, or transfer of these products without required authorization from the U.S. Department of Commerce, Bureau of Industry and Security, or the U.S. Department of State, Directorate of Defense Trade Controls, as applicable, is prohibited. Any party exporting, re-exporting or transferring FreeWave products is responsible for obtaining all necessary U.S. government authorizations required to ensure compliance with these and other applicable U.S. laws. Consult with your legal counsel for further guidance.

Safety Information

Warning! *Do not* remove or insert diagnostics cable while circuit is live.

Warranty

FreeWave Technologies, Inc. warrants your product against defects in materials and manufacturing for a period of two years from the date of shipment, depending on model number. In the event of a Product failure due to materials or workmanship, FreeWave will, at its discretion, repair or replace the Product. For evaluation of Warranty coverage, return the Product to FreeWave upon receiving a Return Material Authorization (RMA) for evaluation of Warranty Coverage.

In no event will FreeWave Technologies, Inc., its suppliers, or its licensors be liable for any damages arising from the use of or inability to use this Product. This includes business interruption, loss of business information, or other loss which may arise from the use of this Product. OEM customers' warranty periods can vary.

Warranty Policy will **not apply** in the following circumstances:

1. If Product repair, adjustments, or parts replacements are required due to accident, neglect, or undue physical, electrical, or electromagnetic stress.

2. If Product is used outside of FreeWave specifications as stated in the Product's data sheet.

3. If Product has been modified, repaired, or altered by Customer unless FreeWave specifically authorized such alterations in each instance in writing. This includes the addition of conformal coating.

Restricted Rights

Any product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

This manual is for use by purchasers and other authorized users of FreeWave products. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, or for any purpose without the express written permission of FreeWave Technologies, Inc. FreeWave reserves the right to make changes to this manual without notice. FreeWave assumes no responsibility or liability for the use of this manual or the infringement of any copyright or other proprietary right.

FCC Notifications

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: 1) This device may not cause harmful interference and 2) this device must accept any interference received, including interference that may cause undesired operation. This device must be operated as supplied by FreeWave

Technologies, Inc. Any changes or modifications made to the device without the express written approval of FreeWave Technologies may void the user's authority to operate the device.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note: Whenever any FreeWave Technologies module is placed inside an enclosure a label ***must*** be placed on the outside of that enclosure which includes the module's FCC ID.

UL Notification

Model ES1000:
"This equipment is suitable for use in Class I, Division 2, Groups A, B, C, and D or non- hazardous locations only."

"Warning—Explosion Hazard—Substitution of components may impair suitability for Class I, Division 2."
The diagnostics port and cable do not have a latching connector and cannot be used in a hazardous location.

GNU Notification

Some of the software in the firmware is licensed under the GNU General Public License and other Open Source and Free Software licenses. You can obtain corresponding source by contacting FreeWave and requesting the source on CD.

FreeWave Technologies
5395 Pearl Parkway, Suite 100
Boulder, CO 80301
www.freewave.com
1.303.381.9200
1.866.923.6168