netAlly

EtherScope® nXG
User Guide

Tap a link to go directly to the app's chapter.
Scroll down to view the full list of Contents.

Software v2.3 Published June 16, 2023

Contents

Contact Us

Online: NetAlly.com

Phone: (North America) 1-844-TRU-ALLY (1-844-878-2559)

NetAlly
2075 Research Parkway, Suite 190
Colorado Springs, CO 80920

For additional product resources, visit:
NetAlly.com/Products/EtherScopenXG

For customer support, visit:
NetAlly.com/Support

Register your EtherScope nXG

Registering your product with NetAlly gives you access to valuable information on product updates, troubleshooting procedures, and other services.

Register on the NetAlly Support Page.

Introduction

The EtherScope nXG Portable Network Expert is a rugged, hand-held tool for testing and analyzing copper, fiber, and Wi-Fi networks. It features applications developed by NetAlly for network discovery, measurement, and validation, which are available from the Home and Apps screens.

All NetAlly hand-held testers include access to Link-Live Cloud Service at Link-Live.com. Link-Live is an online system for collecting, organizing, analyzing, and reporting your test results. Test data is automatically uploaded once your tester is properly configured. Visit Link-Live.com and "Claim" your EtherScope to access these features.

Activating Your EtherScope Support

All EXG-300 models come with one year of NetAlly's AllyCare support. You must activate this support before you can start using your unit.

To activate support, go to the NetAlly support site:

https://support.netally.com/Login/?type=customer

Begin by typing your company email into the field for NEW USERS, and then click **Sign up**.

Follow the screen instructions to register your product. You will then receive an email with additional instructions to register and receive an activation code.

The first time you boot your EXG-300, you must enter the activation code before you can begin using your product. You can then use all features on your EtherScope.

How to Use this Guide

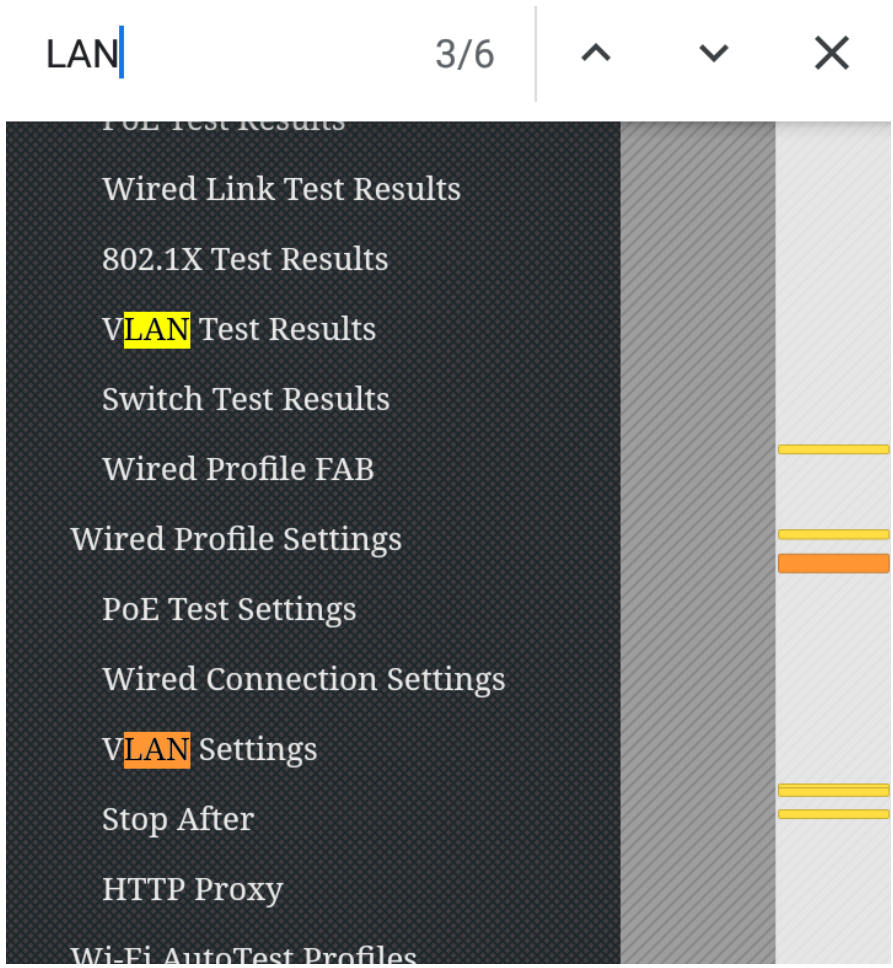
This user guide describes the EtherScope nXG's testing functionality and basic elements of the system interface.

The guide is meant for users who are knowledgeable about network operations, tests, and measurements.

The EtherScope nXG is also referred to as just EtherScope or the "unit" in this guide.

- Tap **blue links** to go to their destinations. Underlined blue links open external websites.
- Tap bookmarks in the list on the left to go to the corresponding section.
- Tap headings in the **Contents** list that starts on page 2 to go to the corresponding sections.
- To search for a word or phrase:
  1. Tap the browser menu  icon in the upper right.
  2. Select **Find in Page** from the menu.

3. Enter the search text.
4. Tap the find icon . This displays the text at the top of the screen. Tap the up and down arrows to search forwards and backwards for the text. In the image below, the user has searched on "LAN". Tap the highlight bars on the right to go to the corresponding manual text.



Online and Local Versions of This Guide, Videos

- Manuals are also available for download at: https://www.netally.com/support/user-guides/
- To view the User Guide on your EtherScope nXG, you must have a network connection with access to the internet (see Connecting to Wi-Fi). When you tap on **Guides > User Guide** on the "Home Screen" on page 38, this user guide is downloaded and displays on your unit.
- After you have downloaded the User Guide to your unit, the guide is stored in a local cache for the browser. You do not have to repeat the download unless you change the device language or clear the browser cache.
- The Guides icon on the Home Screen (used to access this guide) also gives access to training and information videos specific to this product.

International Versions of This Guide

A Chinese or English EtherScope nXG user guide is available if you change the device language to one of those languages. If you choose Japanese, the English user manual is used.

Differences Between Models

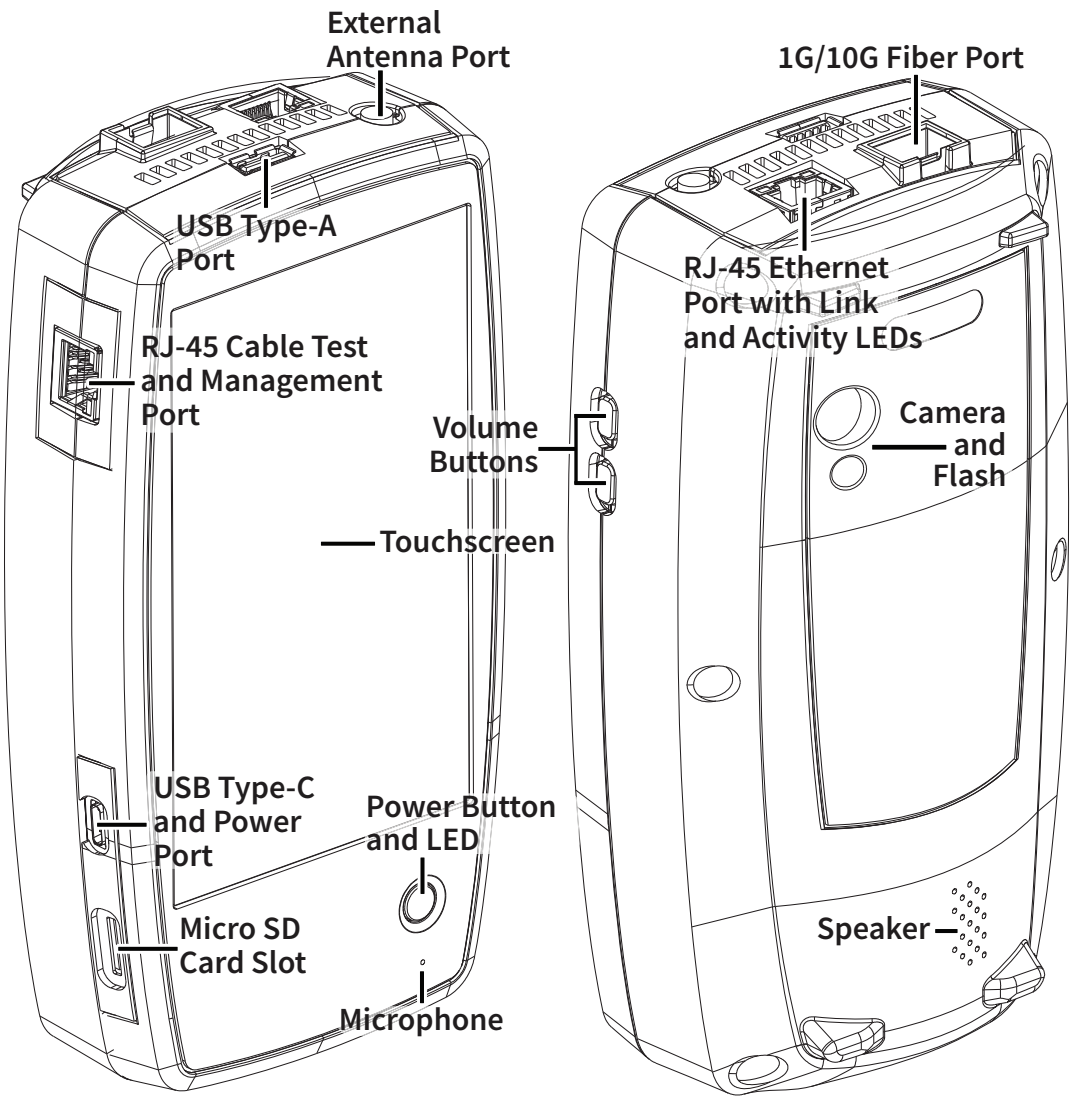
The Model number of your EtherScope appears on the About Screen and is printed on the back panel of your unit. This manual covers all models and identifies features specific to each model if there are differences. In general:

- EXG-200: Supports 2.4 GHz and 5 GHz frequency bands; supports 802.11a/b/g/n/ac Wi-Fi standards.
- EXG-300: Supports 2.4 GHz, 5 GHz, and 6 GHz frequency bands; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.
- EXG-300C: Supports 2.4 GHz and 5 GHz frequency bands; has same features as EXG-300; does not support 802.11d specification.
- EXG-300E: Supports 2.4 GHz, 5 GHz, and 6 GHz frequency bands, limited by 802.11d regional domain specification; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.

For more information, see "EXG-200 Specifications" on page 788 and "EXG-300 Specifications" on page 803.

Buttons and Ports

Button and port functions on your EtherScope unit are described below.



Feature	Description
Fiber Port 1G/10GBASE-X	Connects to an SFP adapter and fiber cable for network testing. NOTE: 100FX SFPs are not supported.
RJ-45 LAN Port 10M/100M/1G/ 2.5G/5G/10G-BASE-T	Connects to a copper Ethernet cable for network testing Supports PoE (with compatible unit hardware)
Transmit LEDs	Green LED lit: Linked Yellow LED flashing: Activity
USB Type-A Port	Connects to any USB device
RJ-45 Cable Test and Management Port	Connects to an Ethernet cable for patch cable testing and unit management
USB Type-C On-the-Go Port	Connects to a USB Type-C connector for file transfer and to the included AC adapter for charging the unit
Microphone	Allows voice input
Camera and Flash	Captures images and acts as a flashlight
Micro SD Card Slot	Used for removable storage expansion (See Inserting a Micro SD Card below.)
Volume Buttons	Increase or decrease the audio volume

Feature	Description
Speaker	Produces audio
Power Button	Press and hold to display menu for **Power off** or **Restart** Green LED: Unit is powered on Red LED: Unit is charging

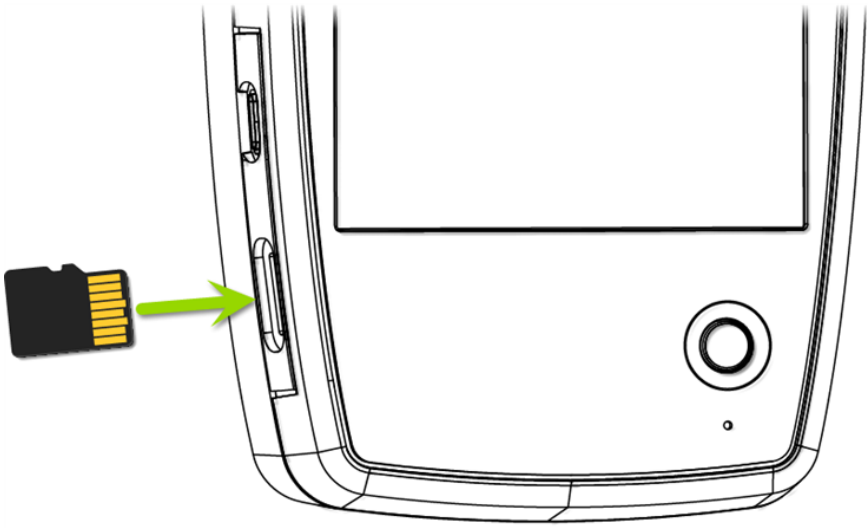
See Test and Management Ports for detailed explanations of the port functions.

See Updating Software for requirements on updating system software.

Refer to the product Specifications if needed.

Inserting a Micro SD Card

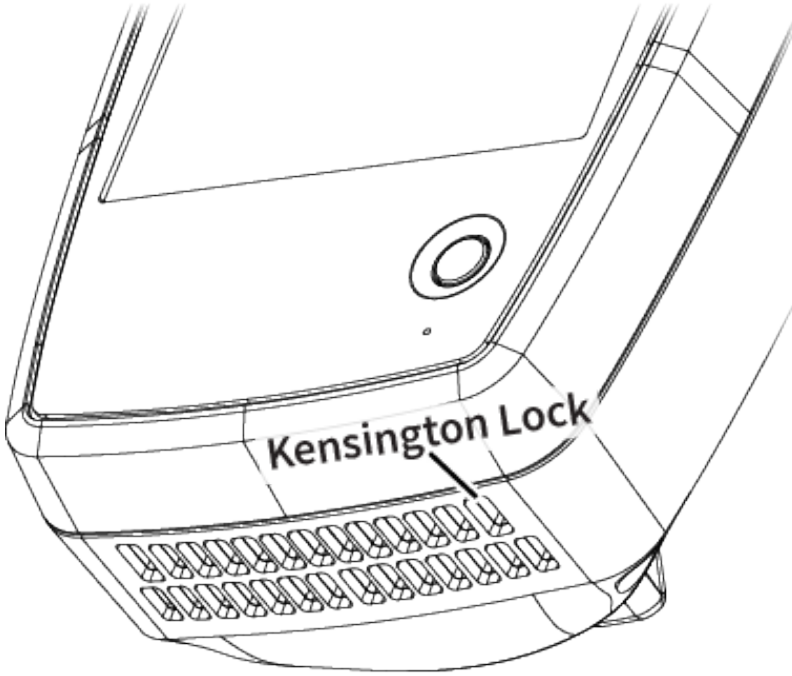
A Micro SD card must be inserted with the ***metal contacts facing the front*** (towards the touchscreen) of the unit, as shown below.



The card should slide in easily when properly oriented. You may need a paperclip or thumbnail to carefully push the SD card in far enough to engage the spring mechanism for insertion and removal.

Using a Kensington Lock

The Kensington Lock slot is the right, front vent hole on the bottom of the unit, as shown below.


Kensington Lock

Charging and Power

Your EtherScope nXG includes a USB-C 15V/3A power adapter.

⚠ **CAUTION**: Only the NetAlly-supplied power adapter is supported.

To begin charging the internal lithium-ion battery, plug the included power adapter into an AC outlet and the USB-C charging port on the left side of the unit. The Power button turns red when the unit is in charging mode and turns off at full charge. Refer to the Specifications for battery run duration and charge times.

PoE Charging

Power over Ethernet (PoE) can provide alternative power to your unit's battery. (Test units that include the **Charge Battery via PoE** setting in General Settings, support PoE.)

- Negotiated PoE class levels 4-8 (≥ 25.5 W) provide enough power to run the test unit indefinitely and to charge the battery.

- Negotiated PoE class levels 0-3 (≤ 15.4 W) provide some power to extend battery run time but not enough to charge the battery.

Use the following steps to enable PoE charging:

1. Connect the top RJ-45 port on the unit to a network switch with PoE or to a PoE injector.
2. Make sure the unit is powered on or in display sleep mode.
3. If your test unit displays the **Charge Battery via PoE** setting in General Settings, tap the setting to enable PoE charging.
4. Detect the PoE availability by running an AutoTest Wired Profile with a PoE test that passes. (The **PoE Test** must be enabled and configured with a **Powered Device Class** that is supported by your switch or PoE Injector.) See Wired Profile Settings and Results.

   NOTE: If the AutoTest app is not currently open, the last Wired Profile in the profile list runs automatically when you power on the

unit or EtherScope detects a new copper link in the top Wired Test Port.

See Buttons and Ports for port locations and descriptions.

Powering On

- To start up the unit, hold down the Power Button for approximately one second, until the Power Button LED turns green.
- When the display goes into Sleep mode, the Power Button LED remains on. Tap the Power Button briefly to wake up the display. (Set the timing for display sleep and auto power off in the Device Settings.)
- To shut down or restart, hold down the Power Button for one second until the “Power off” and "Restart" dialog box appears on the touchscreen, and then tap **Power off** or **Restart**.
- If the unit is unresponsive to a normal power off, press and hold the Power Button for five seconds to perform a hard shutdown.

Back to Title and Contents

Safety and Maintenance

Observe the following safety information:

Use only the Adapter provided or Power over Ethernet (PoE) to charge the battery.

Ensure that the Adapter is easily accessible.

Use the proper terminals and cables for all connections.

⚠ **CAUTION**: To avoid possible electric shock or personal injury, follow these guidelines:

- Do not use the product if it is damaged. Before using the product, inspect the case, and look for cracked or missing plastic.
- Do not operate the product around explosive gas, vapor, or dust.
- Do not try to service the product. There are no serviceable parts.
- Do not replace the battery. There is risk of explosion if the battery is replaced by an incorrect battery type.
- Dispose of battery packs and electronics in compliance with your institution's disposal instructions.

- Use as directed. If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired.

Safety Symbols

	**Warning or Caution: Risk of damage to or destruction of equipment or software.**
	**Warning: Risk of electrical shock.**
	**Not for connection to a public telephone system.**
	**Class 1 Laser Product. Do not look into the laser.**

Cleaning

To clean the display, use a lens cleaner and a soft, lint-free cloth.

To clean the case, use a soft cloth that is moist with water or a weak soap.

Scratches on the dark-colored plastic can be removed by *lightly* scrubbing a 1:2 mixture of

toothpaste to water onto the affected surface with a bristled brush.

⚠ **CAUTION:** Do not use solvents or abrasive materials that may damage the product.

Legal Notification

Use of this product requires acceptance of the Terms and Conditions available at http://NetAlly.com/terms-and-conditions or which accompanies the product at the time of shipment or, if applicable, the legal agreement executed by and between NetAlly and the purchaser of this product.

Open-Source Software Acknowledgment: This product may incorporate open-source components. NetAlly will make available open-source code components of this product, if any, at Link-Live.com/OpenSource.

NetAlly reserves the right, at its sole discretion, to make changes at any time in its technical information, specifications, service, and support programs.

© 2019-2023 NetAlly

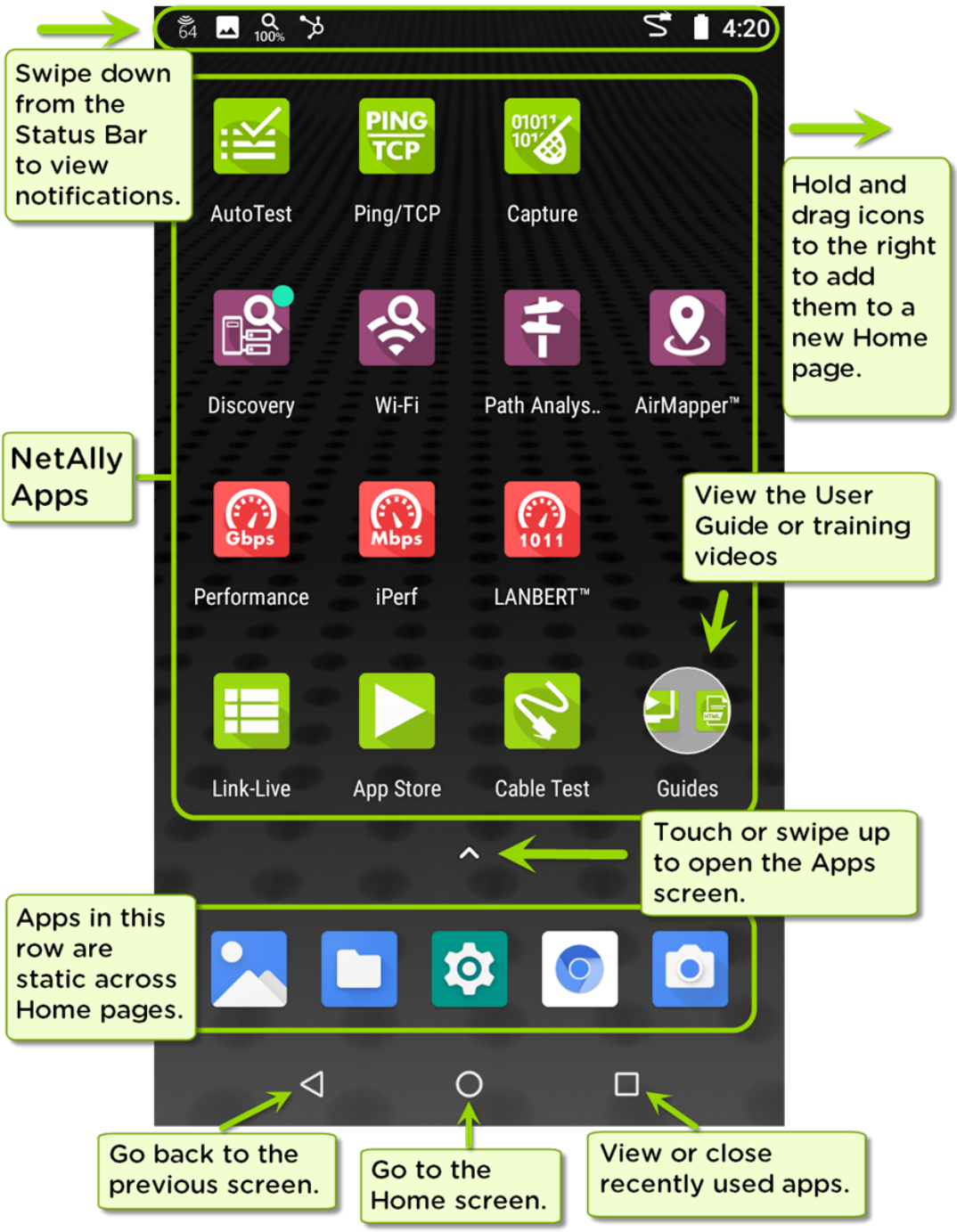
Back to Title and Contents

Home and System Interface

This chapter explains how to use the features of the system Home screen and user interface to navigate and organize your device.

The EtherScope nXG interface supports many of the operations typical of any hand-held device. Use dragging and swiping motions on the touchscreen to navigate through apps, open side menus, drag down the Notification Panel from the Status Bar at the top of the Home screen, or drag up the Apps screen from the bottom.

Home Screen


Swipe down from the Status Bar to view notifications.
4:20
AutoTest
Ping/TCP
Capture
Discovery
Wi-Fi
Path Analys..
AirMapper™
Performance
iPerf
LANBERT™
Link-Live
App Store
Cable Test
Guides
Hold and drag icons to the right to add them to a new Home page.
NetAlly Apps
View the User Guide or training videos
Touch or swipe up to open the Apps screen.
Apps in this row are static across Home pages.
Go back to the previous screen.
Go to the Home screen.
View or close recently used apps.

Like other hand-held devices, your EtherScope nXG Home screen is customizable. The image above shows the default configuration, but you can add, remove, and reorganize app icons and widgets to serve your purposes.

You can also create more Home pages by tapping, holding, and dragging an app icon to the right from the main Home screen.

See the Apps screen section for instructions on adding more apps to your Home pages.

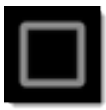
Navigating the System

The navigation actions you can perform to move through screens and panels on the EtherScope nXG are the same as those you would use to navigate many other phone or tablet devices.

The main device navigation buttons appear at the bottom of the touch screen.

The back icon returns to the previous screen.

The circle icon opens the Home screen.



The square icon displays your recently used applications for easily switching between then. This is also the screen where you can close, or stop, the open applications.

TIP: Double tap the square icon to switch back to the previous app you were using and to switch back and forth between two app screens (like a testing app and this User Guide).

Swiping

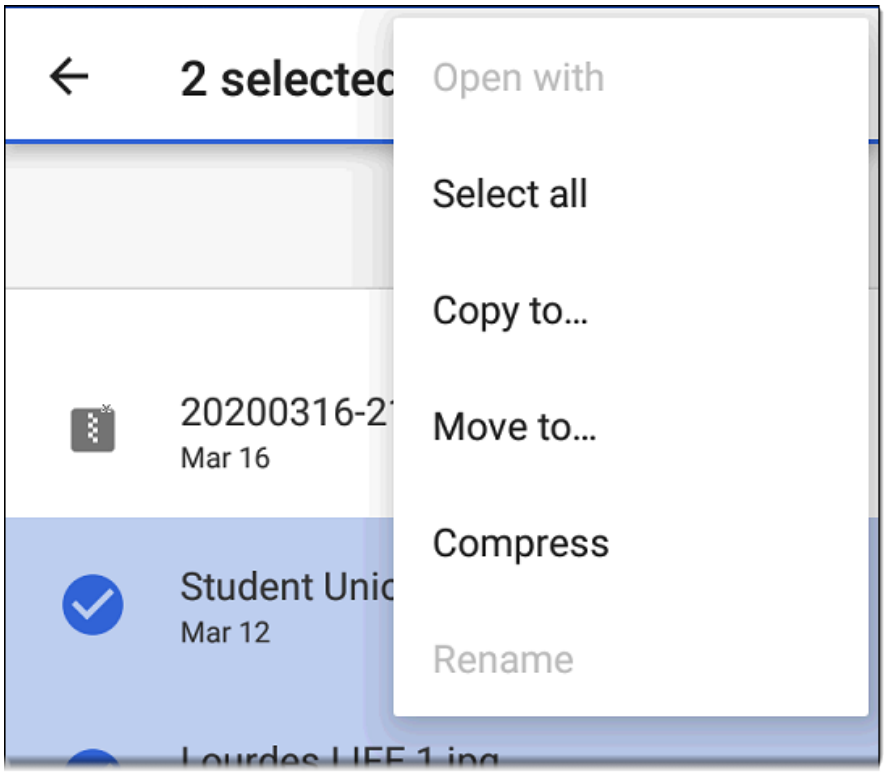
Touch and drag your finger or "swipe" up, down, left, and right to move through pages of the Home screen and applications, scroll up or down, and pull out navigation drawers and panels.

Long Pressing

Touch and hold or "long press" files or application icons to reveal additional operations.

For example, you can long press a file name in the Files Application to reveal the top toolbar with options for sharing, deleting, or moving the file.

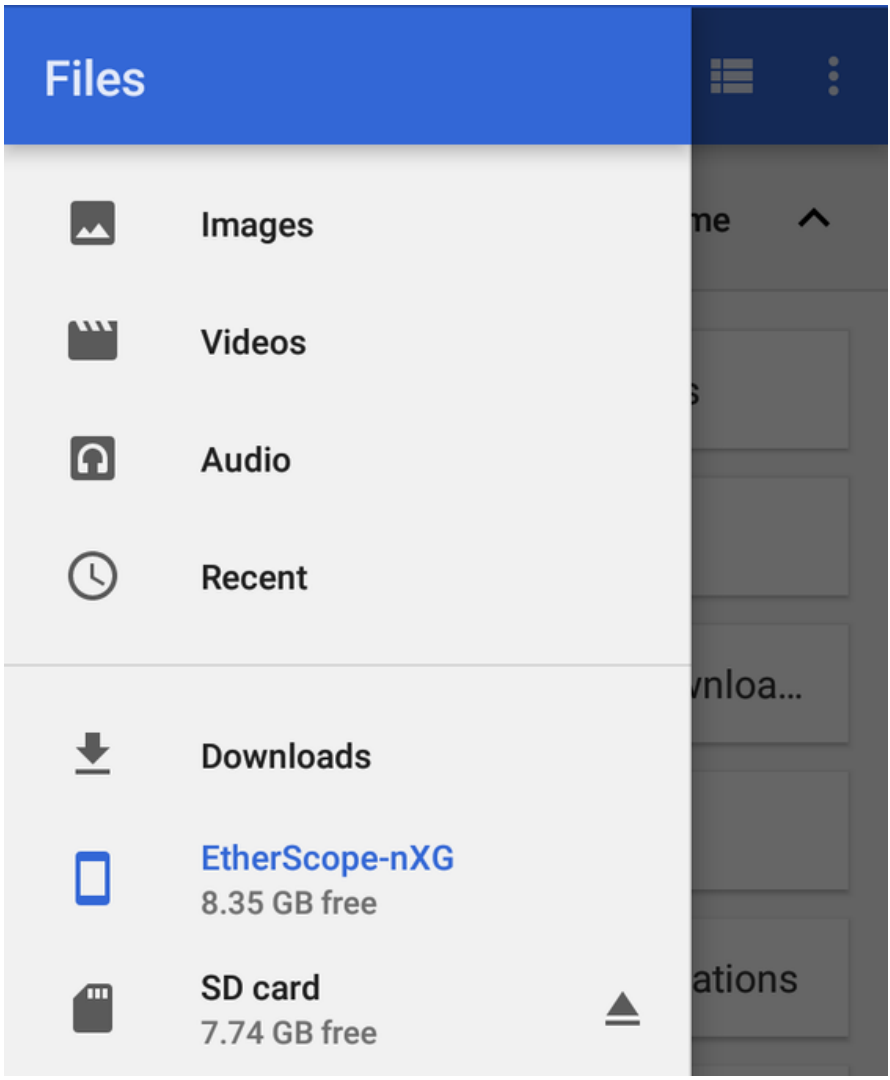
Additional options often appear in an overflow menu, designated by the action overflow icon .



You can also long press on text on most screens to open options for copying and sharing the text.

Left-Side Navigation Drawer

In the Files app, tap the Menu icon or swipe right to open the navigation drawer. It displays the folders in your file system.



NOTE: In the Files app, you may need to tap the action overflow icon ⋮ at the top right and select **Show Internal Storage** to navigate to the **EtherScope-nXG** folder and sub-folders, as shown above.

See the Navigation Drawer topic for additional information.

Back to Title and Contents

System Status Bar and Notifications

The Status Bar across the top of the screen displays notification icons from the system as well as EtherScope nXG-specific icons related to your network connections and test statuses.

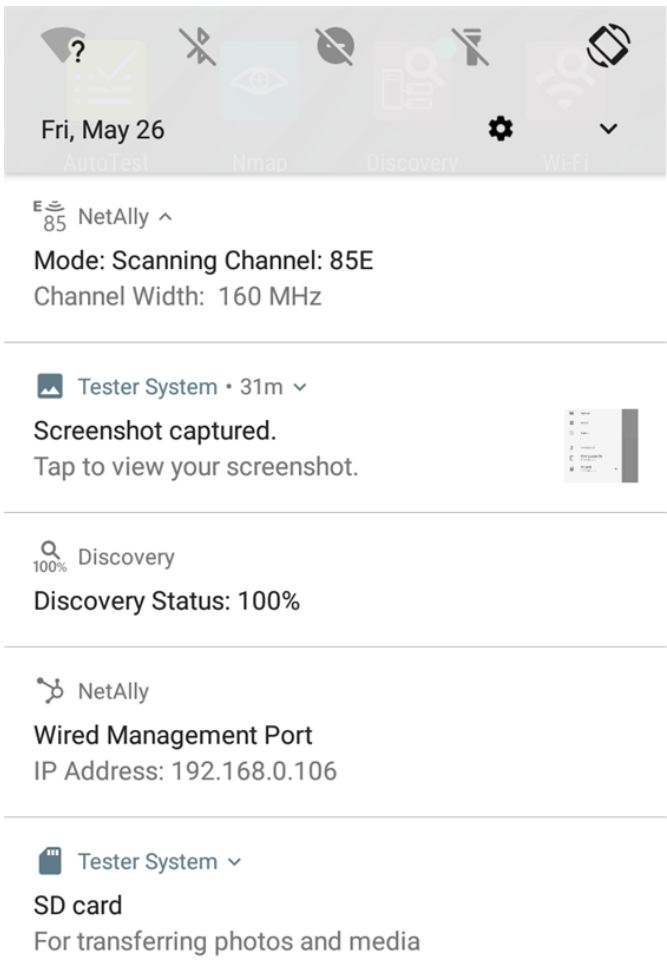
See Test and Port Status Notifications for details about the icons and notifications related to EtherScope nXG network connections, testing, and management.

Tap and swipe down on the Status Bar to open the Notification Panel.

Notification Panel

The Notification Panel contains notifications from your device, such as downloads and installs, inserted hardware, captured screenshots, app and connection statuses, and updates. The panel also displays common system settings icons for quick access.

Swipe (touch and drag) downwards on the Status Bar at very top of the screen to slide down the Notification Panel.



- Tap the title and down arrow ⌄ on a notification (or swipe down on it) to expand the box and view more details or options.
- Tap the middle of a notification to open the related app, image, or device settings or to perform other related actions.

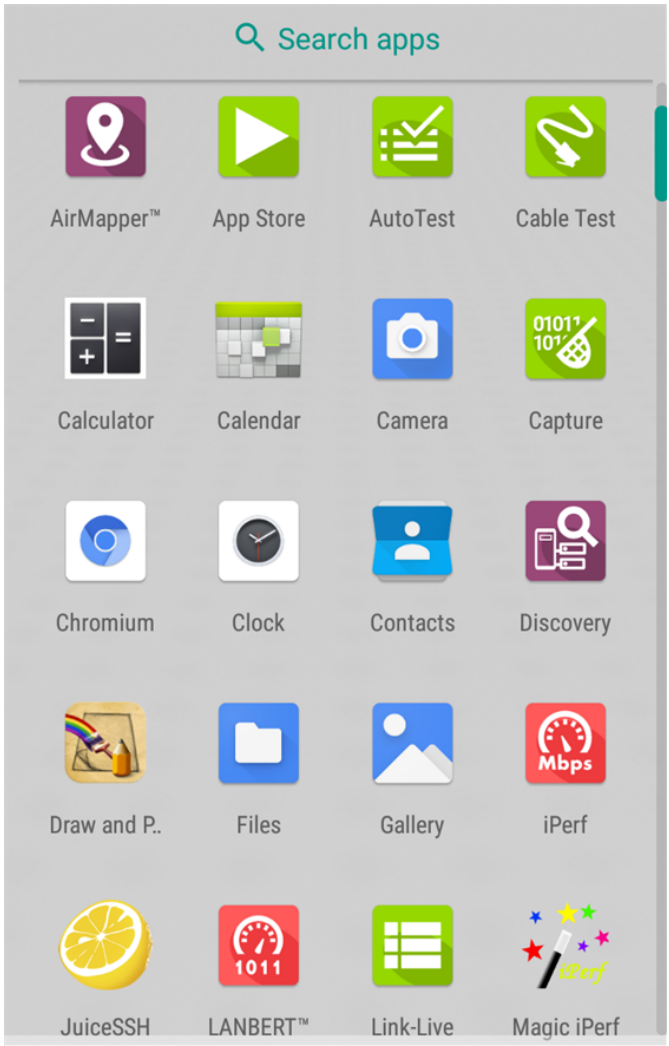
- Swipe left on a notification to dismiss it.

  NOTE: Because they are essential to the EtherScope testing functions, you cannot dismiss the test and management port-related test and port status notifications.

- Tap **CLEAR ALL** at the lower right of the panel to dismiss all system notifications.

Apps Screen and Store

To access the apps that are not shown on the Home screen, swipe up on the Home screen or tap the up arrow icon ^.

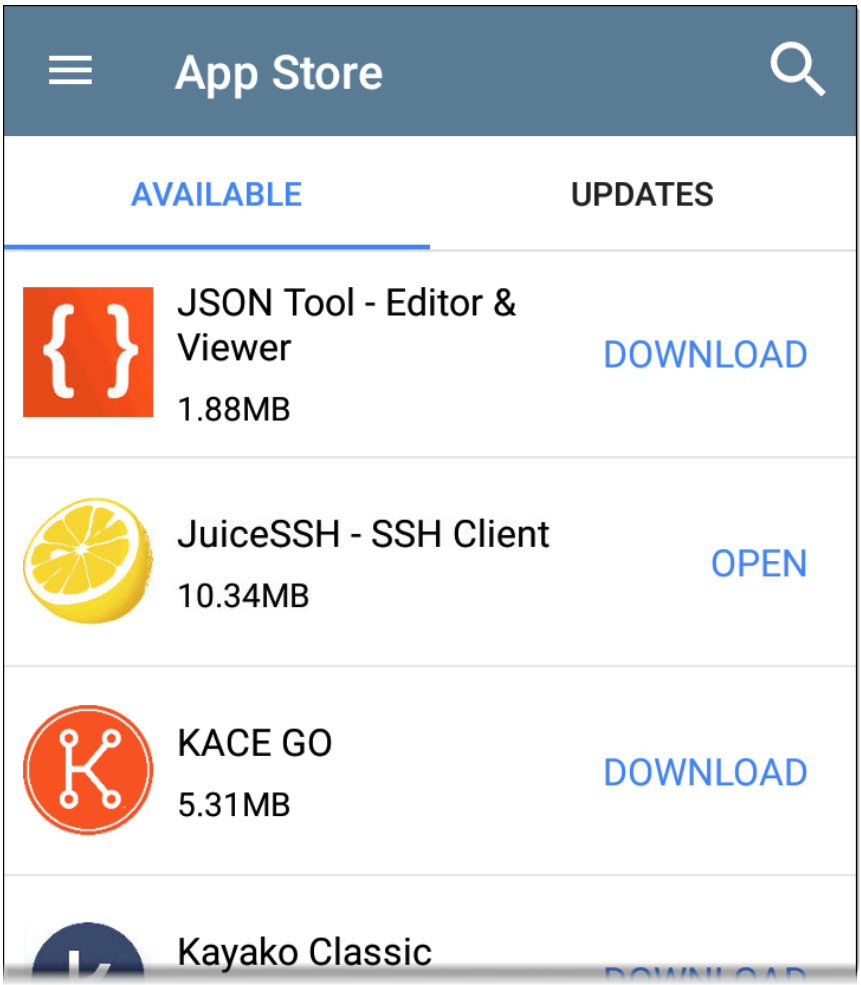


The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.

- Tap an app's icon to open the app.
- Hold and drag an icon upwards to add it to your Home screens.
- Touch and hold (long press) an icon to view App Info or access widgets you can add to the Home screen and other actions you can perform.

App Store

From the Home Screen or Apps Screen, open the NetAlly  App Store to download third-party system applications to use on your EtherScope nXG.



NOTE: Your unit must be "claimed" to Link-Live Cloud Service at Link-Live.com to access the App Store.

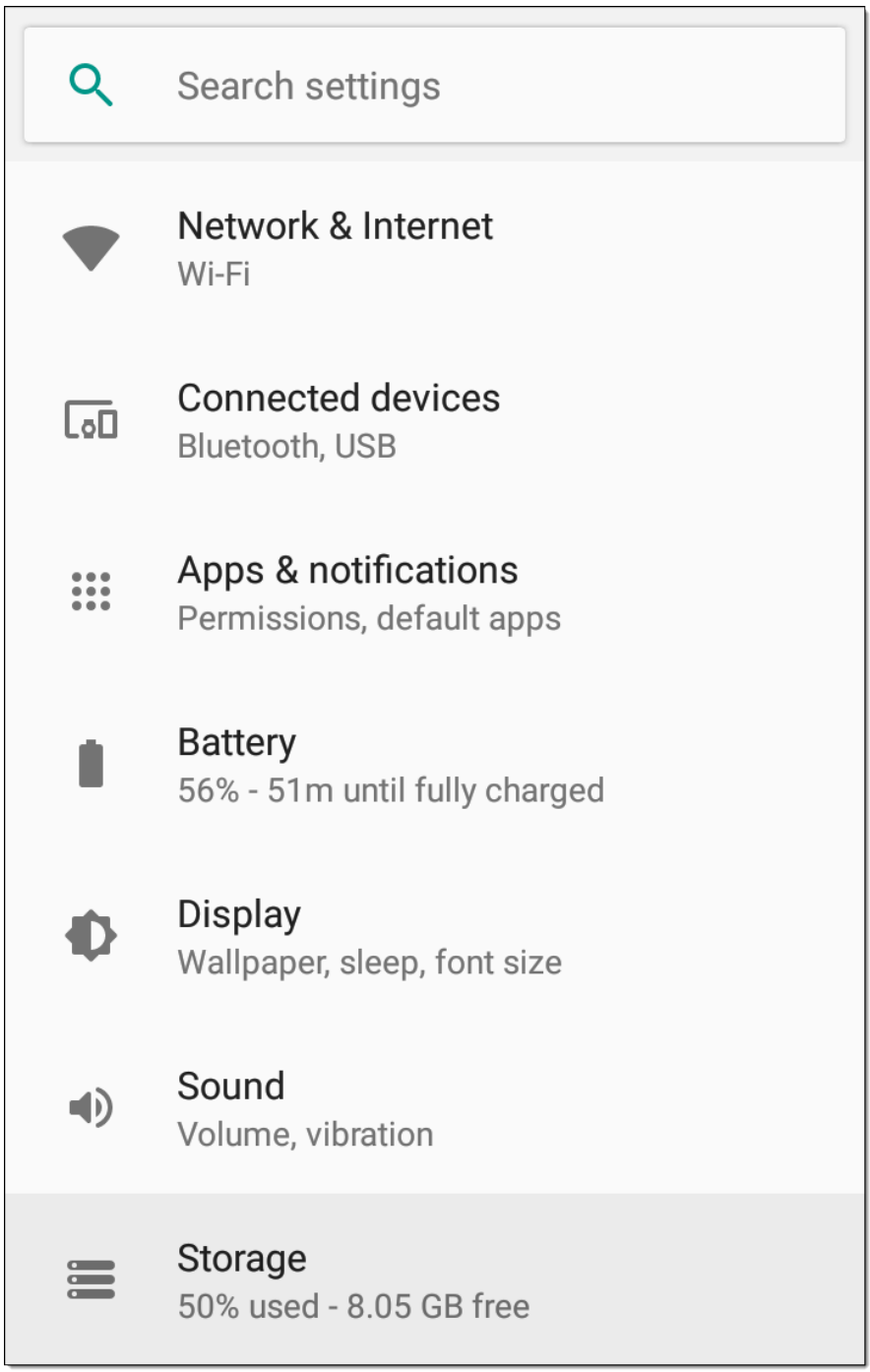
- Tap the search icon to search for an App.
- Tap **UPDATES** to view available updates of installed apps.
- To request that an App be added to the App Store, visit the Apps ▶ page at Link-

Live.com, and select the floating action button (FAB) at the lower right corner to

- **Request** or **Upload an App**.

Device Settings

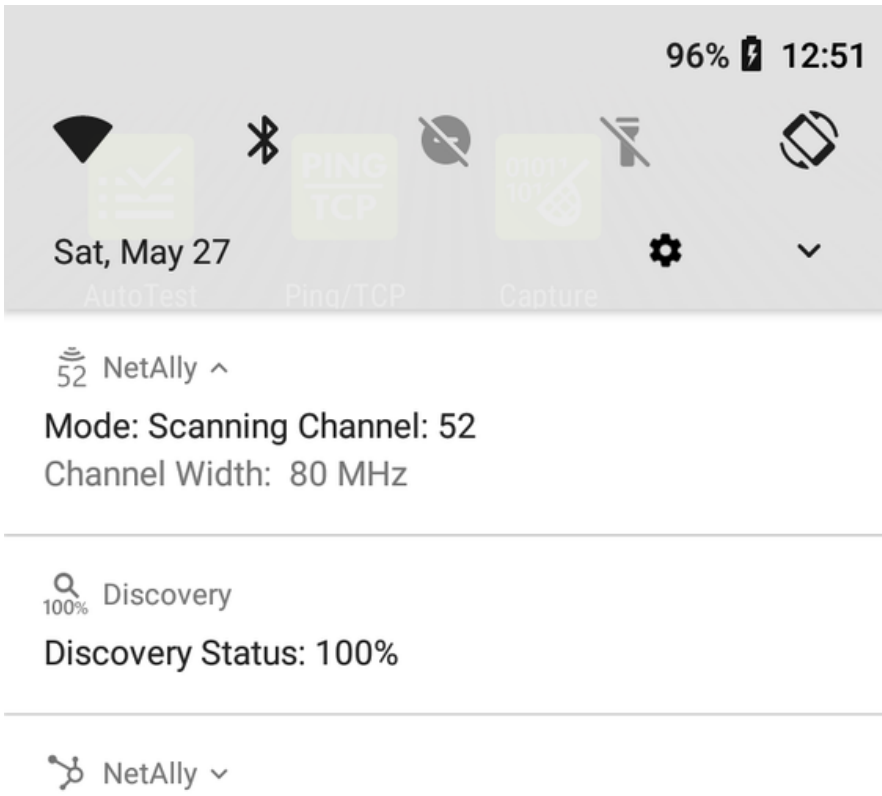
To access the system device settings, tap the Settings icon at the bottom of the Home screen.



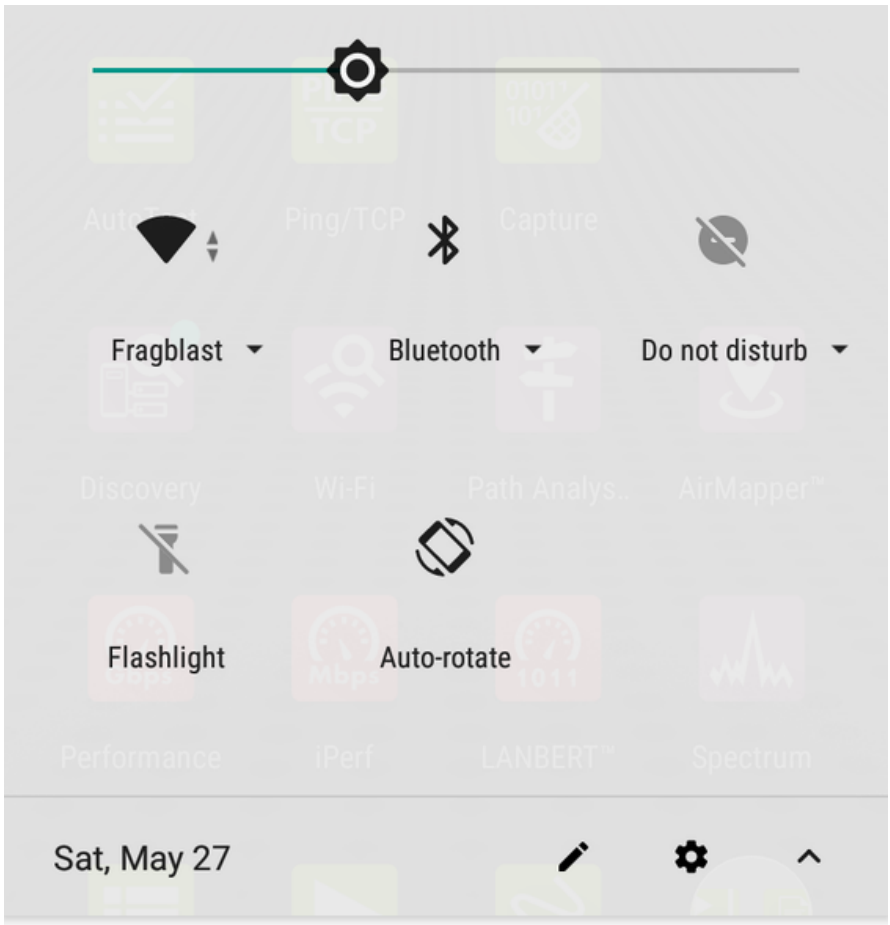
The device settings screen lets you adjust the display; adjust sound (including volume for external Bluetooth or USB speakers or headsets); set date and time; view installed applications and memory devices; connect to Wi-Fi; or reset to factory defaults.

Quick Settings Panel

You can also access some of the most common device settings, like Wi-Fi, from the Quick Settings Panel by swiping down from the Status Bar at the top of the touchscreen.



Swipe down twice to open the full Quick Settings Panel.



- Touch and drag the slider control at the top of the panel to adjust the screen's brightness.
- Tap an icon in the panel to enable or disable the corresponding feature. For example, you can turn the unit's **Wi-Fi** functions on or off from the quick settings.

- Touch and hold an icon to open the relevant device setting screen, if there is one. For example, touch and hold the Wi-Fi icon  to open system's Wi-Fi settings or the Auto-Rotate icon  to open Display settings.
- Tap the pencil icon ✎ at the bottom of the Quick Settings Panel to configure the icon controls that appear in the panel.

Auto Power Off

Activating the Auto Power Off function helps to extend the battery run time.

1. From the Device Settings  , select **Display**.
2. On the Display settings screen, tap **Device auto power off**.
3. In the pop-up dialog box, select how long you want the unit to remain On with no activity occurring. The unit automatically powers off after the selected period of inactivity has passed.

Similarly, you can adjust the setting that controls when the display goes into **Sleep** mode from the **Display** settings screen.

Language

Your device supports English, Japanese, and Chinese language displays. See "Changing the Device Language" on page 74 for information on changing the language.

Connecting to Wi-Fi

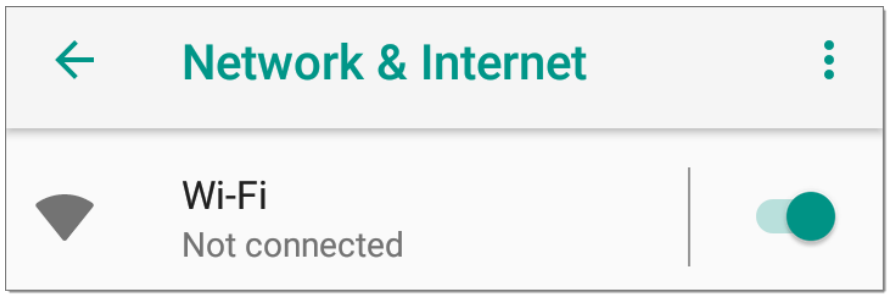
Basic connectivity to Wi-Fi is done using the Wi-Fi Management Port, which is configured in the system network settings. The Wi-Fi Management Port is separate from the Wi-Fi test ports. It can access the internet, be used by other system applications, upload test results to the Link-Live web site, and be used for remote control. The management port also provides a more stable network connection than the test port, which can change connections during AutoTests or be disconnected during Wi-Fi scanning. See Test and Management Ports for more information.

> NOTE: NetAlly testing apps use the Wi-Fi Test Ports and Wi-Fi AutoTest Profiles to connect to Wi-Fi networks during testing. See Test and Management Ports for more information.

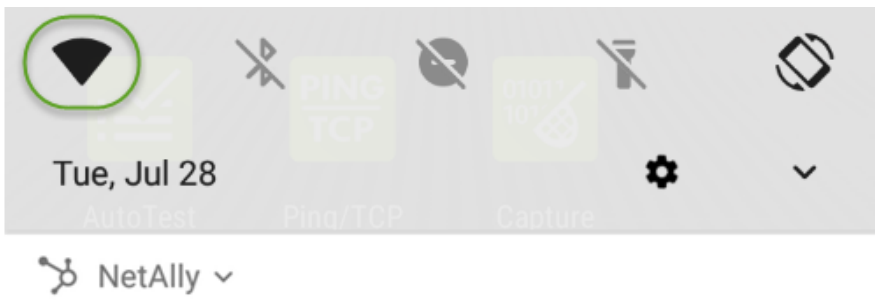
To connect your EtherScope to a Wi-Fi network, access the system Wi-Fi Device Settings using either method below:

- Open the device Wi-Fi settings from the main Device Settings screen by tapping the Settings icon  and selecting **Network &**

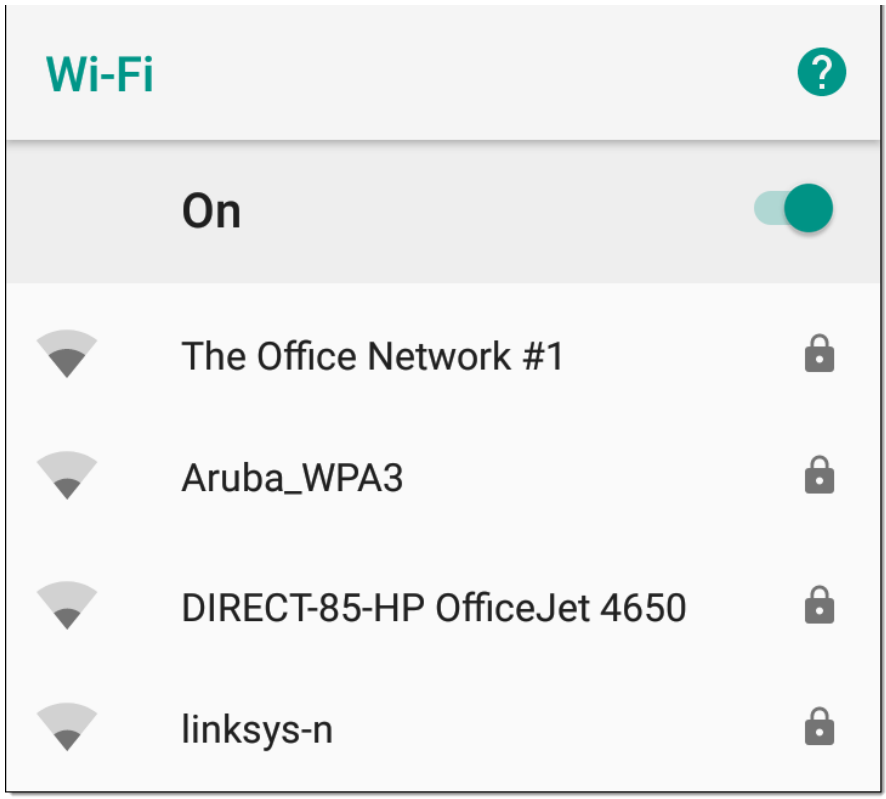
Internet > Wi-Fi.



- Open device Wi-Fi settings from the Quick Settings panel by dragging down the top Status Bar and tapping and holding (long pressing) the Wi-Fi icon.



Either path opens the Wi-Fi settings screen.



1. Ensure the Wi-Fi feature is **On**.
2. Tap an available Wi-Fi network in the list.
3. Enter the network's security credentials. (Most networks only require a password, but depending on the security settings, some may also require a company username, EAP type, authentication type, certificate, or other credentials.)
4. Tap **CONNECT**.

The network you selected moves to the top of the list, and your connection status is displayed below its name in device and quick settings.

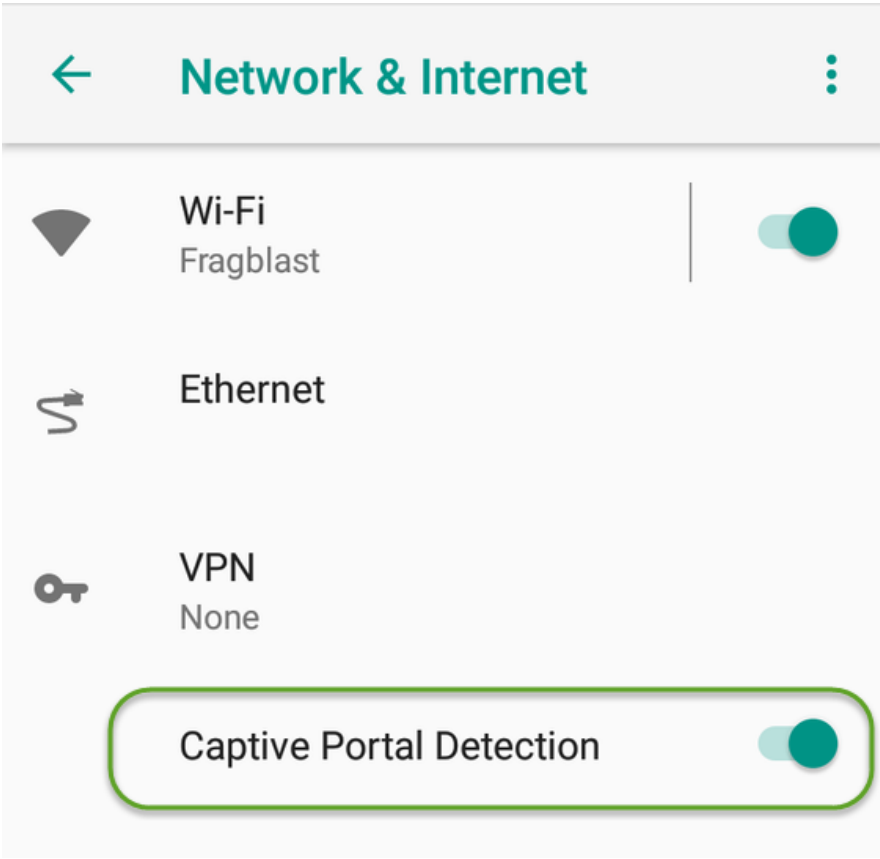
The Status Bar displays the Wi-Fi status icon at the top right of the screen.

Captive Portals

When you try to connect to a network with a Captive Portal requirement, this system notification icon appears in the top Status Bar. Drag down from the top of the screen to open the notification.

Tap the notification to open a web browser window where you can enter the required information for the captive portal. When finished, you can access the internet through the connected network.

If you are trying to connect to a network with a captive portal, but the system notification is not appearing, check that the **Captive Portal Detection** setting is enabled in Device Settings > **Network & Internet**.



Configuring for Enterprise Security

Enterprise security requirements for WPA/WPA2/WPA3 Enterprise now require a CA certificate file to be imported to your unit. Some EAP types also require a client certificate and key. This procedure assumes that you are trying to connect to an AP using WPA2-E with PEAP.

- Before You Begin
- Import the Certificate Authority File

- Test Wi-Fi Management Using WPA2-E with PEAP
- Import the Client Certificate

Before You Begin

You may depend on your IT department to provide authorization certificates, which may be created by a Trusted Root Authority like VeriSign or DigiCert. If so, contact your IT department for the certificate resources. You will need:

- CA certificate in .pem format
- Client certificate in .p12 format with private key (EAP TLS only)
- Common name, domain name, username, and password for the server you to which you want to connect.

If you have the ability to generate your own self-signed certificates, such as a FreeRADIUS server, you can create these resources as needed. This procedure uses examples generated by a FreeRADIUS server as a certificate source, although other sources are available.

Import the Certificate Authority File

1. Copy the self-signed Certificate Authority (CA) file (in .pem format) onto a USB thumb drive.
2. Transfer the USB thumb drive to your EtherScope nXG, and then copy the .pem file to the **Downloads** folder.
3. Open the Settings app.
4. Navigate to **Security > Encryption & credentials > Install a certificate > Wi-Fi certificate**. This opens the file picker.
5. Navigate to the Downloads folder, and select the .pem file that contains your CA certificate.
6. Rename this certificate (for example, **CA FreeRadius self-signed**). A message confirms that the Wi-Fi certificate has been installed.
7. (Optional) Verify the CA certificate installed correctly:

a. Tap the system **BACK** button to return to Encryption & credentials.

b. Tap **User credentials**.

c. Verify that the name of your CA file (for example, **CA FreeRadius self-signed**) is displayed.

8. If you are creating your own certificate:

   a. Verify the common name for the enterprise server. For example, using a FreeRADIUS server, create a common name of Example Server Certificate by entering:

      ```
      sudo -s

      cd /etc/freeradius/certs

      openssl x509 -in server.pem
      -text | grep Subject |
      grep CN
      ```

      Output:

      ```
      Subject: C=FR, ST=Radius,
      O=Example Inc., CN=Example
      Server Certificate
      ```

```
emailAddress=
admin@example.org
```

b. On the same server, create a user login to access the enterprise server. For example, with a FreeRADIUS server, you would edit /etc/freeradius/users, locate the section for "# The canonical testing user", and then create the new user by inserting 2 lines:

```
entuser1 Cleartext-Password
:= "randompw"
Reply-Message := "Hello, %
{User-Name}"
```

This creates a user login called **entuser1** with a password of **randompw**.

Test Wi-Fi Management Using WPA2-E with PEAP

1. Open the Settings app on your unit and navigate to **Network & internet**.
2. Toggle the Wi-Fi button to On/Enabled.
3. Tap **Wi-Fi** to view available networks.

4. Scroll down to and then select the SSID of the enterprise server you wish to connect to using WPA2-E (for example, **TEST-Ruckus-WPA2-E**).
5. Configure the following WPA2-E options in the pop-up dialog:
    - EAP method: **PEAP**
    - Phase 2 authentication: **MSCHAPV2**
    - CA certificate: (use whatever name you chose for your CA certificate, for example, **CA FreeRadius self-signed**)
    - Online Certificate Status: **Do not validate**
    - Domain: (enter the Common Name recorded above, for example, **Example Server Certificate**)
    - Identity: (enter whatever test user name was set up for the server, for example, **entuser1**)
    - Anonymous identity: (leave blank)

- Password: (enter the password set up for the server)

6. Tap the **CONNECT** button to apply settings and close the configuration page.
7. Verify that the test SSID appears at the top of the list with a status of Connected.

Import the Client Certificate

NOTE: Applies to EAP TLS only.

1. Obtain a client certificate in .p12 format. Be sure it includes the private key.

   NOTE: Although the imported CA certificate is a .pem file, NetAlly recommends a .p12 file format for the client certificate. Below is a sample openssl command to convert a client certificate from .pem to .p12 format:

   ```
   <path_to_openssl_bin>\openssl.exe
   pkcs12 -legacy -provider-path
   <openssl_path>/providers -export
   -inkey <privateKey>.key
   -in <client_cert>.pem
   -out <client_cert>.p12
   ```

2. Rename the certificate file, for example, **client.p12**.
3. Copy the .p12 file to a USB thumb drive.
4. Transfer the USB thumb drive to your EtherScope nXG, and then copy the .p12 file to the **Downloads** folder.
5. Open the Settings app.
6. Navigate to **Security > Encryption & credentials > Install a certificate > Wi-Fi certificate**. This opens the file picker.
7. Navigate to the **Downloads** folder, and select the .p12 file that contains your client certificate (for example, **client.p12**). A message prompts you to enter the password.
8. Enter the client certificate password to extract the certificate.
9. Rename the certificate, for example, **FreeRadius client**. A message confirms that the Wi-Fi certificate has been installed.

10. (Optional) Verify the client certificate installed correctly:
    a. Tap the system **BACK** button to return to Encryption & credentials.
    b. Tap **User credentials**.
    c. Verify that the name of your client certificate file (for example, **FreeRadius client**) is displayed.
11. Press the system **BACK** button to return to Encryption & credentials. You can now securely connect to your enterprise server.

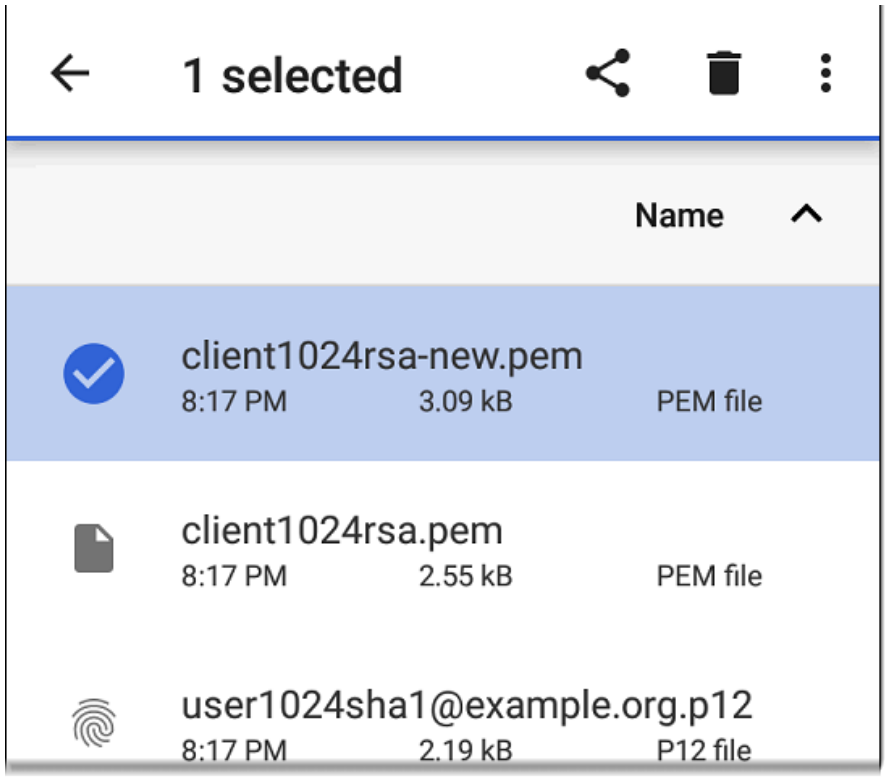
Back to Title and Contents

Sharing

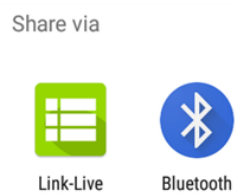
The system Files app lets you share files from internal or external storage can to Bluetooth, a printer, or the Link-Live cloud service. You can upload one selected file or multiple files at once.

NOTE: Many apps on your unit allow you to save settings and configuration information directly to Link-Live. See Saving App Settings and Configurations.

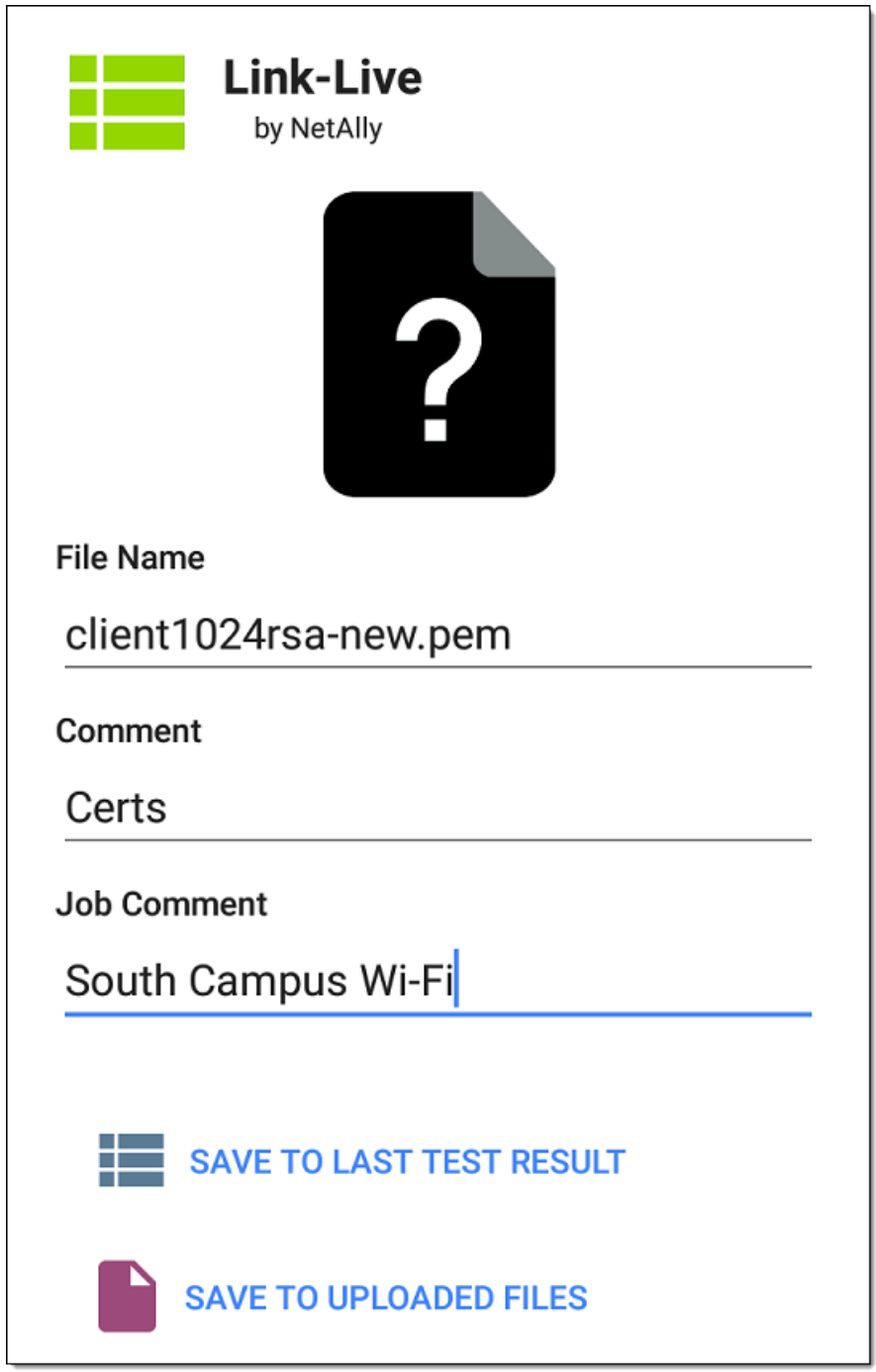
1. On the Home Screen, open the Files app by tapping the icon .
2. Navigate to the folder containing the files you want to share using Navigation menu or the left-side navigation drawer.
3. Long press on one or multiple files to select it.



4. Tap the share icon in the top toolbar to open the Share pop-up dialog.



5. Tap to choose a sharing method and follow the system prompts to share the file or files.
   a. If uploading to Link-Live, tap the **Link-Live** option.



b. Enter any **Comments** you would like attached to your file.

c. Select **SAVE TO LAST TEST RESULT** or **SAVE TO UPLOADED FILES**. Your files are then uploaded and viewable on Link-Live.com. (The **SAVE TO LAST TEST RESULT** option attaches the image to your most recently run AutoTest, Performance, iPerf, or Cable Test results on Link-Live.com.)

   See the Link-Live chapter for more information on using Link-Live with your EtherScope nXG.

Sharing a Screenshot

To take and share a screenshot:

1. Press and hold the **Power** button and the **Volume Down** button at the same time for one second. (See Buttons and Ports for button locations). The unit beeps and adds a notice to the Notification Panel.
2. Access the file either by opening the Notification Panel and tapping the screenshot notice or by using the Files app.

3. Follow the procedure in Sharing to share the image using Link-Live, Bluetooth, or another configured application.

Changing the Device Language

The EtherScope nXG supports Chinese, English, and Japanese language displays.

To change the device's interface language:

1. Go to the Device Settings screen by tapping the Settings  icon at the bottom of the Home screen.
2. Scroll to and select **System**.
3. Select **Languages & input** and then **Languages**. This displays the Language preferences screen.
4. On the Language preferences screen, select **+ Add a language**.
5. Tap the language option you want. This returns you to the Language preferences screen.
6. Touch and hold the icon  to the right of the language, and then drag the language to

the top (number 1) place on the list.

The EtherScope displays the chosen languages, as available, in the priority order shown on the Language preferences screen.

NOTE: The EtherScope nXG supports Chinese, English, and Japanese. This user guide supports Chinese and English. If you choose Japanese as the device language, the system uses the English user guide. See How to Use this Guide for more information about the user guide.

NOTE: Manuals are also available for web download at: https://www.net-ally.com/support/user-guides/

Back to Title and Contents

EtherScope nXG Settings and Tools

The EtherScope nXG features a common set of tools and General Settings that apply to multiple NetAlly apps and testing behaviors. This chapter covers settings, icons, and notifications *specific to EtherScope nXG*.

(See the Device Settings topic for information on the system settings.)

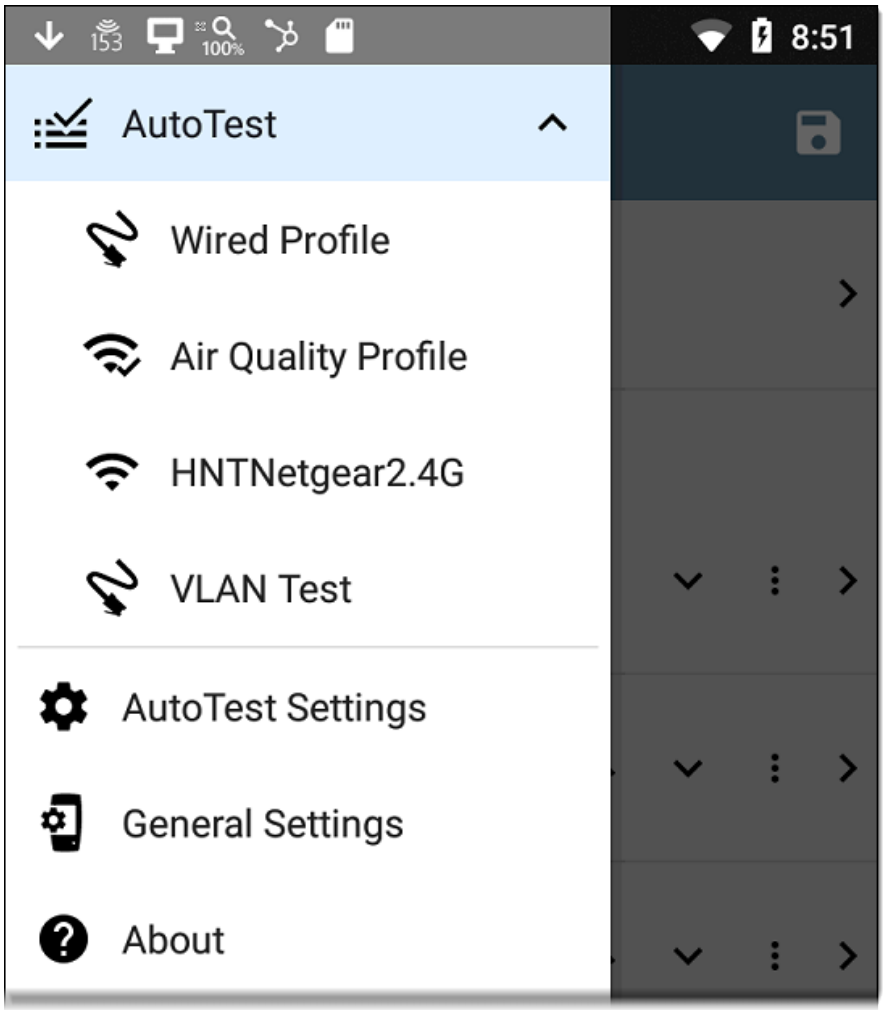
Access common settings and informational screens for the NetAlly testing apps (like AutoTest or Capture) by opening the left-side Navigation Drawers  or Settings  .

Navigation Drawer

Many system apps, including the NetAlly test apps, contain additional settings, tools, and information in a "navigation drawer" that slides out from the left side of the screen.

To open the navigation drawer:

- Tap the menu icon  at the top left of one of the testing application screens.
- Touch and drag (swipe) to the right from the very left side of the app screens.



As an example, the AutoTest navigation drawer (above) provides access to the enabled AutoTest profiles, AutoTest Settings, General Settings, and the About screen.

Settings for each specific app are described in the chapter for the app.

About Screen

The About screen displays the model number, serial number, MAC addresses, software versions, SFP details, and current AllyCare contract status for your EtherScope nXG.

If a **User-Defined MAC** is enabled in an NetAlly apps' General Settings or in the "Wired Profile Settings" on page 226, (User-defined) appears next to the MAC address on the About screen.

Exporting Logs

The About screen contains the Export Logs function, which allows you to save your unit's logs for analysis by NetAlly's technical support team.

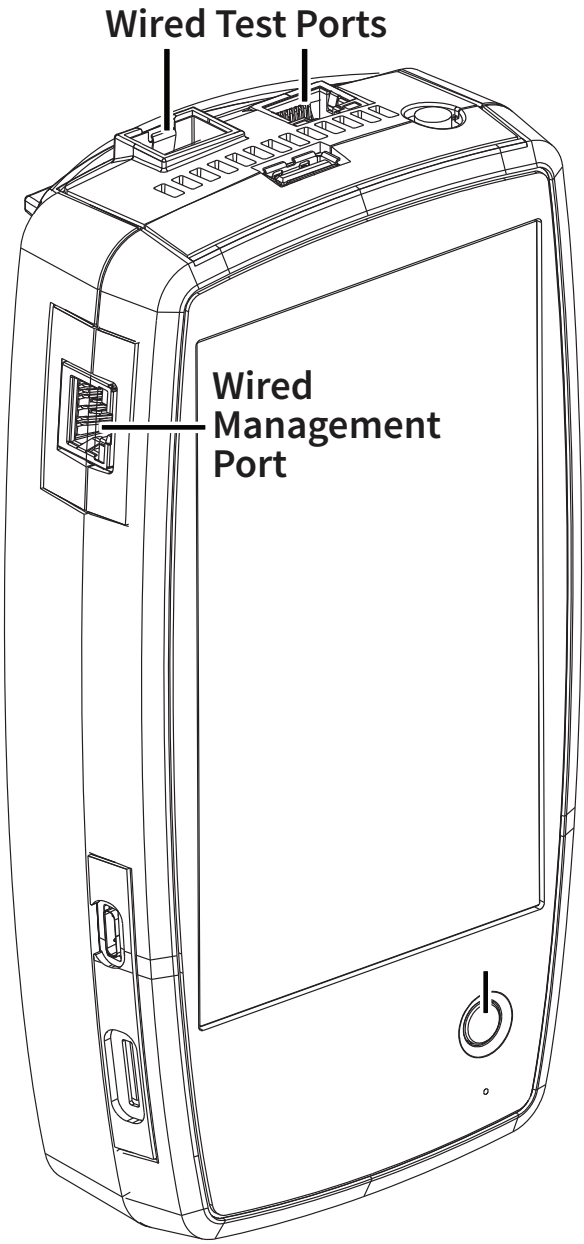
Tap the **EXPORT LOGS** link to download a .tgz file to the Downloads folder on your unit. Open the Files app to transfer the file using email or another method. (See Managing Files.)

Exporting Settings for All Apps

The action overflow icon ⋮ on the About Screen supports the importing or exporting of settings for *all* applications that allow import/export. See Importing and Exporting Settings for All Apps for details.

Test and Management Ports

The EtherScope nXG has two wired RJ-45 copper ports, a fiber port, and two Wi-Fi radios, each with specific test or management functions described in this section.


Wired Test Ports
Internal Wi-Fi Test Port
Internal Wi-Fi Management Port
Wired Management Port

Either the top copper port or fiber port can act as the Wired Test Port, so in total, the EtherScope has *four* network interfaces: 1) Wired Test, 2) Wi-Fi Test, 3) Wired Management, and 4) Wi-Fi Management. The Wi-Fi test radio is controlled by in general settings in NetAlly applications such as AutoTest and AirMapper. The Wi-Fi management radio is set up by system network settings. See "Selecting Ports" on page 88 below for more information.

See the sections below for more information on the ports. Also see Buttons and Ports and the technical Specifications if needed.

Test Ports

Wired Copper Test Port: The copper test port is the RJ-45 port on the top of the unit. To disable, unplug the connection.

Wired Fiber Test Port: The SFP and fiber test port is also on the top of the unit. To disable, unplug the connection.

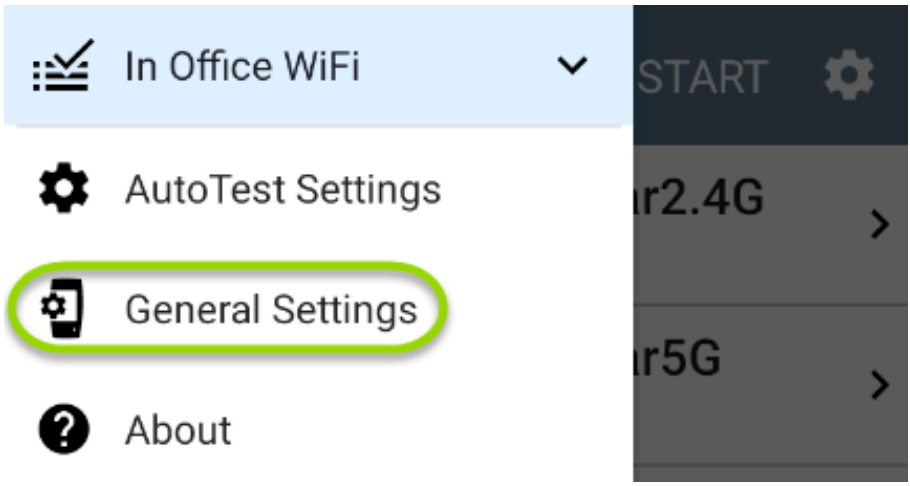
Wi-Fi Test Port: The internal Wi-Fi test adapter is a 4x4 Dual-band 802.11ac wireless radio. To disable, see General Settings in the testing apps' left-side navigation drawer.

NOTE: If both the top fiber and copper ports are connected to an active network, the EtherScope uses the fiber link as the Wired Test Port connection.

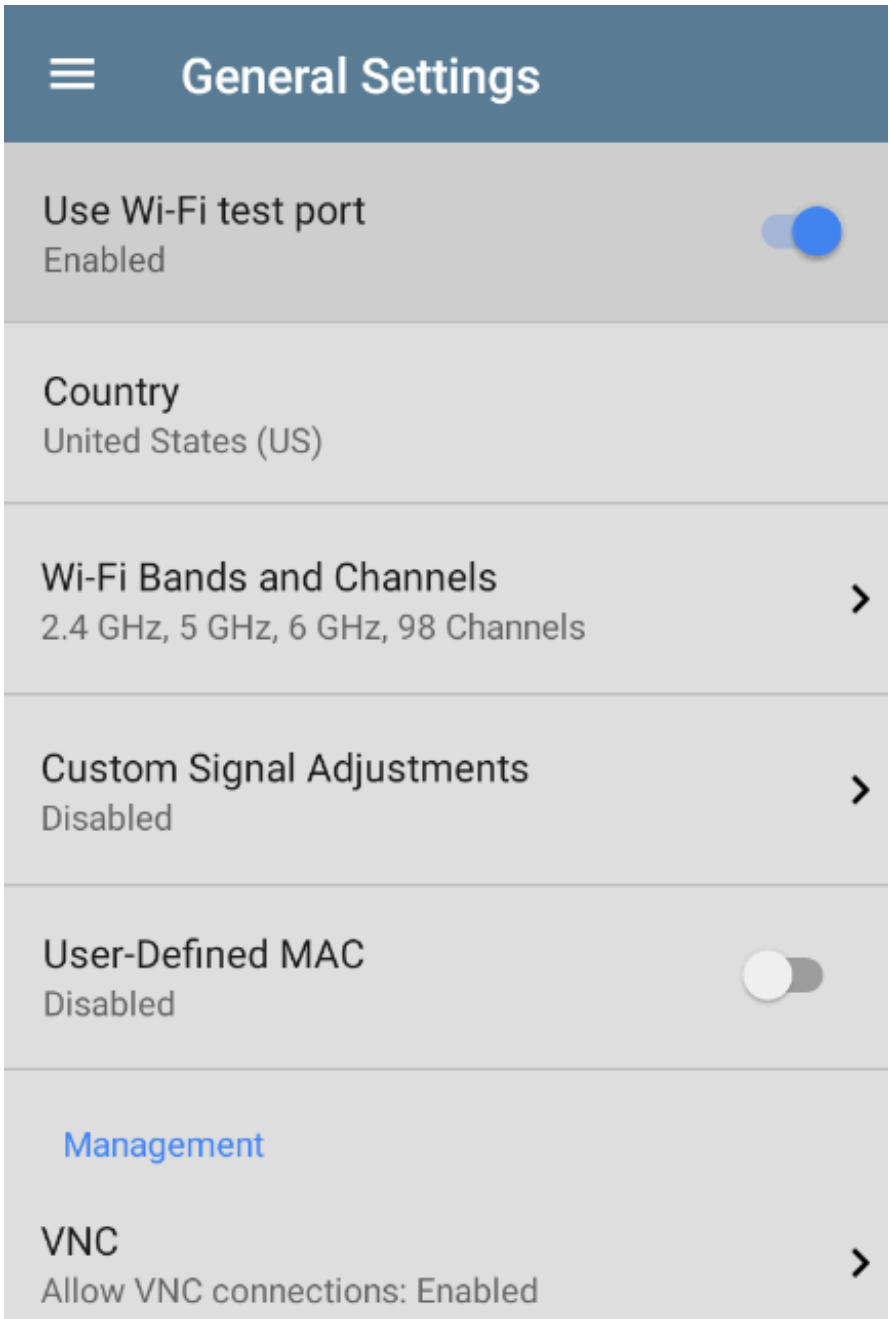
EtherScope runs Wired and Wi-Fi AutoTests, Captures, Discovery, and other comprehensive network analysis apps over the test ports. The Wi-Fi test radio is primarily controlled by the settings in applications, especially AutoTest.

You must also run an AutoTest Wired or Wi-Fi Profile to establish a link on the Wired or Wi-Fi test ports. If the AutoTest app is not currently open, the last Wired Profile in the profile list runs automatically when you power on the unit or EtherScope detects a new copper link in the top Wired Test Port. Wired fiber connections and Wi-Fi Profiles must be started manually in the AutoTest app.

Note that the General Settings affect how you can use the test port. (The General Settings are accessible from the left-side navigation drawer from most NetAlly testing apps.)



The **Use Wi-Fi test port** option must be enabled for the test ports to function. (Enabled is the default setting.)



NetAlly also recommends that you enable all Wi-Fi Bands and Channels before setting up Wi-Fi Test Profiles:

1. Tap the **Wi-Fi Bands and Channels** option to open the Wi-Fi Bands and Channels screen.

2. Tap the Wi-Fi band(s) option to open a selection screen, and then enable all available bands.

3. Tap the option for each frequency band to open a selection screen, and then enable all available channels for each band.

This process makes it easier to set up the Wi-Fi Test Profiles, which you can limit to specific channels, APs, SSIDs, etc. See AutoTest Wi-Fi Profile for more information.

See General Settings for more information about all General Settings options.

 Management Ports

 **Wi-Fi Management Port**: The internal Wi-Fi management port runs on the main system's 1x1 Dual-band 802.11ac + Bluetooth 5.0 wireless adapter, which is configured in the system Device Settings. See "Connecting to Wi-Fi" on page 56 to configure this connection.

 **Wired Management Port**: The wired management port is the RJ-45 port on the left side of the unit.

The Wi-Fi management radio is set up by the system network settings. The Management Ports provide full Internet access and a more stable network connection than the Test Ports, which may frequently drop links and reconnect or resume scanning.

EtherScope can run Discovery, Ping/TCP Connect tests, Path Analysis, and iPerf tests on the management ports, but not AutoTests, packet captures, or Performance tests.

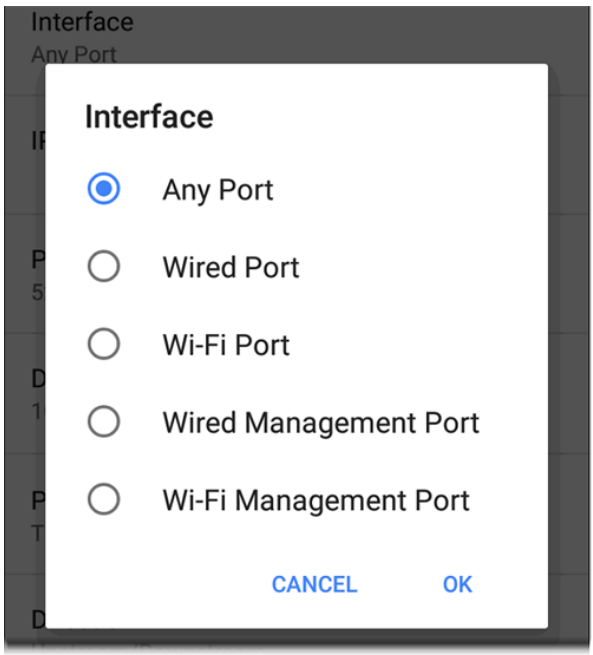
Selecting Ports

Some of the individual NetAlly testing apps let you select which port interface to use for tests or analysis. For example:

- You may want to verify that you are getting a reliable connection to the Internet and the Link-Live cloud service while you are actively using the Wi-Fi Test port to perform an AirMapper survey. To check connectivity, you can configure the Ping/TCP app to use the Wi-Fi Management port to run a continuous background ping to the Internet.

- Each port can connect to different networks. For example, an organization might have one network for visitors and another for staff. You can use multiple ports to check connectivity on each network without the need to link and relink through a single interface.

To change the port, tap an app's settings icon to display the settings screen. Then tap **Interface** to select the port.



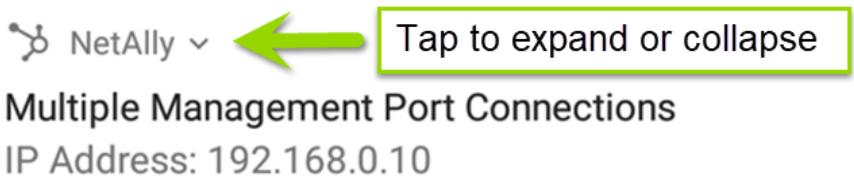
- The top two Wired and Wi-Fi Ports refer to the Test ports.
- An AutoTest Wired or Wi-Fi Profile must run to establish test port links.

- The last listed Wired Profile runs automatically when you start up the EtherScope if a connection is available.

Test and Port Status Notifications

EtherScope nXG shows notifications from the NetAlly testing apps and unit ports in the top Status Bar and Notification Panel. Swipe down on the Status Bar to view the notifications.

On each notification, you can tap the title and down arrow to expand the box and view more details or options.



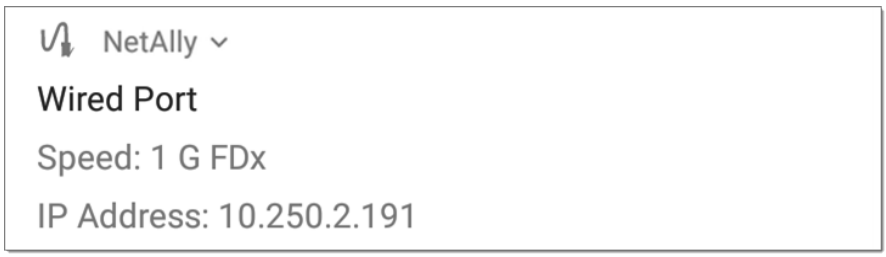
Various EtherScope icons appear in your Status Bar, as listed in the following sections.

> NOTE: Read Test and Management Ports for descriptions of the port functions.
>
> See General Settings for settings that control port functions.

Test Port Notifications

Active network connections on the test ports are established using the AutoTest app.

A **Wired Test Port** connection, called the "Wired Port" in app settings, is established in either the top RJ-45 Ethernet port or the top Fiber port.



> NOTE: If both the fiber and top copper ports are connected to an active network, the EtherScope uses the fiber link as the "Wired Port" for testing.

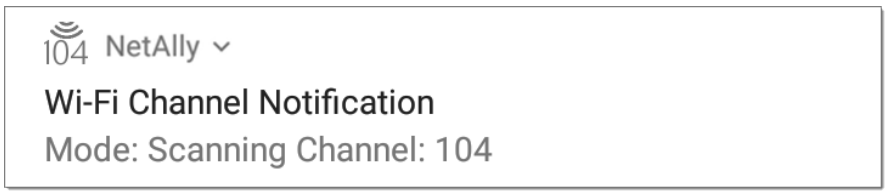
or


The **Wi-Fi Test Port** status displays with the wireless channel number under a Wi-Fi or Link icon. Channels in the 6 GHz band (EXG-300/300E only) display with an E by the Wi-Fi or Link icon.

> 

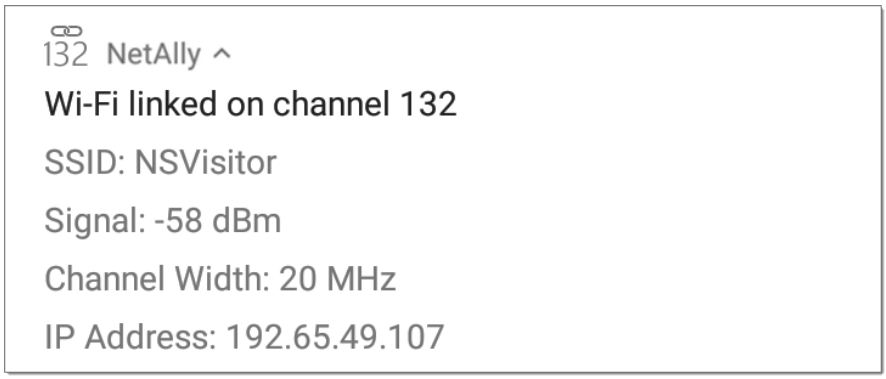
When the EtherScope unit is dwelling on a Wi-Fi channel (in this case channel 64), the

channel number is static. When the EtherScope is scanning for discovery, Wi-Fi analysis, or air quality measurements, the channel number changes dynamically to show which channel is currently being scanned.



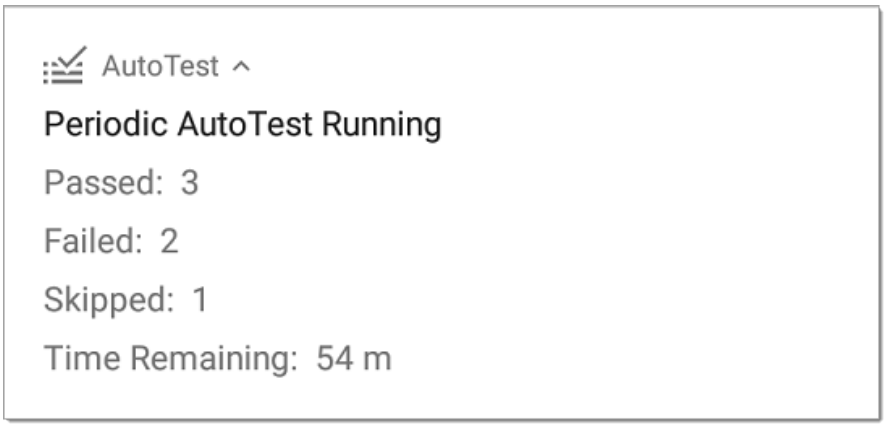
 or  or  When the EtherScope unit connects to an AP on a Wi-Fi channel, the channel number is static, and the Link icon displays above it. If the link is dropped, the channel number changes to an X.

 (EXG-200 only) Active scanning while the EtherScope unit is in all-channel-scanning mode.



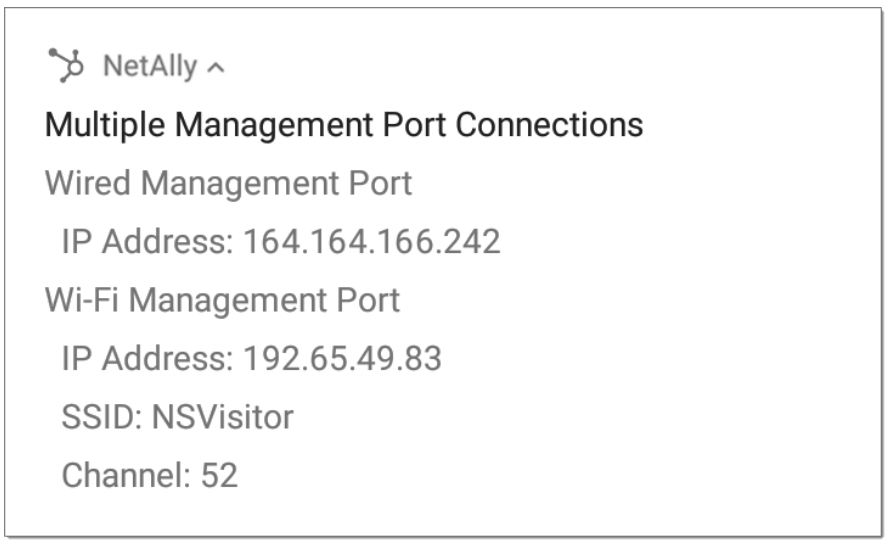
 **Periodic AutoTest** is running or has completed. When Periodic AutoTest is running,

the Wired and/or Wi-Fi Test Ports may not be available to other testing apps.



Management Port Notifications

A **Management Port** connection is established through the left-side RJ-45 Management port and/or the main system Wi-Fi adapter.



 A **Wired Management Port** connection is established through the left-side RJ-45 Management port. Its details are displayed under the Management Port notification (above).

 A **Wi-Fi Management Port** connection is established via the main system Wi-Fi adapter. Its details are displayed under the Management Port notification.

If your Management connection is lost, the following notification displays.

Discovery Notifications

The Discovery notifications show the progress of the discovery process. See the Discovery app chapter for more information.

 The active discovery process is running and has progressed to the specified percentage.

 No links are currently available for active discovery, either because none of the ports

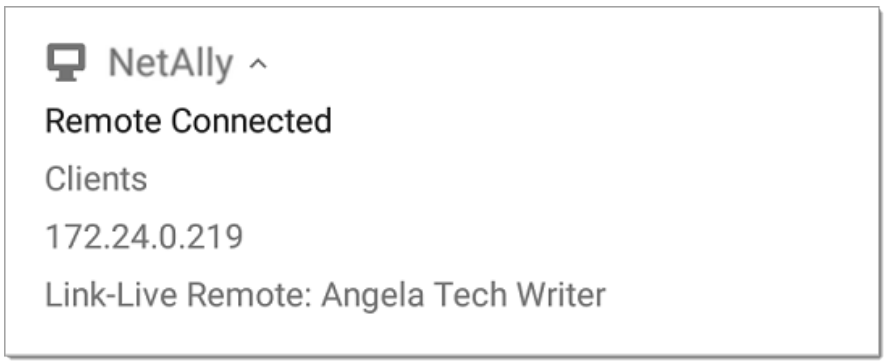
enabled for discovery are connected or AutoTest is running. Discovery is temporarily disabled when AutoTest is running.

PoE

PoE Indicates that your unit is connected to a Power over Ethernet source. See PoE Charging.

VNC/Link-Live Remote

A remote VNC connection is active through a standalone VNC client and/or the Remote function in Link-Live Cloud Service.

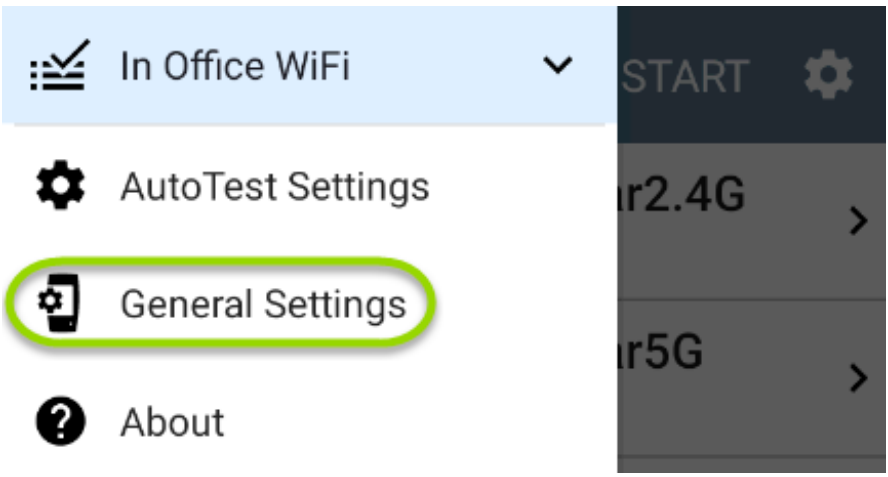


Back to Title and Contents

EtherScope nXG General Settings

EtherScope's General Settings control test and management-related connections that affect multiple test apps.

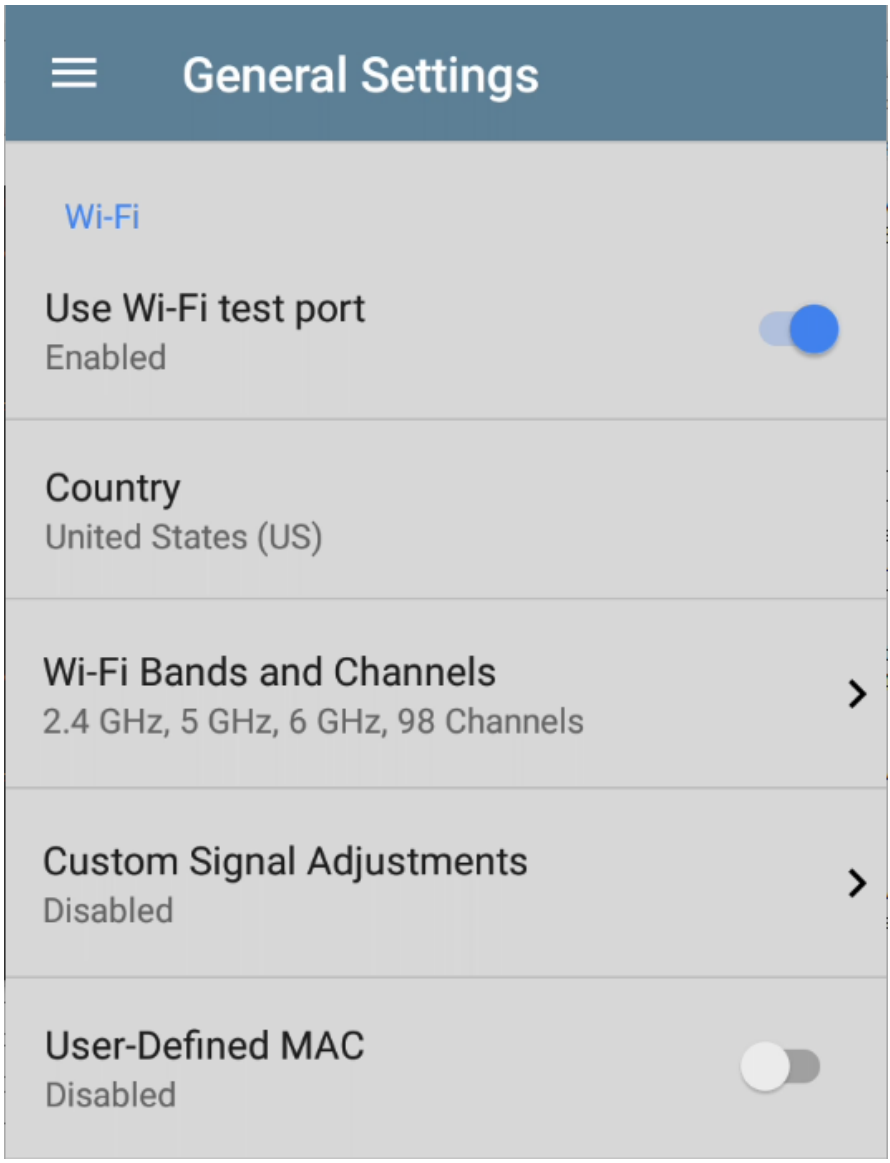
Access the General Settings from the left-side navigation drawer in the NetAlly testing apps, such as AutoTest, Discovery, Capture, iPerf, etc.



See also Test and Management Ports and Test and Port Status Notifications for related information on port functionality and status icons.

Wi-Fi

The Wi-Fi General Settings control functions of the Wi-Fi Test Port functions.



Use Wi-Fi test port: Enable or disable Wi-Fi tests, connections, and measurements in the testing apps, including AutoTest Wi-Fi Profiles and the Wi-Fi analysis app.

NOTE: This setting does not disable the main system device Wi-Fi function, which controls the Wi-Fi Management port connection. See Device Settings to disable the system Wi-Fi.

Country: Set the country code for your unit. This setting controls which channels can be scanned and which channels are reported as illegal or which may have Dynamic Frequency Selection (DFS).

Wi-Fi Bands and Channels: Select the wireless frequency bands and channels the unit scans for devices and measurements such as utilization.

Tap each band or channel setting to open a selection dialog.

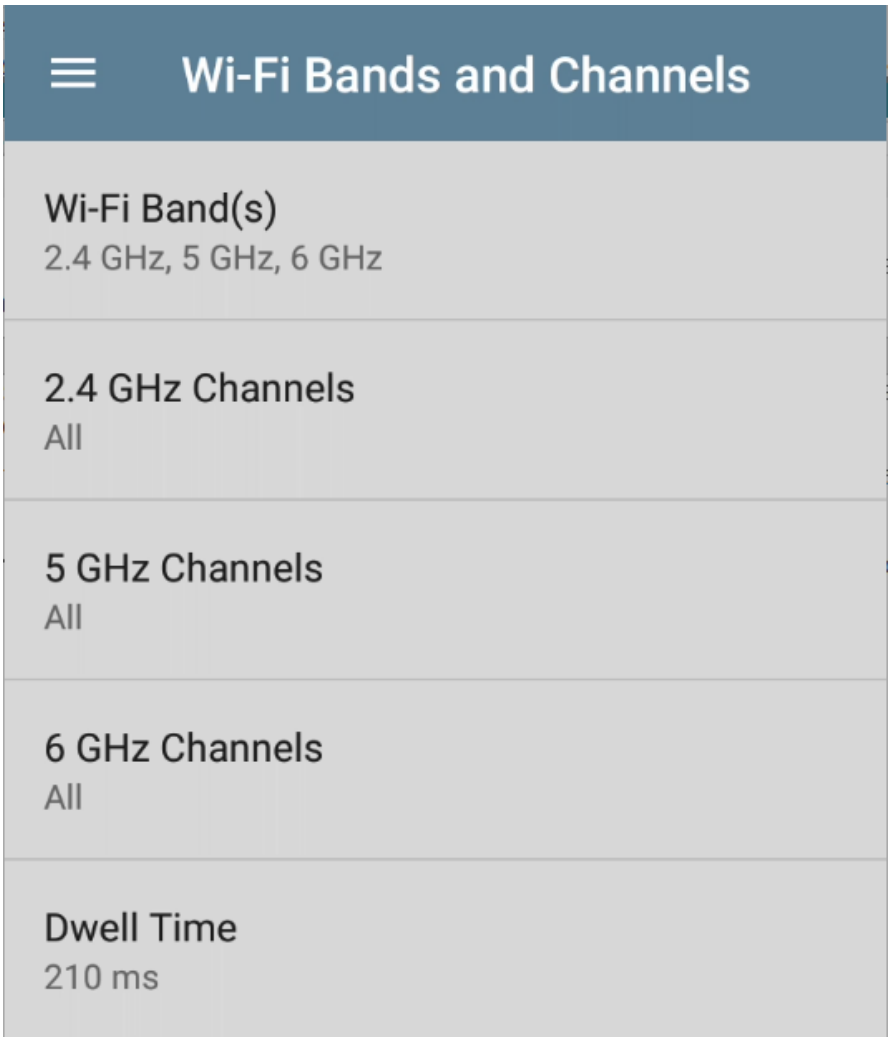
Unchecking a Wi-Fi Band prevents any linking to, or scanning of, channels in that band.

Unchecking a Channel means the channel still links but does not get scanned.

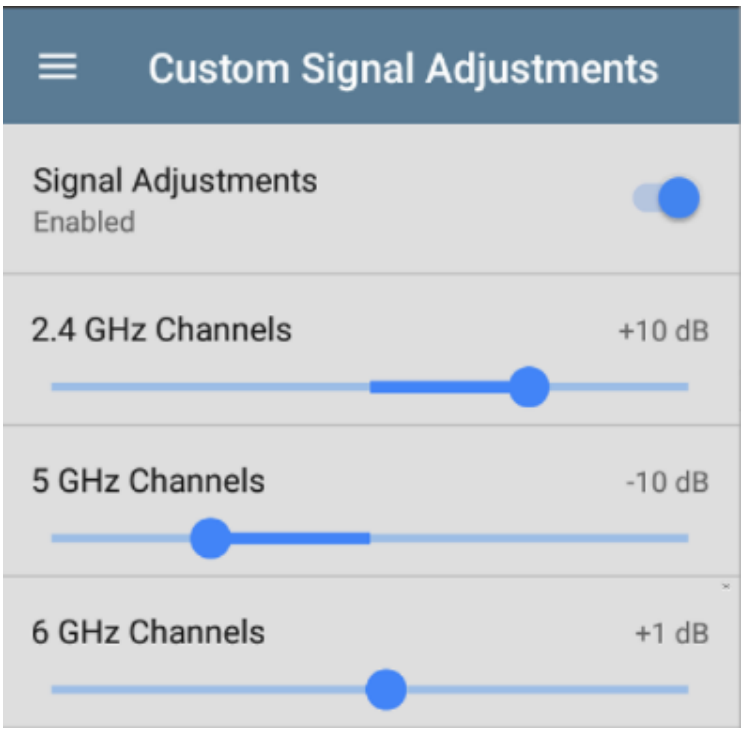
Channel changes affect these apps: Air Quality scans, Wi-Fi results (scanning), Discovery, AirMapper (passive surveys)

Channel changes do *not* affect these apps: AutoTest results (linking), Wi-Fi Capture, AirMapper (active surveys)

Tap the **Dwell Time** field to adjust the amount of time the EtherScope stays on each channel to gather data.



Custom Signal Adjustments: Tap this setting and then tap the **Signal Adjustments** toggle to open an adjustment panel for each frequency band. You can adjust the signal strength for each band from -20 dB to +20 dB.



Combine Utilization: (EXG-200 only) Enable this setting to combine 802.11 and non-802.11 channel utilization into one total utilization measurement. In environments with 802.11ax traffic, turn this setting on to accurately measure channel utilization. When this setting is enabled, EtherScope app screens that typically show both 802.11 and non-802.11 utilization (such as the

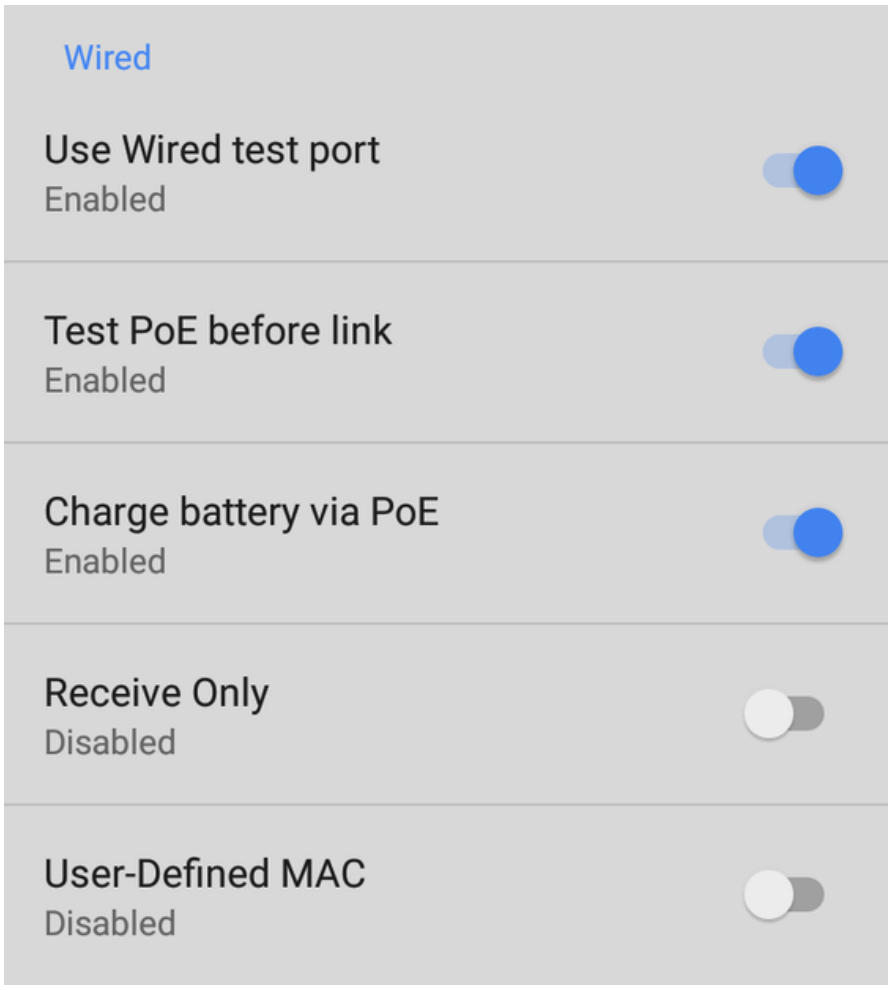
Wi-Fi Channels Map) now show the total utilization.

User-Defined MAC: This setting affects the Wi-Fi Test Port only. Tap the toggle switch to enable a user-defined MAC address. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. Tap the lower field to enter your desired MAC address for the EtherScope. When a User-Defined MAC is enabled, **(User-defined)** appears next to the MAC address on the About screen and on relevant test result screens.

> NOTE: Both Wi-Fi and Wired test ports have their own User-Defined MAC settings.

Wired

Wired General Settings control functions of the Wired Test Port.



Use Wired test port: Enable or disable wired tests, connections, and measurements in the testing apps, including AutoTest Wired Profiles.

NOTE: the tester reboots when you leave the General Settings screen after you toggle this

option. (This changes the powered state of the wired test port.)

Test PoE before Link: By default, an AutoTest Wired Profile performs the Link test before the PoE test can complete. Enable this setting to make your EtherScope complete the PoE test before the Link test. Enabling this setting forces PoE negotiation to be completed before establishing link, improving compatibility with some switches.

Charge Battery via PoE: (Available if supported by tester hardware.) This setting is enabled by default. If you do not want your EtherScope unit to charge when connected to a switch with PoE, tap the toggle button to disable. An AutoTest Wired Profile must run and detect PoE availability before the unit can use it for charging.

See also PoE Charging.

Receive Only: Enabling this setting prevents the EtherScope from transmitting packets on the Wired Test Port. You can also use the **Stop After** function in Wired AutoTest Profile Settings to hide the AutoTest cards that require transmit capability. Set the AutoTest **Stop After** setting to

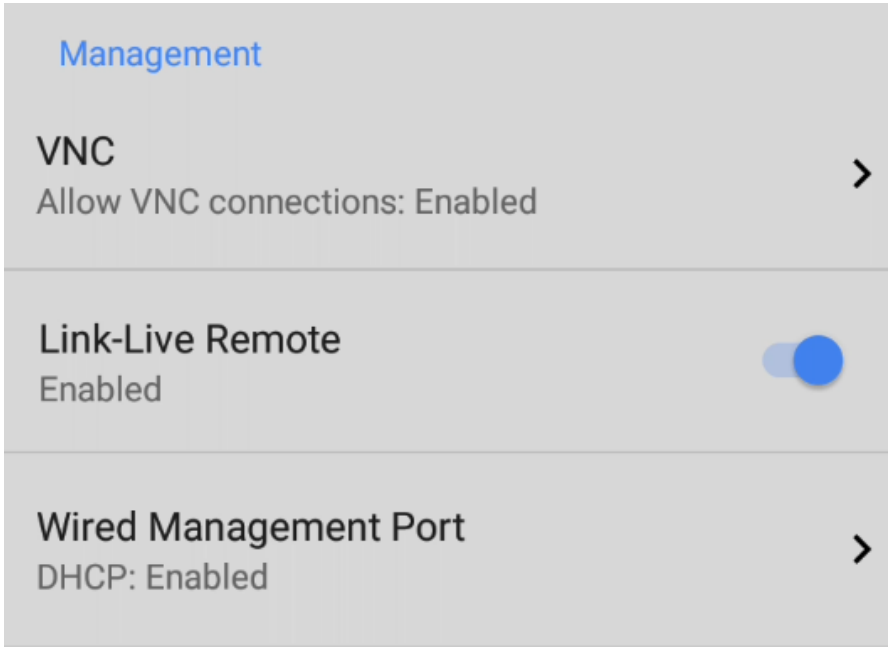
Switch. Otherwise, when **Receive Only** is enabled, the Wired DHCP/Static IP test shows a Result Code of "Interface is configured to only receive packets," and the subsequent tests do not run.

User-Defined MAC: This setting affects the Wired Test Port only. Tap the toggle switch to enable a user-defined MAC address. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. Tap the lower field to enter your desired MAC address for the EtherScope. When a User-Defined MAC is enabled, **(User-defined)** appears next to the MAC address on the About screen and on relevant test result screens.

> NOTE: This definition can be overridden by a profile-based user-defined MAC. See " Wired Connection Settings" on page 230 for more information.

Management

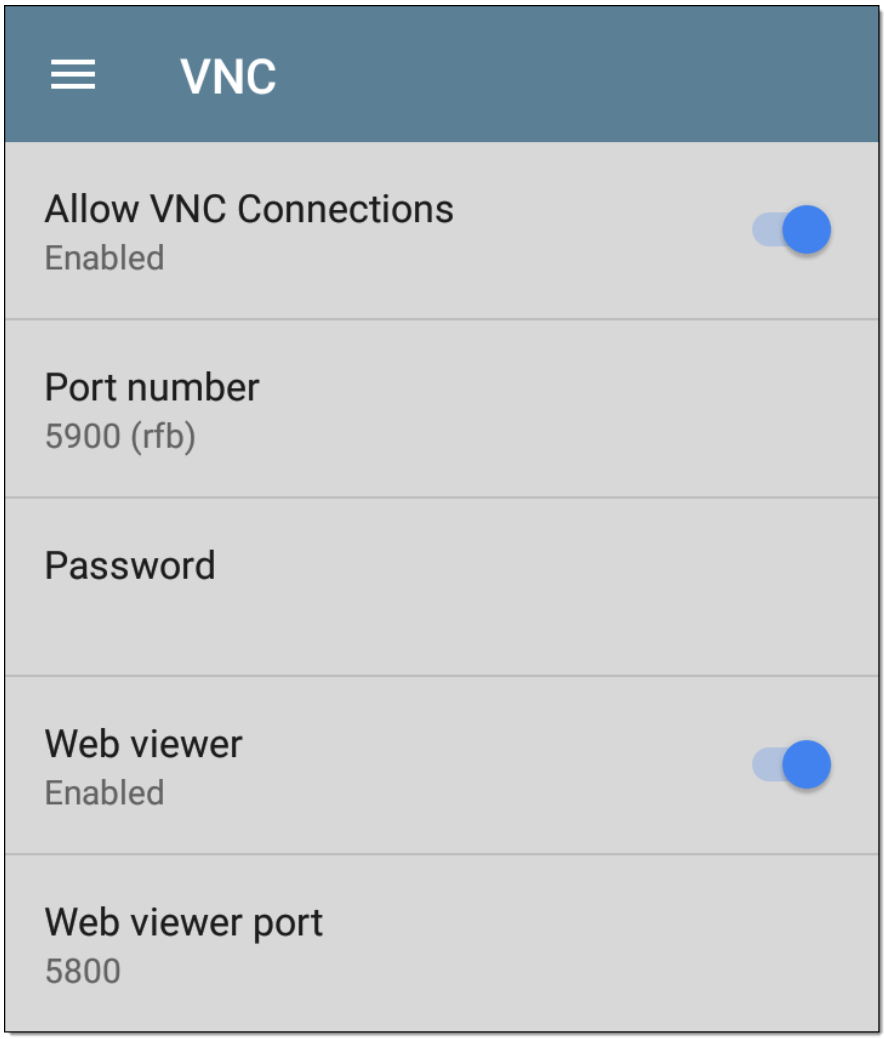
These settings affect management-related functions on the EtherScope, including remote access.



VNC

Tap **VNC** to open the VNC settings screen and configure your unit's VNC connections for remote operation.

See Using VNC for more information about connecting to a VNC client or Link-Live Remote.



Allow VNC Connections: (Disabled by default.) Tap the toggle button to enable remote connections from VNC clients and display VNC options.

Port number: Tap to enter a port number other than the default.

Password: Tap to enter a password, which a VNC user must enter to access the EtherScope interface remotely.

NOTE: If you set a **Password** here in the **VNC** settings, the password is required to connect to both a standalone VNC client and the Remote feature at Link-Live.com.

Web viewer: Tap the toggle to enable or disable web viewer access.

Web viewer port: Tap to enter a port number other than the default.

 Link-Live Remote

This setting enables or disables the EtherScope's remote control function in Link-Live Cloud Service at Link-Live.com.

NOTE: The Link-Live Remote feature is only available to customers with an active **AllyCare** subscription. Your EtherScope must be claimed. See NetAlly.com/Support for more information.

Access the Remote function on the **Units** page at Link-Live.com by selecting the claimed EtherScope nXG.

Wired Management Port

DHCP: This setting controls IP address assignment of the RJ-45 Wired Management Port on the left side of the EtherScope. By default, DHCP is enabled. Tap this field and tap the toggle button to disable DHCP and enter static IP information.

Preferences

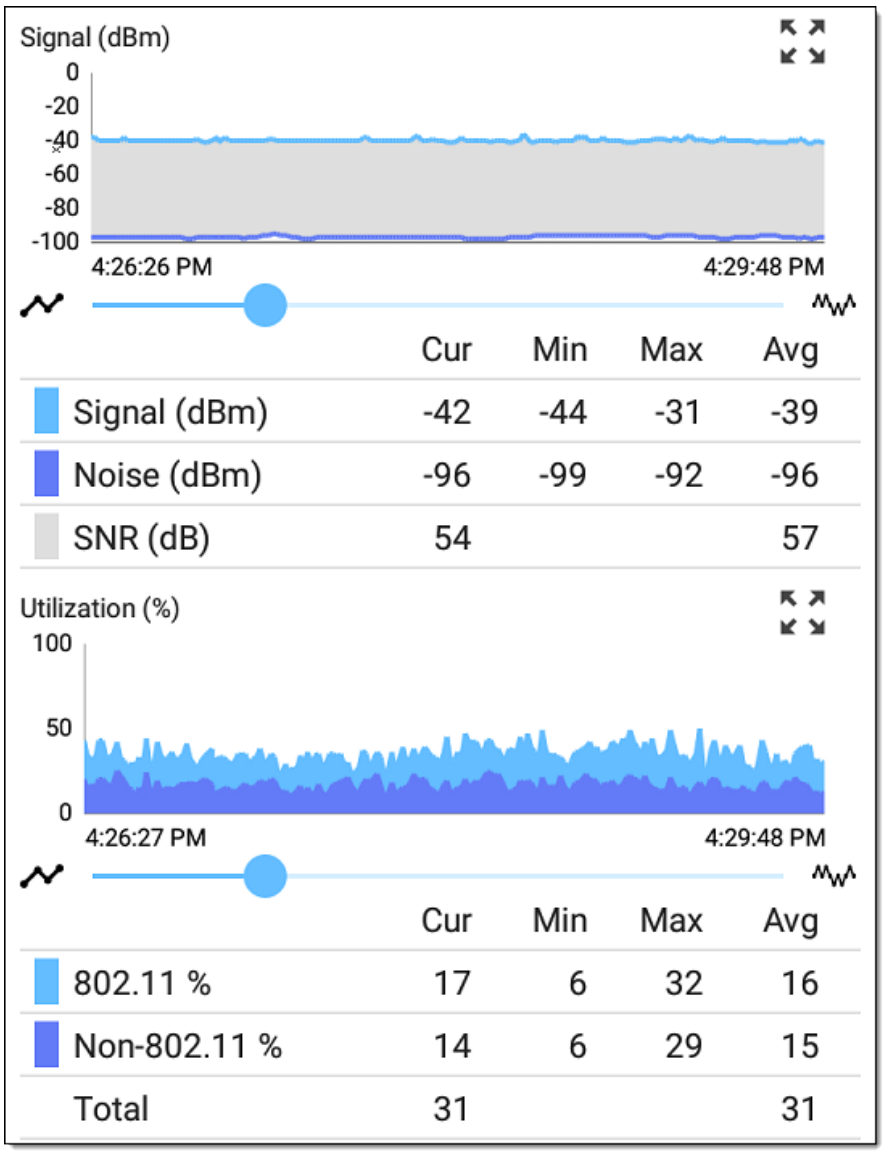
Distance Unit: This is the unit EtherScope uses for distance measurements in the testing apps, specifically AirMapper and Cable Test.. Tap the field to switch between Feet and Meters.

Save Locally Only: Tap this toggle field to change the unit default behavior for savings files. (The default is to give you the option to save to Link-Live *or* locally.)

Back to Title and Contents

Trending Graphs

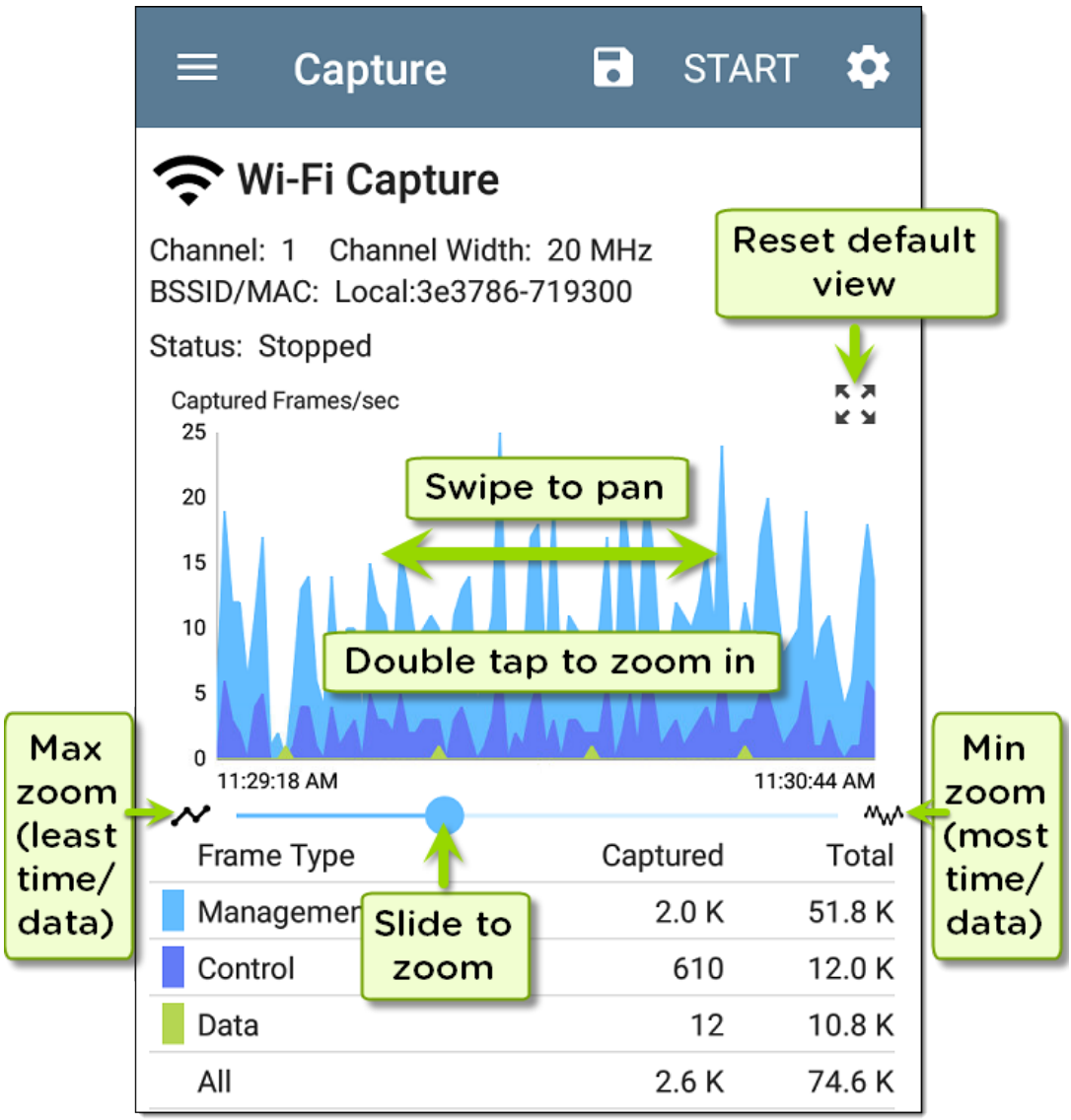
Many of the EtherScope nXG testing apps feature time-based line graphs of recorded measurements, which you can pan and zoom to view different time intervals. For example, the image below shows the Signal and Utilization graphs from the AutoTest Wi-Fi Link Screen.



The graphs update in real time and then save and display data for up to 24 hours (depending on test type and/or link status).

A legend indicates the measurements that correspond to each plotted color.

For another example, the image below shows the Capture app graph.



- To pan, or move backward and forward in time, touch and drag (swipe) left and right on each graph.
- To zoom in on a specific point, double tap the point on the graph. The view zooms in 2x (or displays half the amount of time) for each double tap.
- To zoom in or out, decreasing or increasing the time interval displayed, drag the slider or tap the slider bar below the graphs.
    - The largest time interval (maximum zoom out) is the total time data has accumulated.
- To reset the graph to the default time interval, tap the zoom reset icon  .
    - The zoom reset icon appears *after* you zoom or pan on the graph.
    - The default time interval varies across different apps.

The following apps and screens contain trending graphs:

- AutoTest Wi-Fi Profiles – Link and Channel
- Ping/TCP – Ping Test

- Capture
- Discovery – Interface Statistics
- Wi-Fi – RF and Traffic Statistics
- Performance
- iPerf

Common Icons

The icons below appear in multiple NetAlly test and system apps.

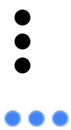
Menu Icon - opens the left navigation drawer or other menus

Refresh Icon - restarts testing and measuring on the current screen

Settings Icon - opens configuration options for the current app

Save Icon - saves settings or files or loads saved configurations

Floating Action Button (FAB) - opens the Floating Action Menu, which contains additional actions



Action Overflow Icon - contains additional actions

Directional Arrows (or Carets) - indicate the ability to "drill in," open a screen, or expand a panel for more detailed information, or to change the order of a list

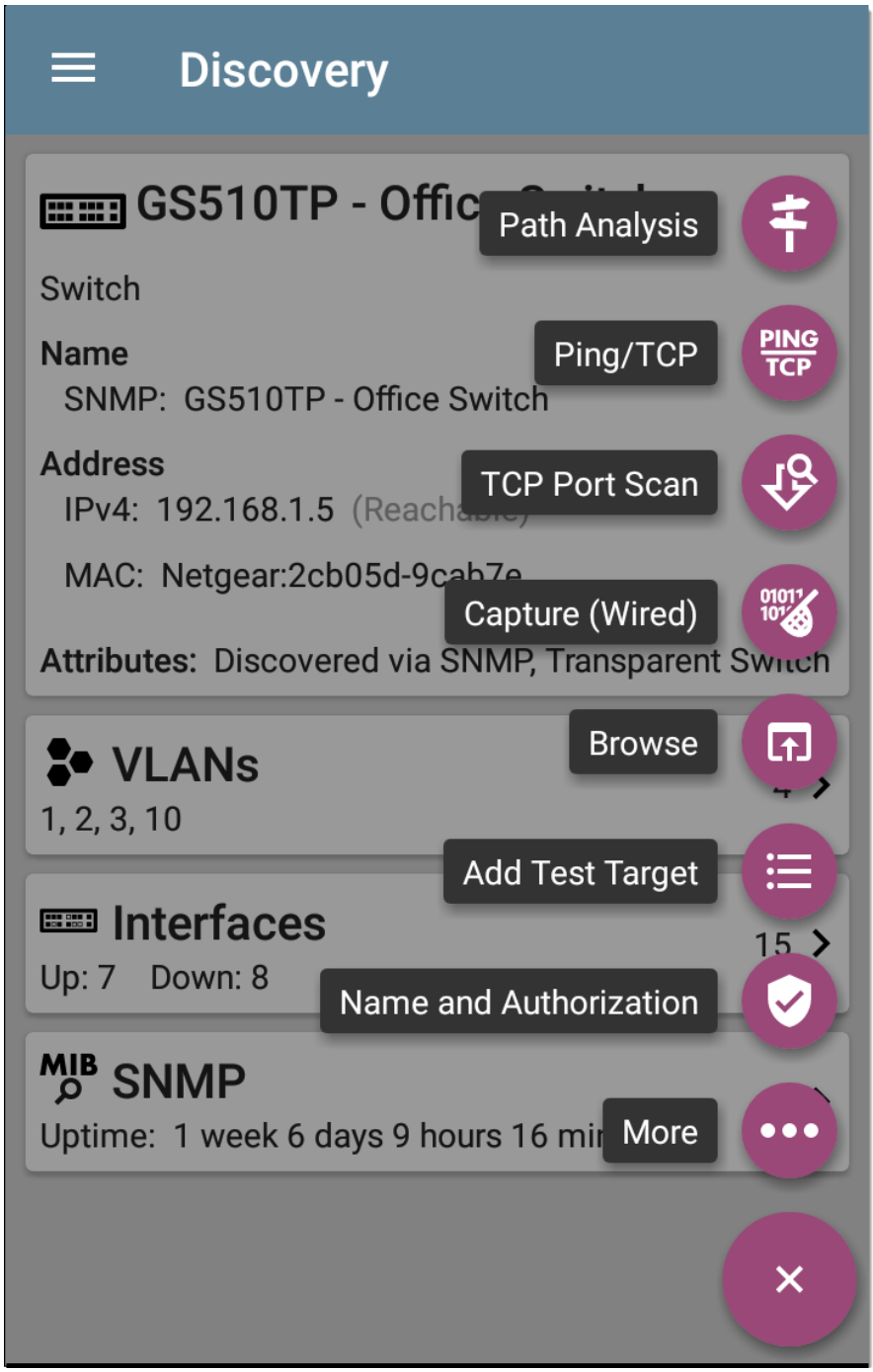
For explanations of the EtherScope icons that appear in the Status Bar at the top of the screen, see Test and Port Status Notifications.

Floating Action Button (FAB) and Menu

Many system applications, including NetAlly's AutoTest and Discovery apps, feature a Floating Action Button or "FAB"  that opens a floating action menu with more options for analysis.

The FAB on the main AutoTest app screen allows you to add new testing Profiles.

The FAB on the Discovery app's Details screen opens other apps for further testing of the selected device.



See the chapter for each app for descriptions of the FABs specific to that app. For example, see Discovery App Floating Action Menu describes the Discovery FAB in more detail.

Common Tools

Web Browser/Chromium

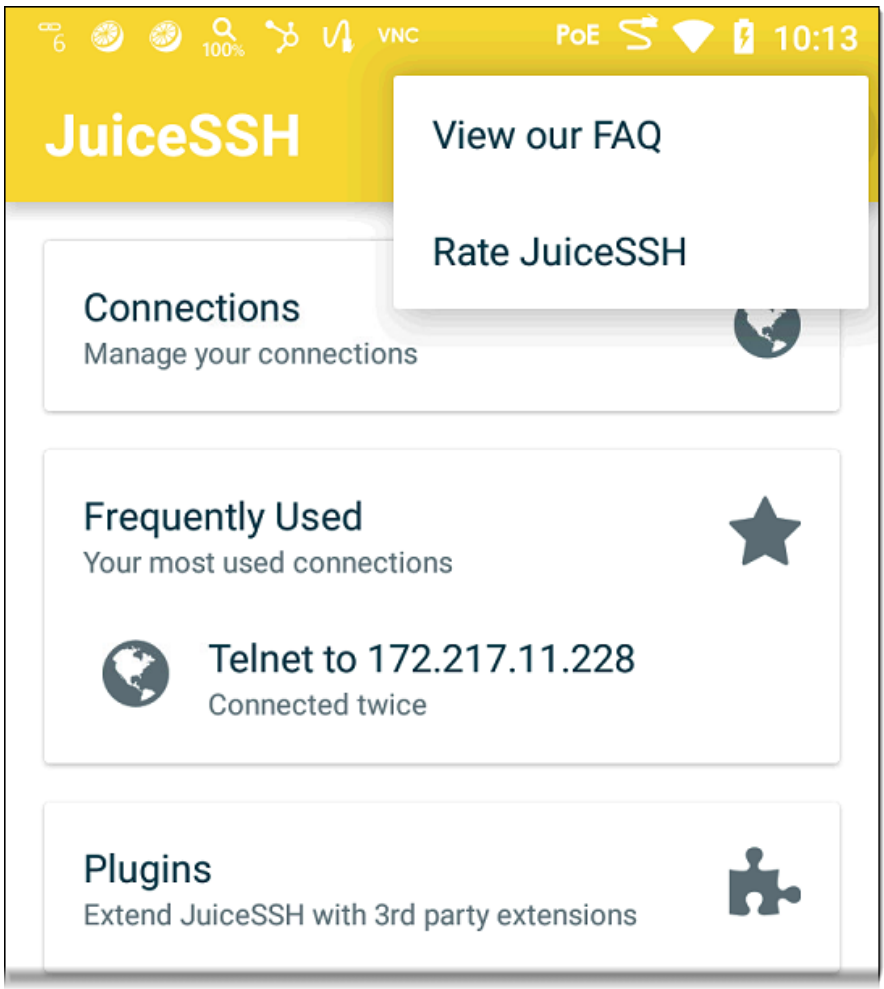
Some of the testing apps, like AutoTest, Ping/TCP, and Discovery, give you the option to **Browse** to internet addresses using a web browser application. EtherScope has the Chromium browser pre-installed.

Telnet/SSH

Starting with v1.1, EtherScope has the JuiceSSH application pre-installed. Both the AutoTest and Discovery apps provide options to start a Telnet or SSH session using the current device address. Selecting these options opens JuiceSSH and starts a session. You can also open JuiceSSH from the Apps screen.

The JuiceSSH app maintains a list of previous connections. When opened from a NetAlly app, JuiceSSH uses the first connection in the list that matches the IPv4 address or device name and type. If no match is found, a new connection entry is created and used.

As a third-party app, JuiceSSH contains its own tutorials. For additional help, tap the action overflow button ⋮ at the top right of the JuiceSSH app screen, and select **View our FAQ**.



Camera and Flashlight

The camera lens and flash are located on the back of the unit. (See Buttons and Ports.)

The Camera application  is located in the Apps screen and on the Home screen by default. Tap the icon to open the camera app and take a photo, which you can then share to other applications.

Additionally, once a Wired or Wireless AutoTest Profile has completed, the floating action button appears and provides the option of opening the camera application to take and attach a picture to the AutoTest result uploaded to Link-Live Cloud Service.
The Flashlight feature can be accessed from the Quick Settings Panel by swiping down twice from the top of the screen.

Back to Title and Contents

Back to Title and Contents

Software Management

This chapter explains how to save and transfer files, reset app and device defaults, update your software, and remotely access your EtherScope nXG.

Tap a link below to skip to a topic:

Managing Files

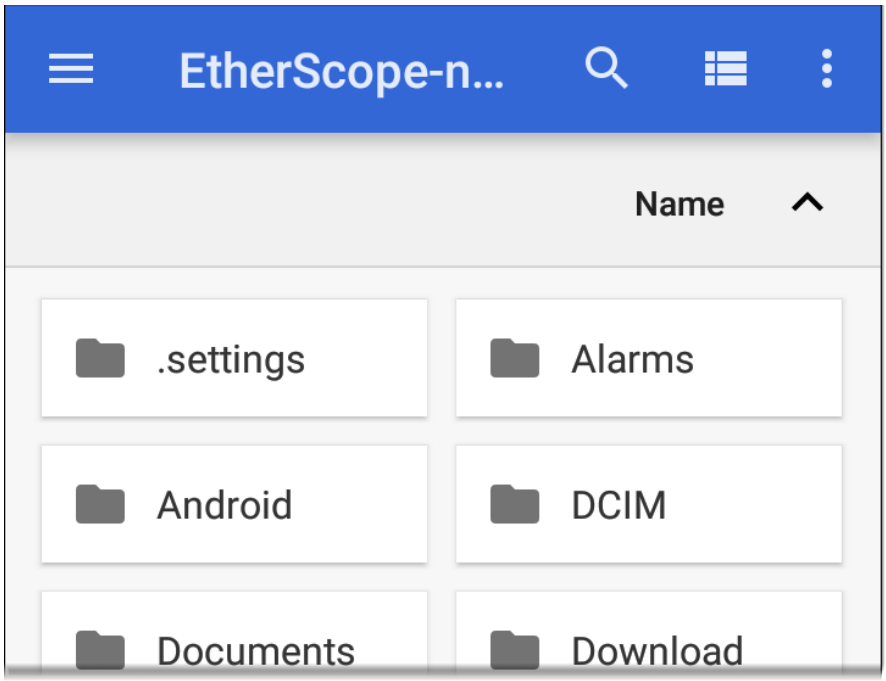
The EtherScope nXG operating system, images, documents, and other files reside in a folder system, where you can copy, move, and paste them between folders or to external storage locations.

See also Sharing.

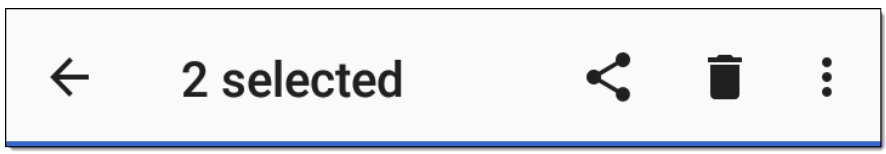
Files Application

The Files app allows you to access the files saved on your EtherScope. Tap the icon at the bottom of the Home Screen (or from the Apps screen) to manage your files.

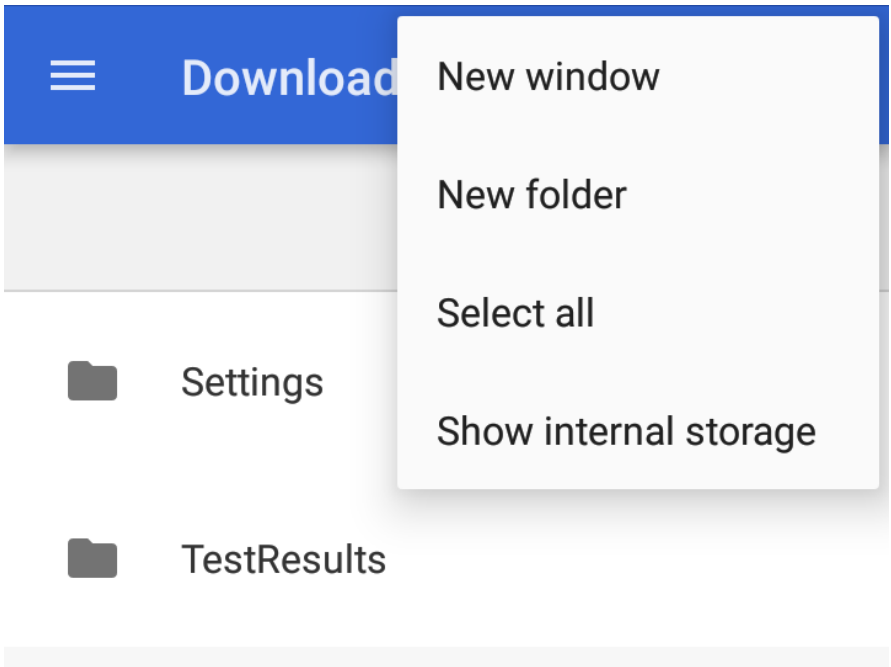
> NOTE: To select the device sub-folders in the Files app as shown below, you may need to open the navigation drawer by swiping from the left side of the screen or by tapping the navigation icon at the top left and then tapping the **EtherScope-nXG** folder.



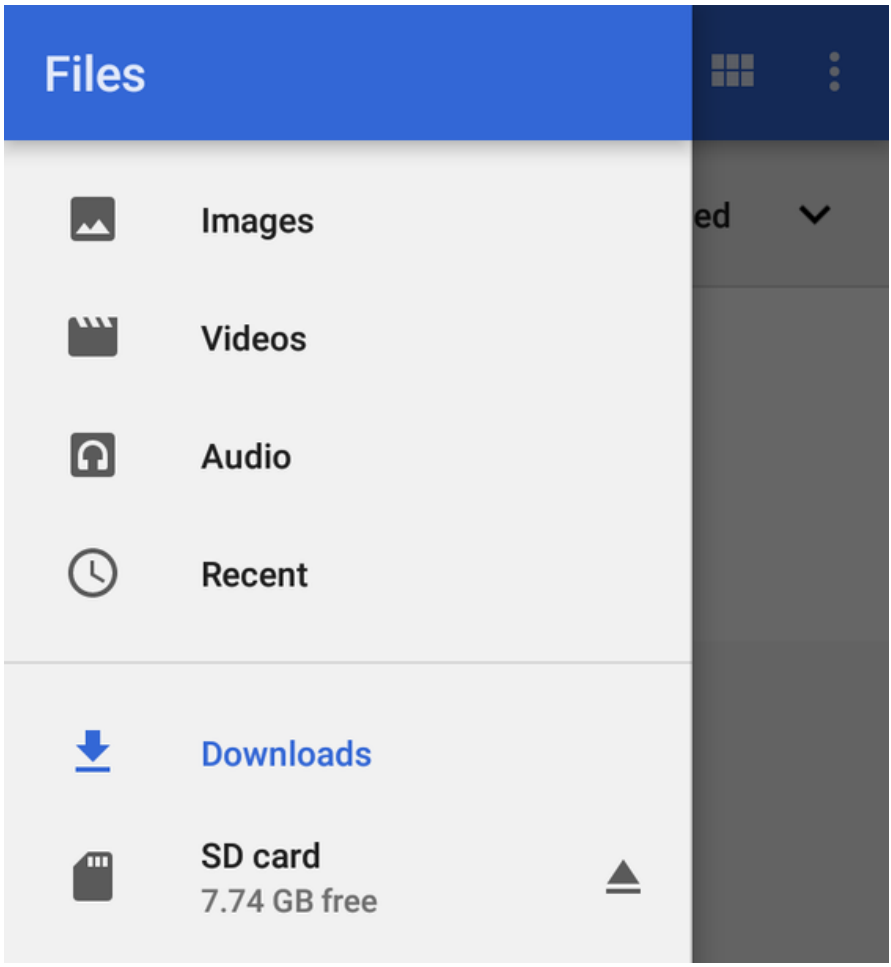
- Tap a folder or file to open it.
- Long press on folders or files to select multiple and to view additional file management operations in the top toolbar, including the Share and Delete buttons.



- Tap the action overflow icon to see even more actions, such as to create a new folder, move a file, delete an item, and to show or hide the main internal storage folder.

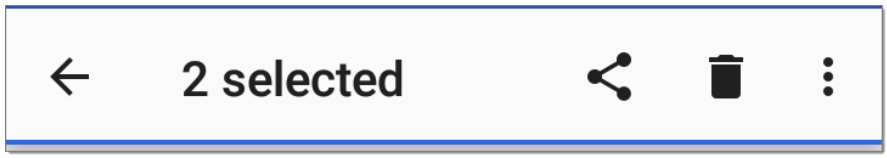


- Open the left-side navigation drawer to easily navigate through the top-level folders and attached storage devices.



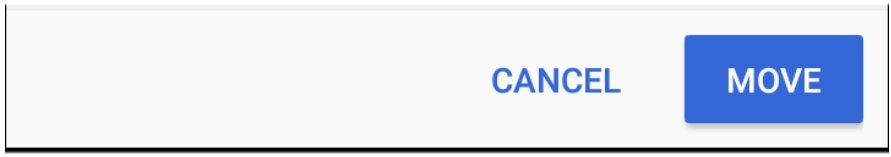
How to Move or Copy a File

1. Long press on a file to select it. You can then select more files as needed by tapping them.



2. Tap the overflow icon ⋮ at the top right.
3. Select **Copy to...** or **Move to...**. Your selected action button appears at the bottom of the

screen.

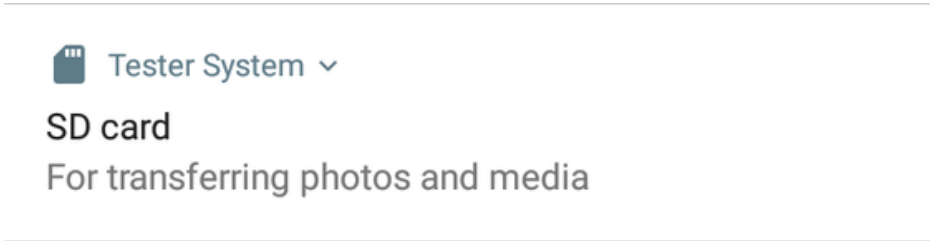


4. Navigate to the folder where you want to move or copy the file.
5. Tap the **Move** or **Copy** button at the bottom of the screen.

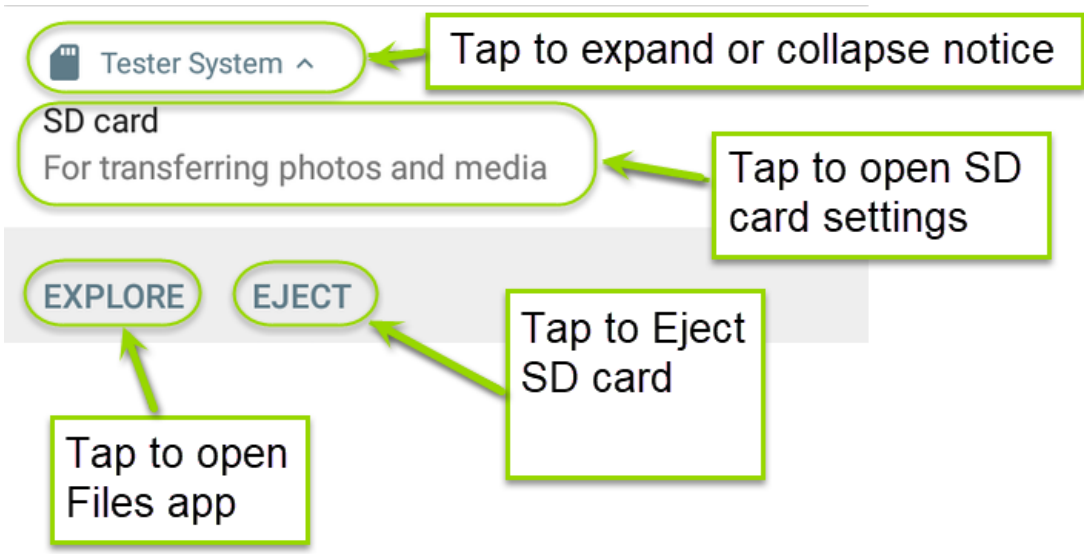
Using a Micro SD Card

To use a Micro SD card for storage, insert it into the Micro SD card slot on the left side of your EtherScope nXG. See Inserting a Micro SD card.

A Micro SD card icon appears in the Status Bar at the top of the screen. Pull down the top Notification Panel to reveal the SD card notification.



Tap the notification title or down arrow to expand the notification and display additional options:



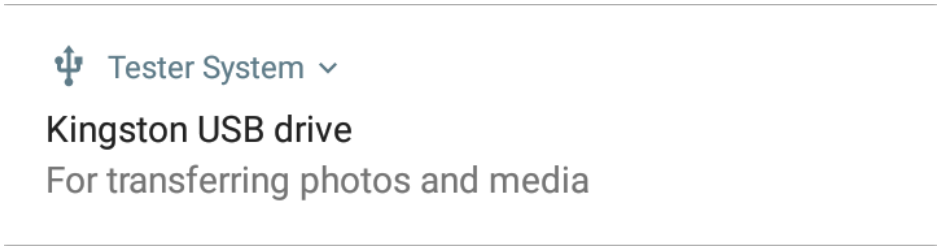
The **SD card** storage location is also available from the Files application.

⚠ **CAUTION:** Use the system **EJECT** function before physically removing your Micro SD card from the USB port to avoid potential corruption of your storage device's file system.

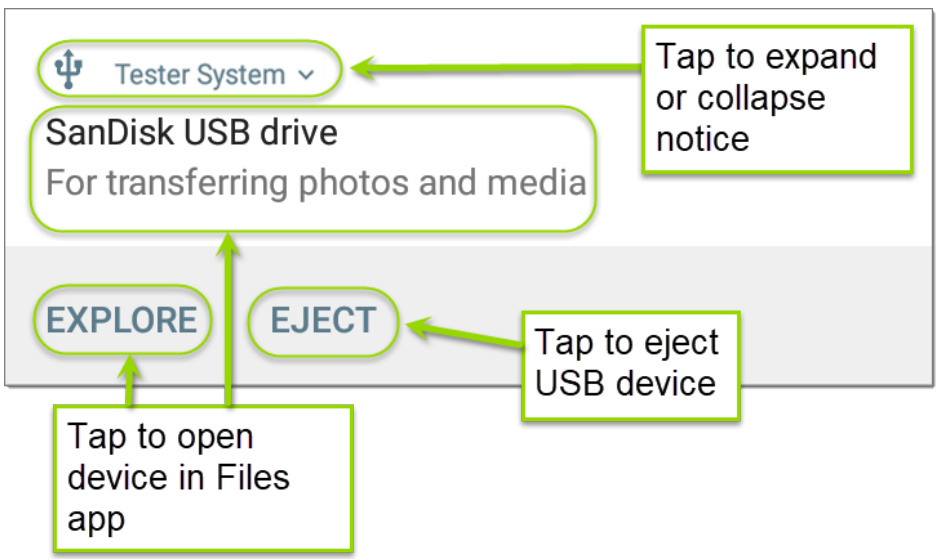
Using a USB Drive

Insert a USB flash drive into the USB port on the top of the EtherScope.

A USB icon appears in the Status Bar at the top of the screen. Pull down the top Notification Panel to reveal the USB drive notification.



Tap the notification title or down arrow to expand the notification and display additional options:



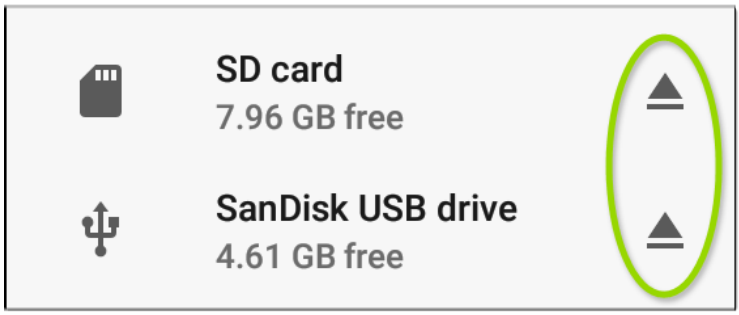
The **USB storage** location is now available from the Files application.

CAUTION: Use the system **EJECT** function before physically removing your USB drive from

the USB port to avoid potential corruption of your storage device's file system.

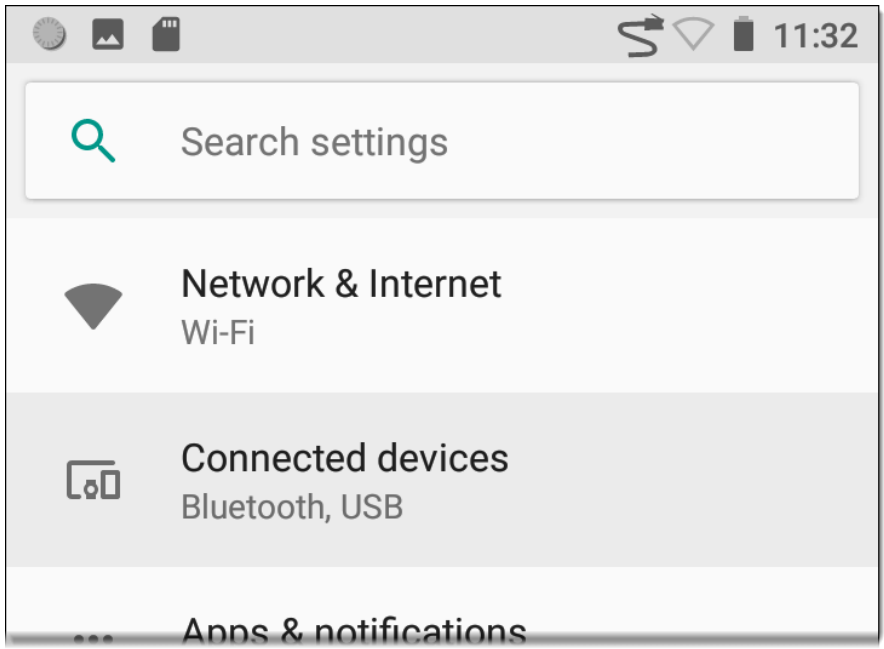
Ejecting Storage Media

You can eject storage media from the expanded system notification (as shown above) in the Notification Panel or from the left-side navigation drawer in the Files app (below).

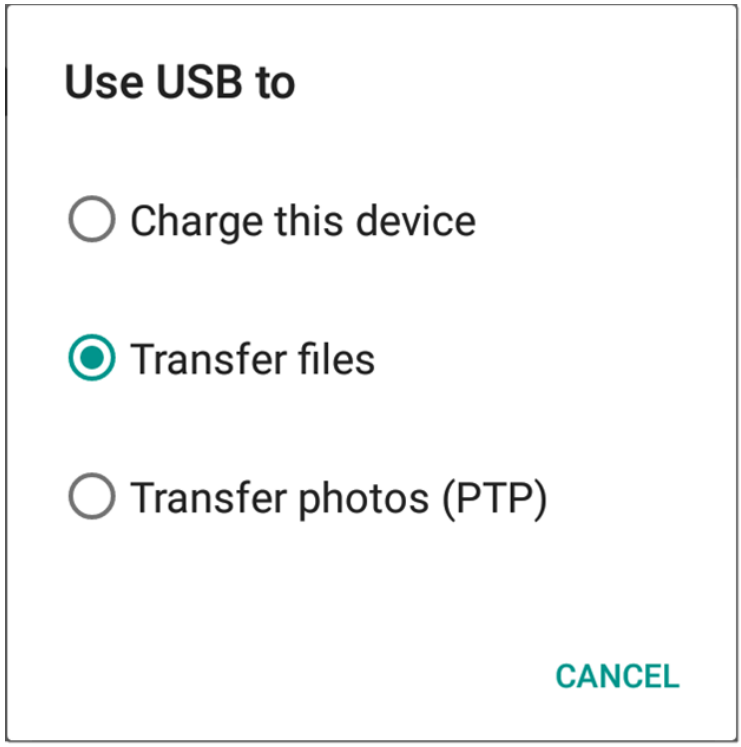


Using a USB Type-C to USB Cable

1. Plug a USB-C cable into the USB-C port on the left side of the EtherScope, and connect to a PC or tablet.
2. On the EtherScope Unit, open the system device settings by tapping the Settings icon at the bottom of the Home screen.
3. Select **Connected devices**.



4. On the Connected devices screen, select **USB**.
5. In the pop-up dialog, tap **Transfer files** to enable file transfer.



NOTE: EtherScope does not charge through a USB cable connected to a PC.

6. On a PC or tablet, navigate to the EtherScope nXG folder, and then move, copy, and paste files to and from the EtherScope nXG's file system.

⚠ **CAUTION:** Use the system **EJECT** function before physically disconnecting the USB cable from your PC or EtherScope to avoid potential corruption of your storage device's file system. See Ejecting Storage Media above.

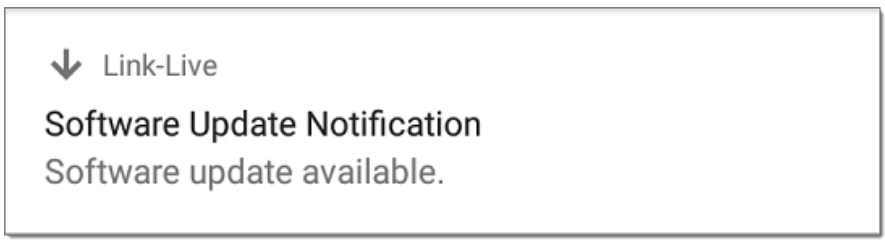
Updating Software

Your EtherScope nXG accesses software updates from the Link-Live Cloud Service "Over-the-Air" (OTA). However, you can also manually download and install updates if you do not want to claim your unit to Link-Live. See Manual Updates below.

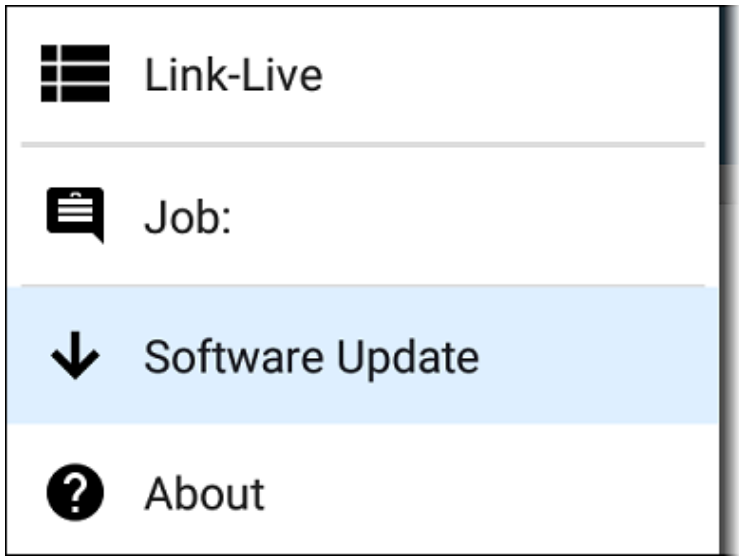
Over-the-Air Updates

For an OTA update, you must create an account and "claim" your EtherScope nXG unit at Link-Live.com. Then your EtherScope can find and download software updates. See Getting Started in Link-Live.

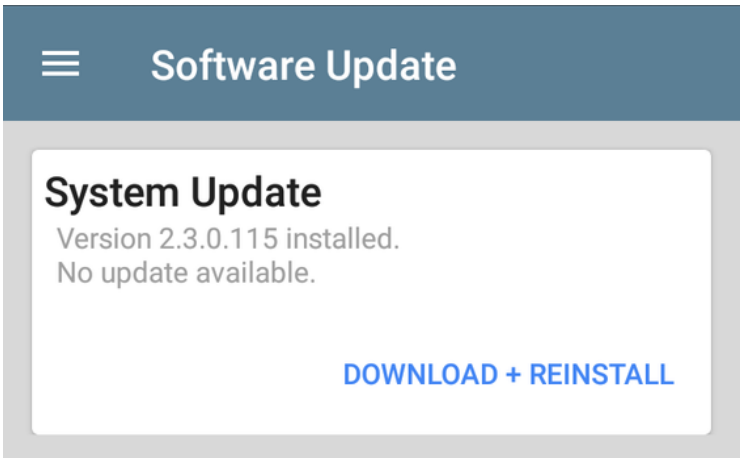
The first time you claim your EtherScope nXG to Link-Live, a software update may be available. If so, an update icon appears in the Status Bar. Slide down the Top Notification Panel, and then select the notification to update your unit.



1. To check for available software updates at any time, open the Link-Live App from the Home screen.
2. In the Link-Live App, tap the menu icon or swipe right to open the left-side navigation drawer.



3. Tap **Software Update**.
   The Software Update screen opens and displays the version number of any available updates.



4. Tap **Download + Install** (or **Download + Reinstall**) to update the operating system and NetAlly applications. The update downloads and installs automatically. When finished, the unit restarts.
5. After updating, check the Software Update screen again in case another update is still required.

Manual Updates

You can acquire update files by contacting NetAlly's Technical Support at NetAlly.-com/Support or by downloading them from Link-Live.com as follows:

1. Log in to the Link-Live web site.
2. Open the left-side navigation drawer by clicking the menu icon  , and then select **Support > Software Downloads**.
3. Locate and select the update file for your unit (esnxg-ota-user.zip).
4. Save the update file to a PC.

Updating the System Software

Reference Buttons and Ports if needed.

1. From your PC, copy the .zip file to a Micro SD card, and then insert the card into your EtherScope.
2. Power off your EtherScope unit.
3. Press and hold the **Volume Up** button, and then press the **Power** button. Continue to hold the **Volume Up** button until the Recovery screen appears. (You can release the **Volume Up** button a few seconds after this screen appears.)
4. In Recovery Mode, use the volume buttons to highlight **apply update from SD card**,

and then press the **Power** button to confirm the selection.

5. Use the volume buttons to highlight the correct update file on the Micro SD card, and then press the **Power** button to confirm. The EtherScope opens the Updater, installs the update, and then restarts with the update installed. This process can take 5 to 10 minutes. When complete, the message 'Install from Micro SD card completed with status 0.' should show on the install line.
6. Use the volume keys and **Power** button to select **reboot system now**. Your unit should boot normally.

Back to Title and Contents

Remote Access

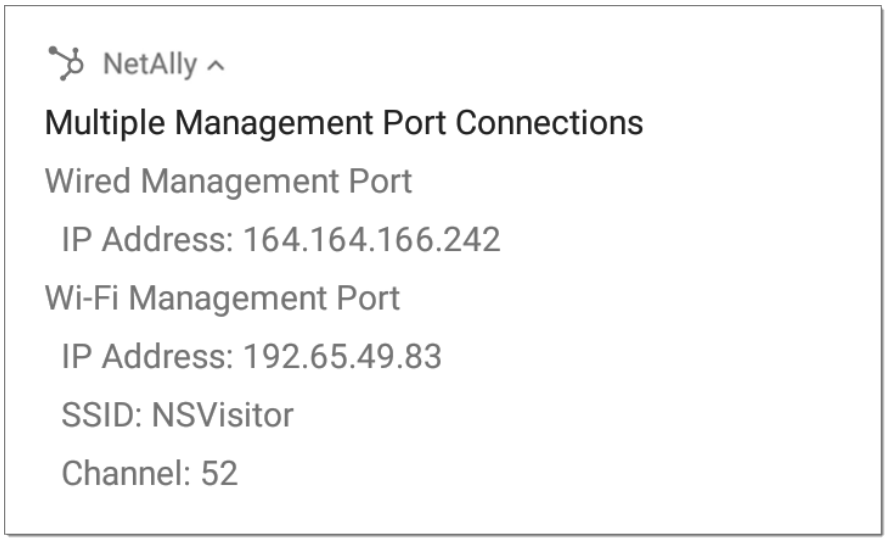
EtherScope supports remote access and control using either a standalone VNC client or the Link-Live Remote feature, which uses a VNC client through the Link-Live website.

> NOTE: The Link-Live Remote feature is only available to customers with an active **AllyCare** subscription. Your EtherScope must be claimed. See NetAlly.com/Support for more information.

You can establish remote connections using the Wired or Wi-Fi Test Ports. However, the Management Ports provide more stable links for remote control because the test ports may disconnect and reconnect frequently.

See Test and Management Ports.

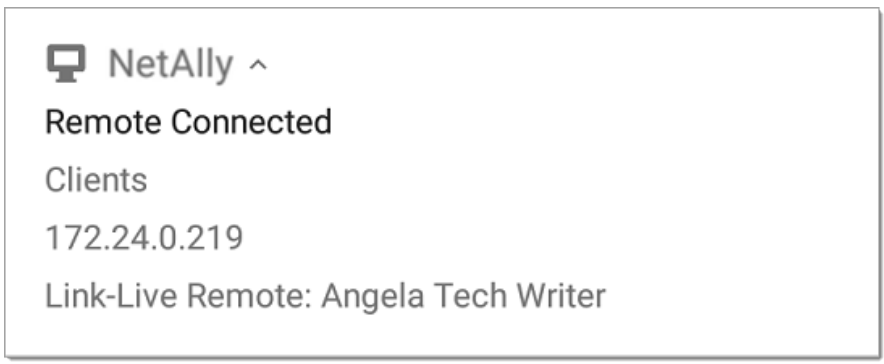
The top notifications are the quickest way to find assigned IP addresses for your EtherScope ports. Swipe down from the Status Bar to view them.



For a wired management connection, you must have an Ethernet cable with an active network connection plugged into the left-side RJ-45 Management Port.

For a Wi-Fi Management Port connection, you must have the main System Wi-Fi settings configured to connect to a wireless network.

When a remote session is active, the remote icon appears in the top Status bar, along with a notification.



Using VNC

Remotely access the EtherScope nXG using a peer-to-peer VNC client installed on a PC or other machine.

See **General Settings > VNC** to enable and configure VNC connections.

To connect to EtherScope using a VNC client:

1. Get the IP address of a connected port (preferably a management port) by swiping down from the Status Bar at the top of the screen to view the notification panel.
2. Provide the wired or Wi-Fi Test or Management Port's IP address to your chosen VNC client application.
3. Connect using your VNC client.
4. If needed, enter the password that is set in the VNC settings.

Using Link-Live Remote

The Link-Live Remote feature uses end-to-end encryption, allowing secure remote control of your EtherScope.

On your EtherScope, go to General Settings > Link-Live Remote to ensure the feature is enabled.

NOTE: If a Password is enabled in the VNC General Settings, you must also enter the same password to access the Remote feature in Link-Live.

1. If you have AllyCare, sign in to Link-Live.com to access the Link-Live Remote feature. Your EtherScope must be claimed.
2. Navigate to the **Units** page at Link-Live.com.
3. Select the EtherScope you want to remote control from the list of claimed units.
4. Click or tap the **REMOTE** icon at the top right of the page to open an embedded window containing the EtherScope interface.
5. If necessary, at the top of the window, enter the Password set in General Settings **> Management > VNC** on the EtherScope unit.

To use the Link-Live website while your remote session is active, you must open a new Link-Live tab or window.

Back to Title and Contents

Managing NetAlly App Settings

This topic explains how to reset, load, save, import, and export the test settings for individual NetAlly testing apps, such as AutoTest, Discovery, and Performance.

For instructions on restoring factory defaults to the entire test unit, see Restoring EtherScope nXG Factory Defaults.

Resetting Testing App Defaults

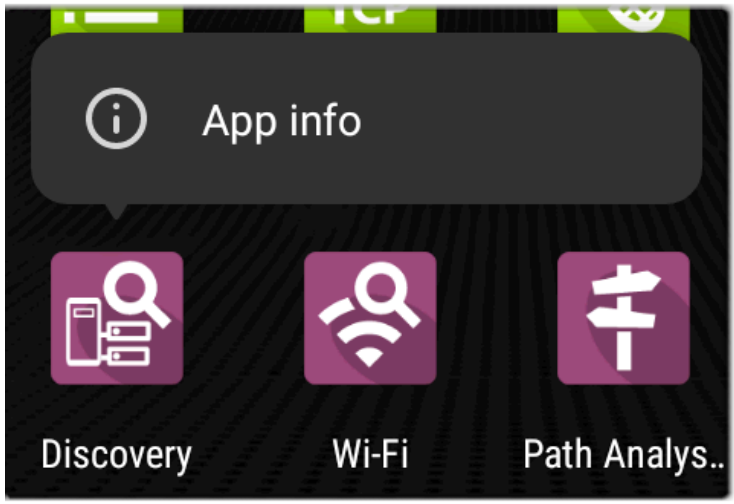
After you adjust settings in the NetAlly apps, you may need to reset an app's settings to the defaults. The following process resets all app-specific settings to the factory defaults.

> ⚠ **CAUTION:** This operation deletes all saved settings, including testing profiles and other application data.

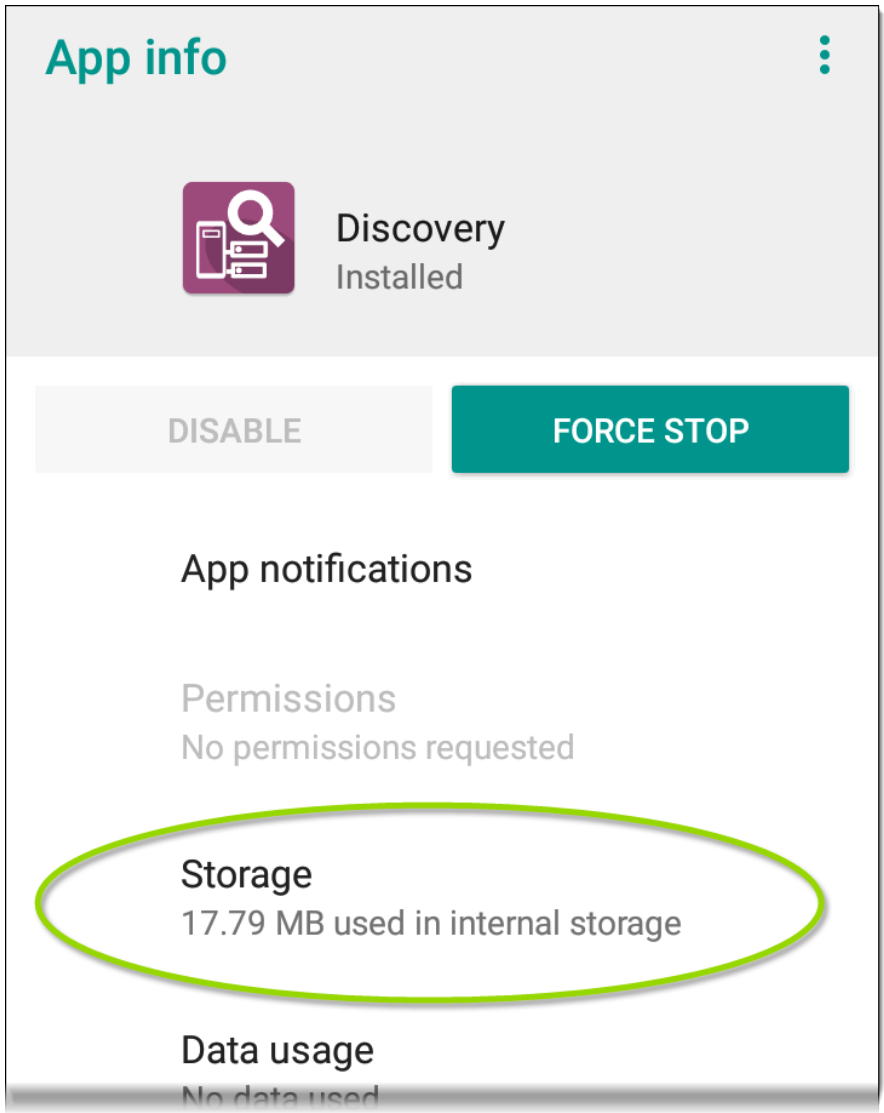
The Discovery app is used as an example in the following steps:

1. Access the **App Info** screen by long pressing (touch and hold) on an app's icon on the

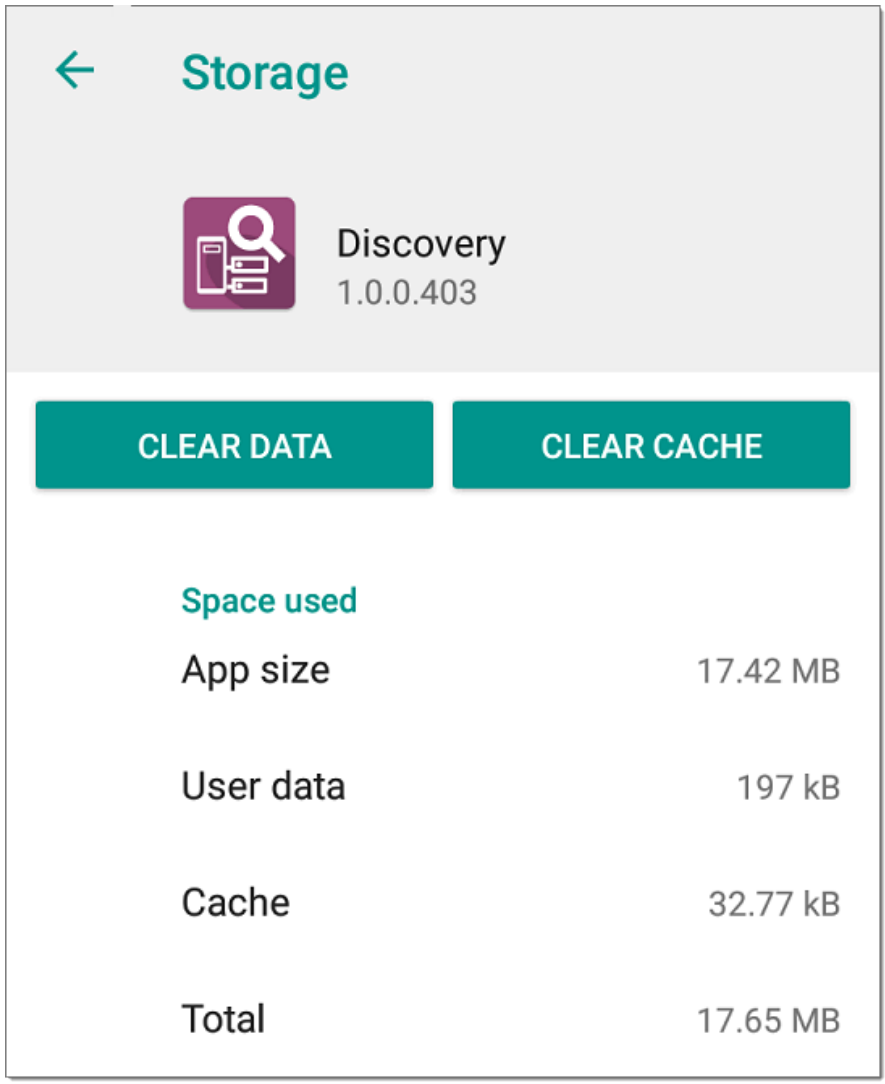
Home or Apps screen.



2. Tap **App info**.



3. On the App info screen, select **Storage**. (You can also access the App Storage screen from Device Settings > **Storage > Internal shared storage > Other apps**.)
4. On the Storage screen for the app you selected, tap **CLEAR DATA**.



5. When a dialog prompts you to delete the data, tap **OK**.

All of the app's settings are reset to factory defaults.

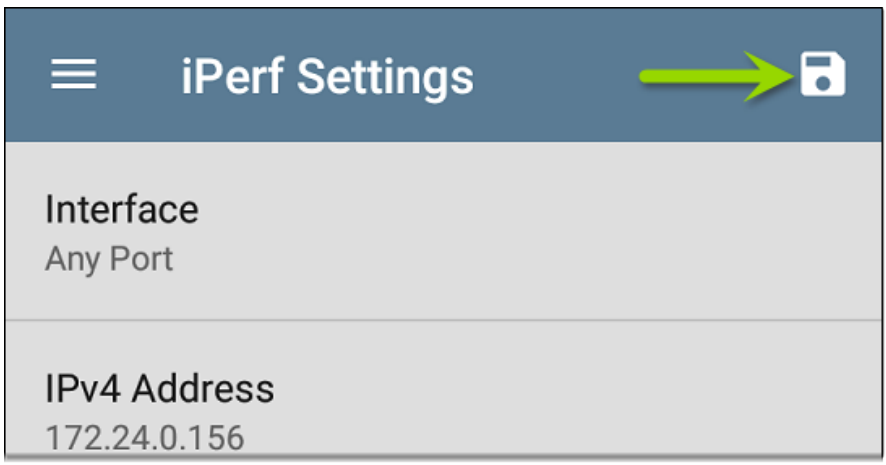
Saving App Settings and Configurations

Many of the NetAlly testing applications allow you to save and reload configured settings by selecting the save button that appears at the top right within the app's main screen.

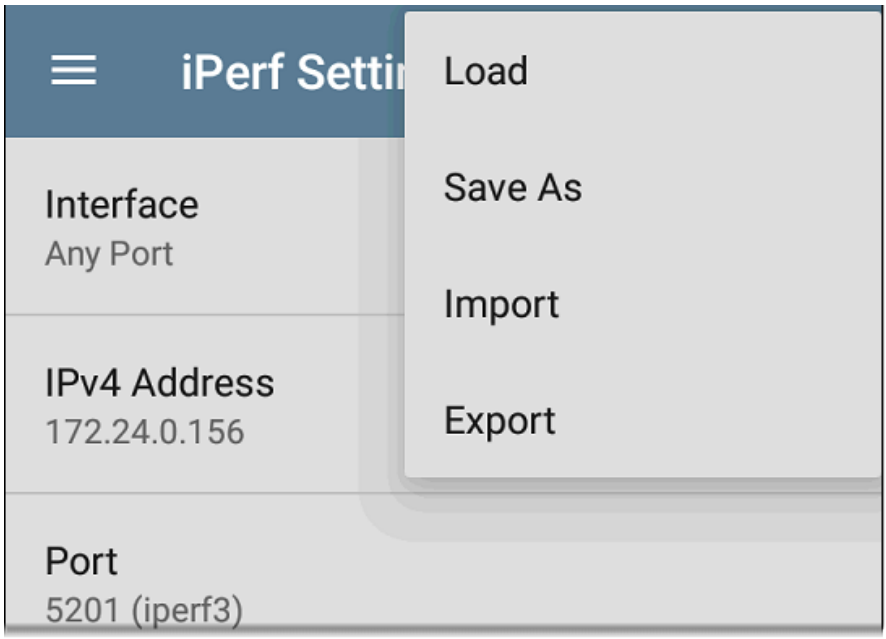
The following apps enable you to save and load settings configurations:

- AutoTest, including Profile Groups
- Discovery
- Discovery Problem Settings
- Performance
- iPerf
- Spectrum

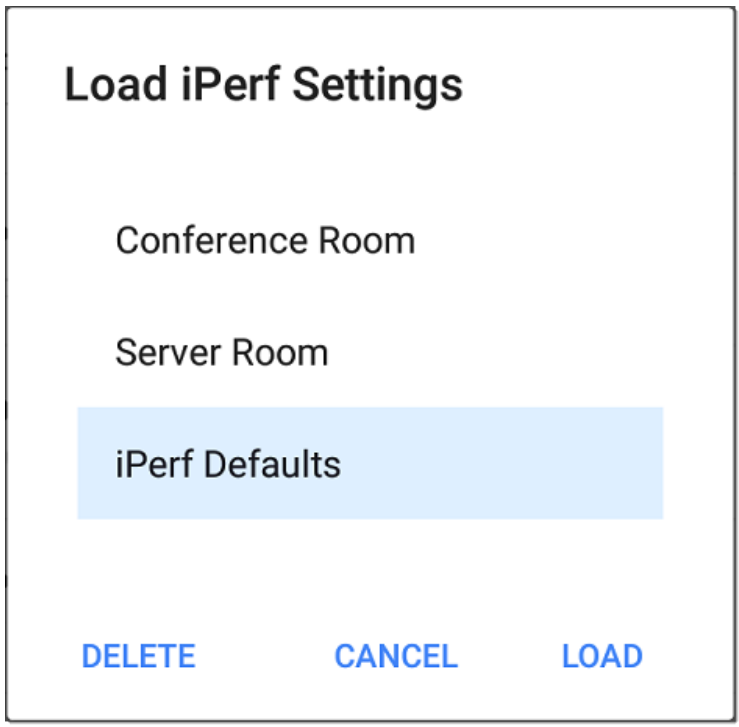
The iPerf app is shown below as an example.



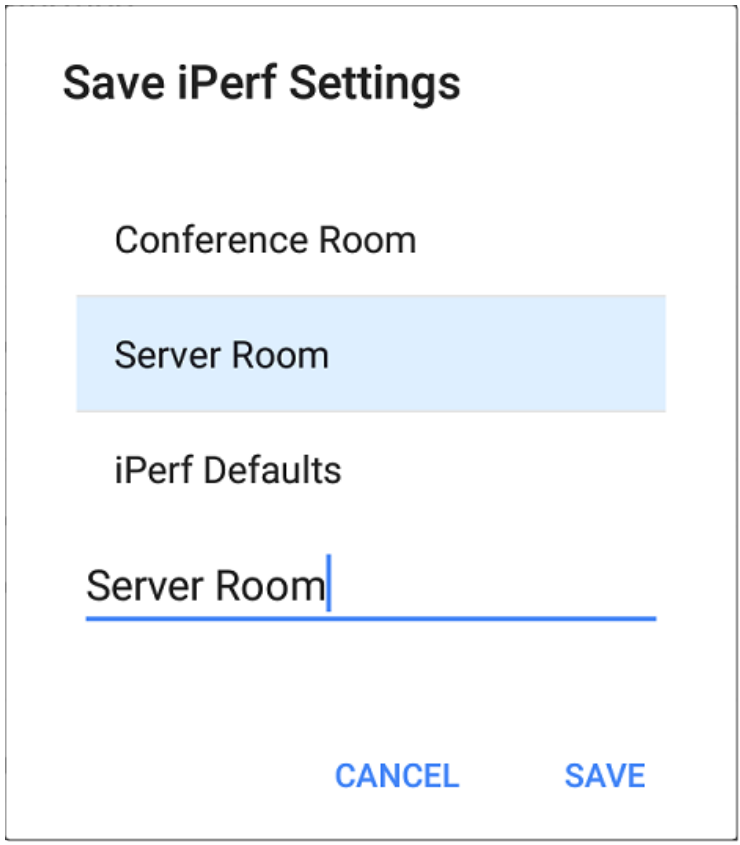
The following options display in a drop-down menu:



- **Load**: Open a previously saved and named settings configuration.



- **Save As**: Save the current settings with an existing name, or enter a new custom name.



- **Import**: Import a previously exported settings file.
- **Export**: Create an export file of the current settings, and save it to internal or connected external storage.
- **Export To Link-Live**: Export the current settings directly to the Link-Live cloud service.

See Exporting and Importing App Settings (below) for more details.

Saving a Default Test App Configuration

If you find you are frequently resetting app defaults, you can save  the default configuration of settings for later use within the NetAlly testing apps. Loading a saved default configuration within an app allows you to access the default settings without deleting other configurations. This strategy can be most useful for Discovery Settings and Problem Settings.

1. Go to an app's settings  screen.
2. With all settings set to the defaults, tap the save button  and **Save As**.
3. Save a default configuration with an obvious name like "Default Profiles" or "Discovery Defaults."
4. Do not change the settings in your default configuration to non-defaults without also saving a new, custom-named configuration.

Importing and Exporting Settings

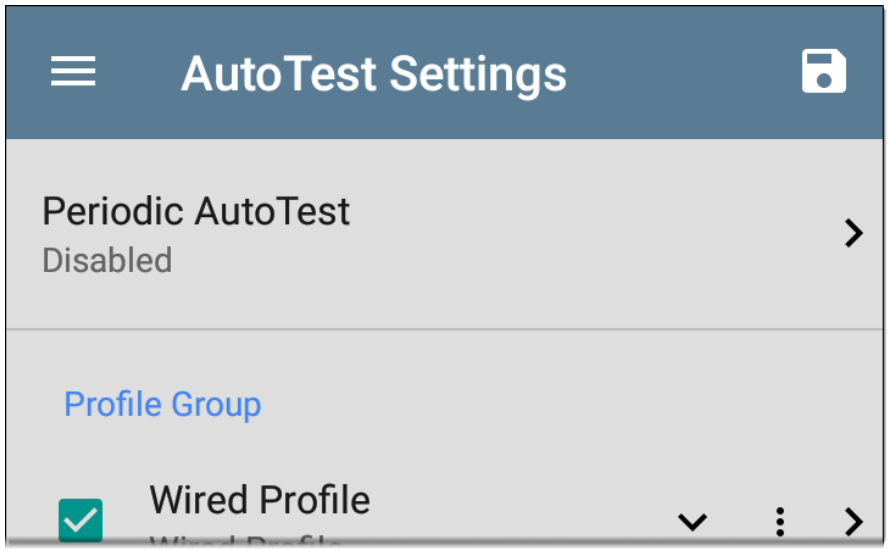
EtherScope nXG provides functionality for importing and exporting saved test app settings for transfer to additional units or exporting to Link-Live. USB and other devices

> NOTE: You can import and export settings only between the same kind of NetAlly products. For example, both units must be EtherScope nXGs for a transfer to work.

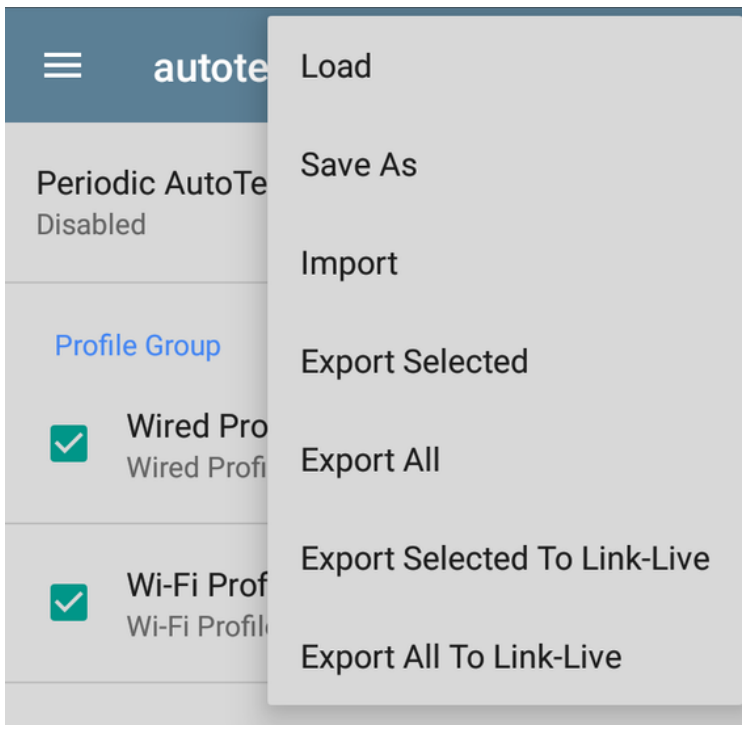
The following apps enable you to import and export settings and configurations:

- AutoTest Settings, including Profile Groups
- Discovery Settings
- Discovery > Problem Settings
- Performance Settings
- iPerf Settings

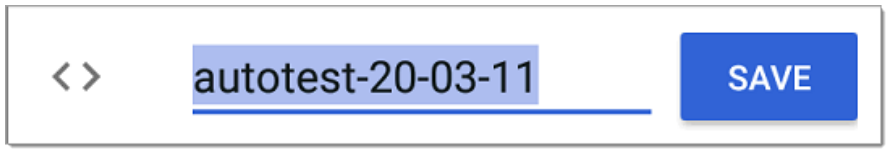
The AutoTest Settings are shown as an example in the images below.



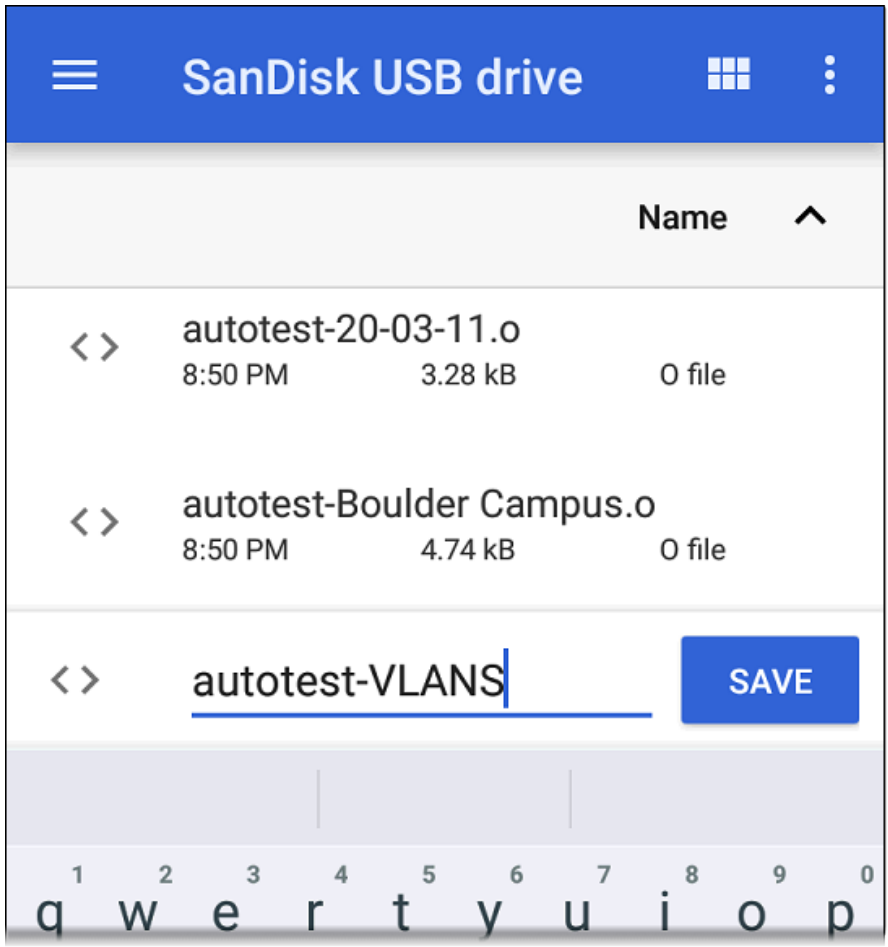
- Tap the save button to import new app settings or export the *currently active and selected* app settings.



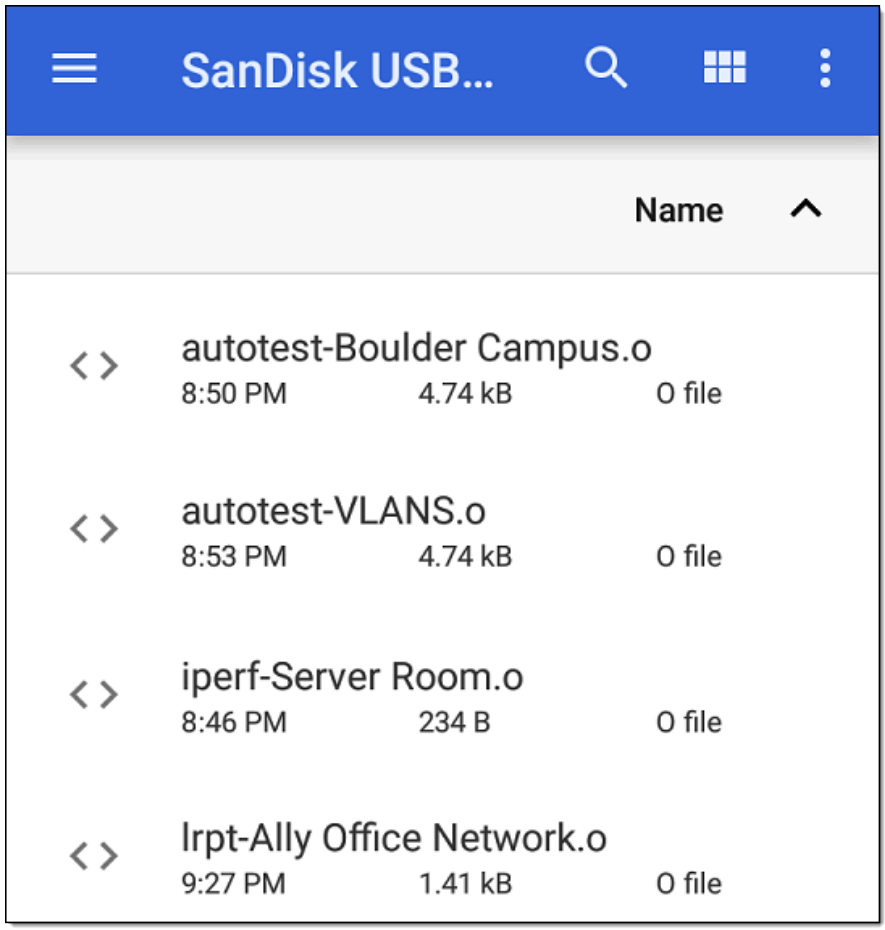
- Selected (checked) items in shared lists of configurations are the only ones exported when you choose **Export Selected**. This can include any checked items in submenus (such as AutoTest Test Targets or Community Strings in Discovery Settings). You can also select **Export All** to export all selected and unselected items.
- Unsaved configurations without a custom name are auto-named with the app name and date:



- Saved configurations are auto-named with the app name and custom settings name:



- You can rename the export file as needed.
- Settings can be saved to any connected external or internal storage. See Managing Files for instructions on accessing folders and moving files.
- Settings are saved with the **.o** file extension.



- Selecting **Import** from an app opens the Files app, where you can navigate to and select the .o file you want to import.
- Imported settings configurations overwrite existing saved configurations with the same name that are already in the app.

Transferring AutoTest Settings to Other Devices Using Link-Live

You can use the Link-Live cloud service to transfer AutoTest settings with other EtherScope

nXG devices.

- Do some setup before you begin.
- Export the settings file(s) that you want to share to Link-Live.
- Use Link-Live to select other devices to which you want to transfer the settings.
- Use each selected unit to import the settings.

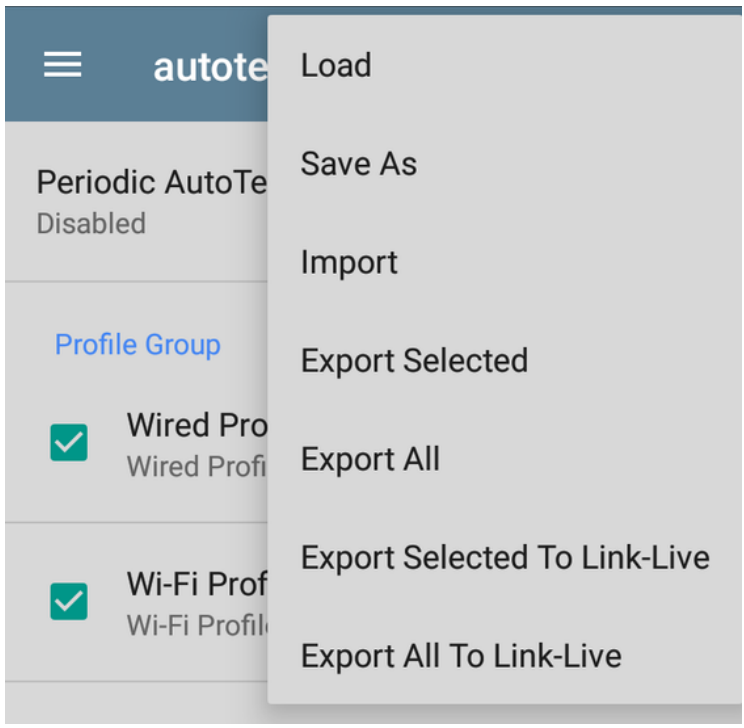
Before You Begin

- Make sure that you have access to the following:
  a. The device from which you will get the settings
  b. A PC-based browser
  c. The devices to which you will transfer the settings file
- Make sure that you have claimed and updated the software for all EtherScope nXG devices to which you want to transfer the settings. (You can use the Link-Live app or web site to do the claiming. See "Claiming the Unit" on page 755 for instructions.)

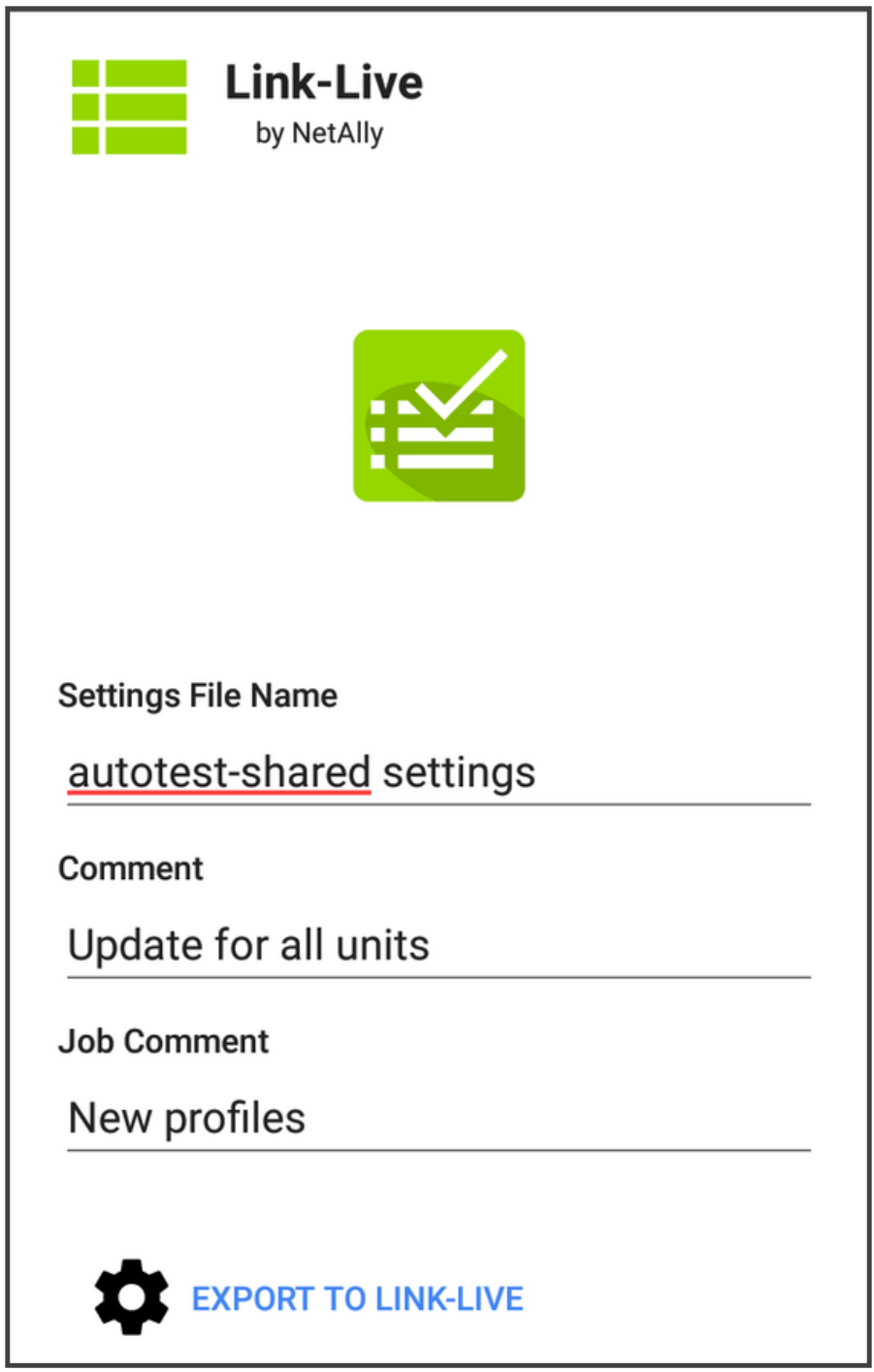
Export the Settings File(s)

This procedure is done on the device from which you are transferring the settings.

1. In the AutoTest app main page, tap the settings icon in the top right. This opens the list of profiles.
2. If you plan to export only selected profiles, use the checkboxes to choose those profiles from the list.
3. Tap on the save icon in the top right to display the save menu options.



4. Tap **Export Selected To Link-Live** (if you selected profiles) or **Export All To Link-Live** on the menu. This opens the save screen for Link-Live.



5. (Optional) Edit the file name, add a comment, or add a job comment on the screen.
6. Tap **Export To Link-Live**. This uploads the file to Link-Live.

Use Link-Live to Select Other Devices

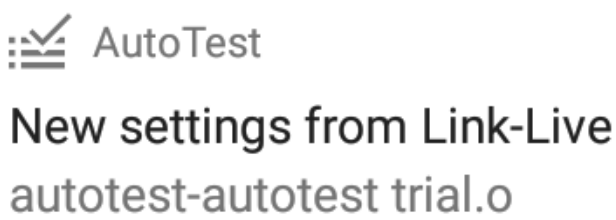
This procedure is best performed on a PC-based browser.

1. Use a PC-based browser to log in to the Link-Live web site.
2. Click the main menu icon  .
3. Click on **Settings** to open the settings menu.
4. Select **EtherScope nXG** to list the .o settings files available for your devices.
5. Select the settings file you want to transfer.
6. Follow the screen instructions to transfer the file to specific units or to all units that you have claimed.

Use Each Selected Unit to Import the Settings

This procedure is performed on the device to which you want to apply the settings.

1. Wait for up to 30 seconds after the file was pushed from Link-Live.
2. Swipe (touch and drag) downwards from the Status Bar at the very top of the home screen to display the Notification Panel.
3. Locate the notification that says there are new AutoTest settings from Link-Live and lists the profile name.



4. Tap on that notification to open the AutoTest application.
5. Tap on the save icon in the top right.
6. Tap on **Import** and navigate to Downloads.

7. Select the downloaded .o file to apply the new profile settings.

Importing and Exporting Settings for All Apps

Your EtherScope nXG supports the importing or exporting of settings for *all* applications that allow import/export of settings.

> NOTE: You can import and export settings only between the same kind of NetAlly products. For example, both units must be EtherScope nXGs for a transfer to work.

To perform a group export or import:

1. Open the About Screen by tapping the navigation menu icon  in any NetAlly application and then tapping **About**.
2. Tap the action overflow icon  to display the export/import menu.
3. To import settings:

a. Tap **Import EtherScope nXG Settings** . This opens the Files app to the default Settings folder.

b. (Optional) Use the Files app to navigate to a different folder.

c. Select the .nas settings file you want to import.

d. Tap **Yes** at the prompt to import the settings for all apps at the next system restart.

4. To export settings:

a. Tap **Export EtherScope nXG Settings**. This opens a dialog with a system-generated file name and the default Save To folder.

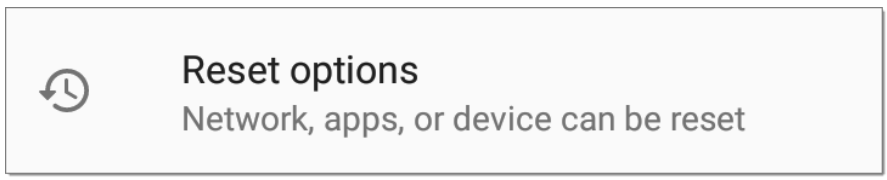
b. (Optional) Tap the Save To folder or tap Save As to open the Files app to select a different folder.

c. Tap **Save** to save the settings file.

Resetting EtherScope nXG Factory Defaults

⚠ **CAUTION:** Resetting your device to factory defaults can delete *all* test results, user-installed applications, testing app settings, and saved files.

1. Make sure to back up any files you wish to keep before resetting.
2. Open the system Device Settings by tapping the Settings icon at the bottom of the Home Screen.
3. On the Settings screen, scroll down to and tap on the **System** section.
4. On the System screen, tap **Reset options**.



5. On the Reset options screen, select an option based on the defaults you want to reset. Your EtherScope displays a list of the items that will be reset based on the option

and a confirmation button.

Reset Wi-Fi, mobile & Bluetooth: resets all network settings for Wi-Fi (test and management), mobile data, and Bluetooth.

Reset app preferences: resets any preferences or settings for applications, although app data is not lost.

Erase all data (factory reset):
⚠ **CAUTION:** Erases ***all*** user data from your tester's internal storage, including: system and app data and settings; downloaded apps; test profiles; credentials; packet information; and screen captures.

6. Tap the confirmation button to begin the reset.
7. Your unit may ask you to confirm a final time before resetting. If so, tap the final confirmation button to reset your EtherScope's defaults. The unit then restarts with the factory default settings you selected.
8. Data on removable drives is not included in the reset. To be thorough, you may also

want to use the Files application to delete any application settings, preferences, or other data that you have saved on an attached Micro SD card or a USB thumb drive. (Do not delete your backup files.)

EtherScope nXG Testing Applications

This section of the User Guide describes the NetAlly-developed network testing apps. Each app is specially designed for fast analysis and intuitive operation to enhance and simplify your network tasks.

Open the testing apps by selecting their icons from the Home screen or the Apps screen.

AutoTest App and Profiles

AutoTest is the most comprehensive NetAlly testing application on EtherScope nXG. You can quickly run a variety of test types and save their configurations and network credentials for access whenever you need them. The app is fully customizable with test "Profiles" for **Wired** and **Wi-Fi**, wireless **Air Quality** network connections, as well as individual **Test Targets**

AutoTest establishes the **Wired and Wi-Fi Test Port connections** used by other testing apps, like Ping/TCP, Capture, and Performance.

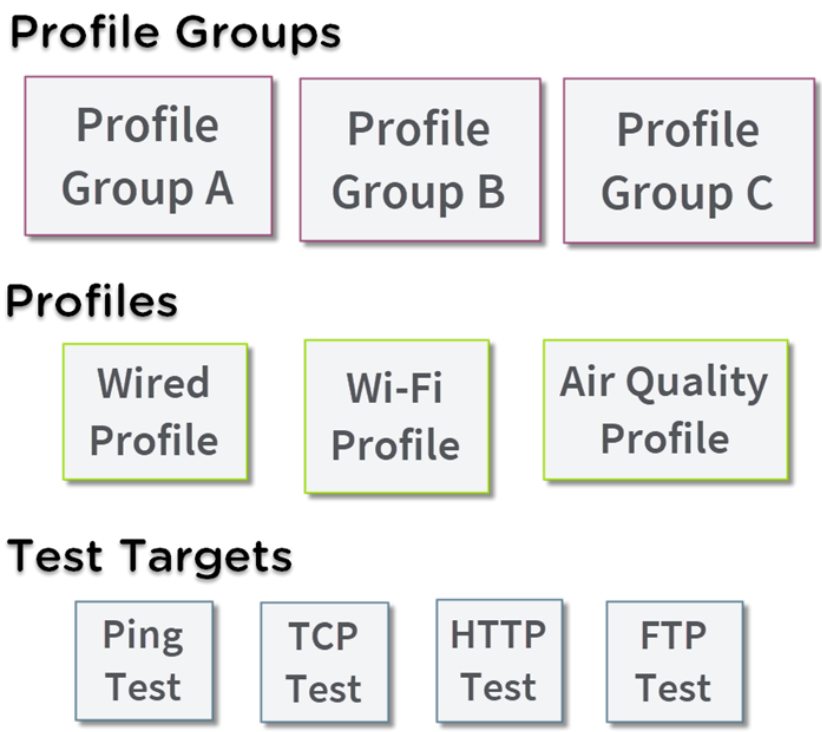
AutoTest results are automatically uploaded to **Link-Live Cloud Service** after you claim your EtherScope.

AutoTest Chapter Contents

This chapter describes AutoTest Profiles, screens, settings, and test results.

AutoTest Overview

AutoTest consists of three distinct testing levels: **Test Targets**, **Profiles**, and **Profile Groups**. You can create as many Profile Groups, Profiles, and Test Targets as you need.



At the bottom level is a set of individual **Test Targets** that connect to network services, such as a web app or FTP site. A Test Target defines parameters including type, target URL/IP address, port number, and Pass/Fail thresholds. More complex tests, like HTTP, allow further Pass/Fail criteria, such as strings that must or must not be contained in the HTTP body.

A Test Target can be added to and used in any number of **Profiles**.

A **Profile** contains a series of individual network tests. There are three different Profile types: Wired, Wi-Fi, and Air Quality. The Wired and Wi-Fi Profiles include connection tests and credentials for a Wi-Fi network or Wired VLAN. Air Quality is a passive scan of your wireless environment. Profiles provide an automated and consistent way to verify a network from layer 1 through layer 7.

A Profile can be added to and used in any number of **Profile Groups**.

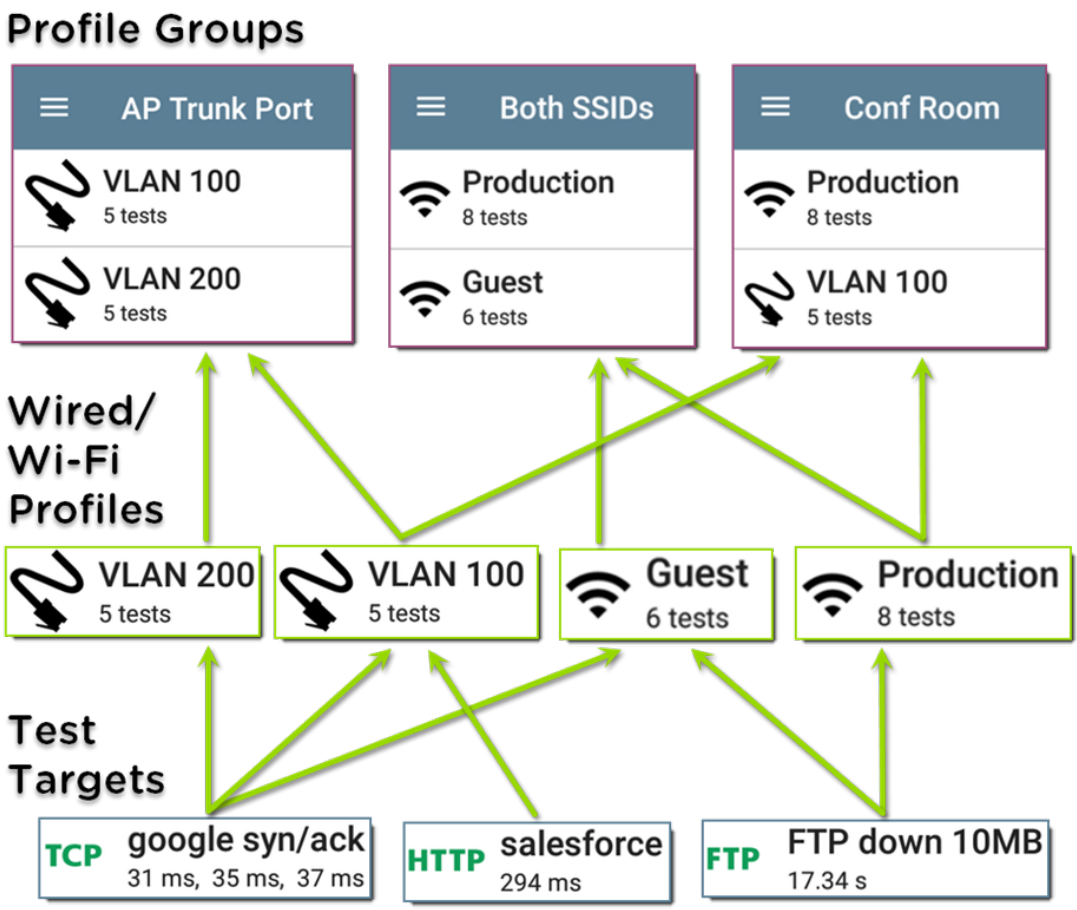
A **Profile Group** is a custom-named collection of Profiles. Profile Groups are designed to allow further automation for testing multiple networks or network elements with a single tap of the START button.

A Test Target can be in any number of Profiles, and a Profile can be in any number of Profile Groups.

For example, you can:

- Test multiple Wired VLANs on a trunk port.
- Test multiple Wi-Fi SSIDs from a single location.
- Test both wired and Wi-Fi access from a conference room.

The graphic below shows each of these scenarios.



Back to Title and Contents

Managing Profiles and Profile Groups

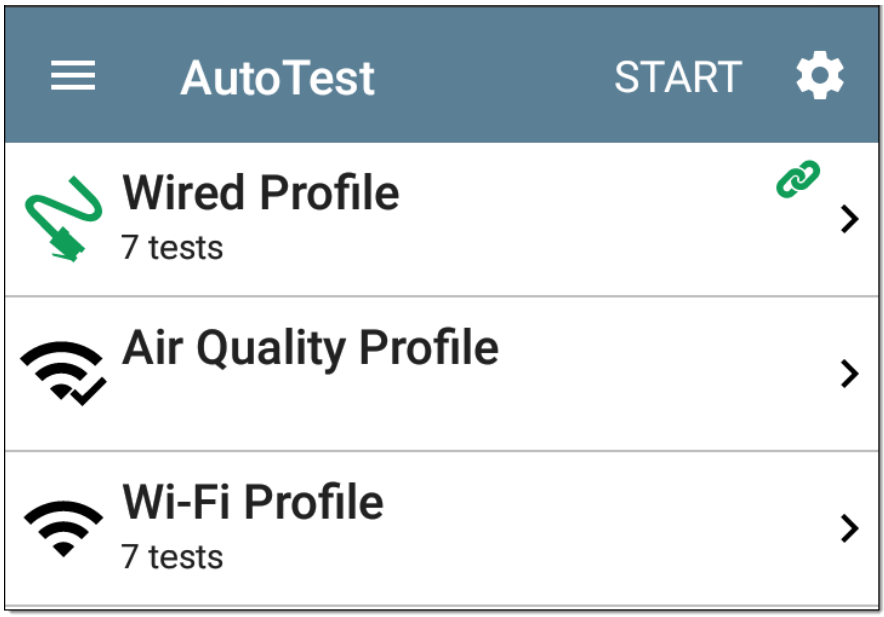
Profiles are a series, or suite, of tests designed to analyze the different characteristics of your networks. The EtherScope nXG AutoTest app features three types of test profiles:

Wired Profiles test copper and fiber connections.
Wi-Fi Profiles test wireless connections.

Air Quality Profiles measure channel utilization and interference.

Factory Default Profiles

The EtherScope begins with a default version of the AutoTest profile types, which you can customize, delete, or replace for your purposes.



To customize each Profile with the required network settings and a custom name, tap the Profile name *first*, and then select the settings icon.

NOTE: Tapping the settings icon on the main AutoTest screen (shown above) opens the AutoTest Settings and Profile Group screen, not the individual Profile settings.

- The default **Wired Profile** runs automatically and establishes a wired link as soon as your unit is powered on and an active Ethernet connection is available on the top RJ-45 port.

  NOTE: The default Wired Profile does not run automatically over a fiber link. You must tap

START in AutoTest to run a Wired Profile on a fiber connection.

The default **Air Quality Profile** runs when you tap **START** on the main AutoTest screen or the Air Quality screen.

For the default **Wi-Fi Profile** to run successfully, you must select an SSID and enter security credentials before the EtherScope can connect to a network.

See Wi-Fi Profile Connection Settings.

Adding New Profiles

To add new test profiles to the current AutoTest, tap the floating action button (FAB) on the AutoTest screen.

The profile's configuration screen appears after you select the type of profile you want to add. See the topic for each profile type for a description of its settings.

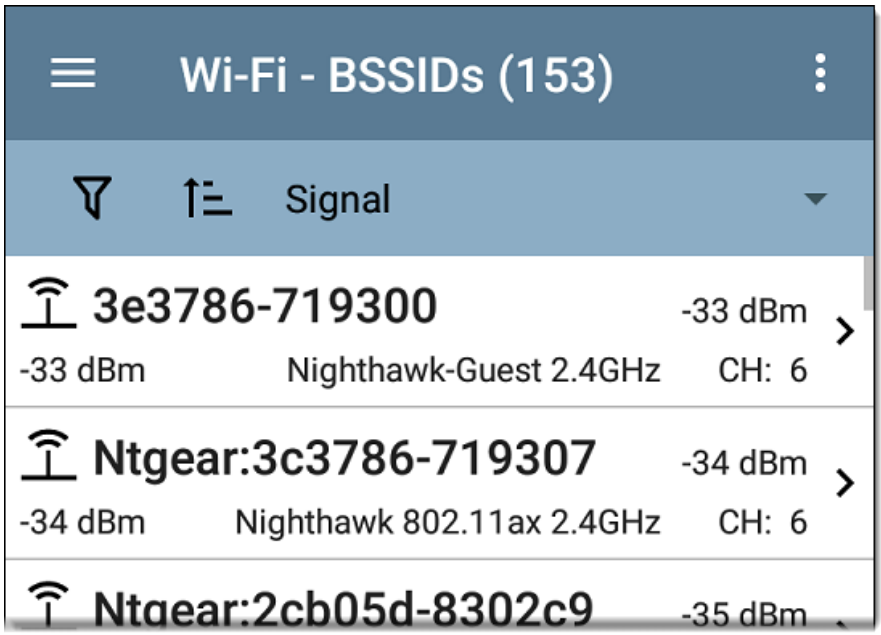
After you configure the profile settings, tap the back button at the bottom of the screen to open and run the new test profile.

Creating a Wi-Fi Profile from the Wi-Fi Analysis App

You can also create an AutoTest Wi-Fi Profile from the Wi-Fi Analysis app's SSID or BSSID Details screen. This is a quick and easy way to add a Profile to connect to a Wi-Fi network in your vicinity.

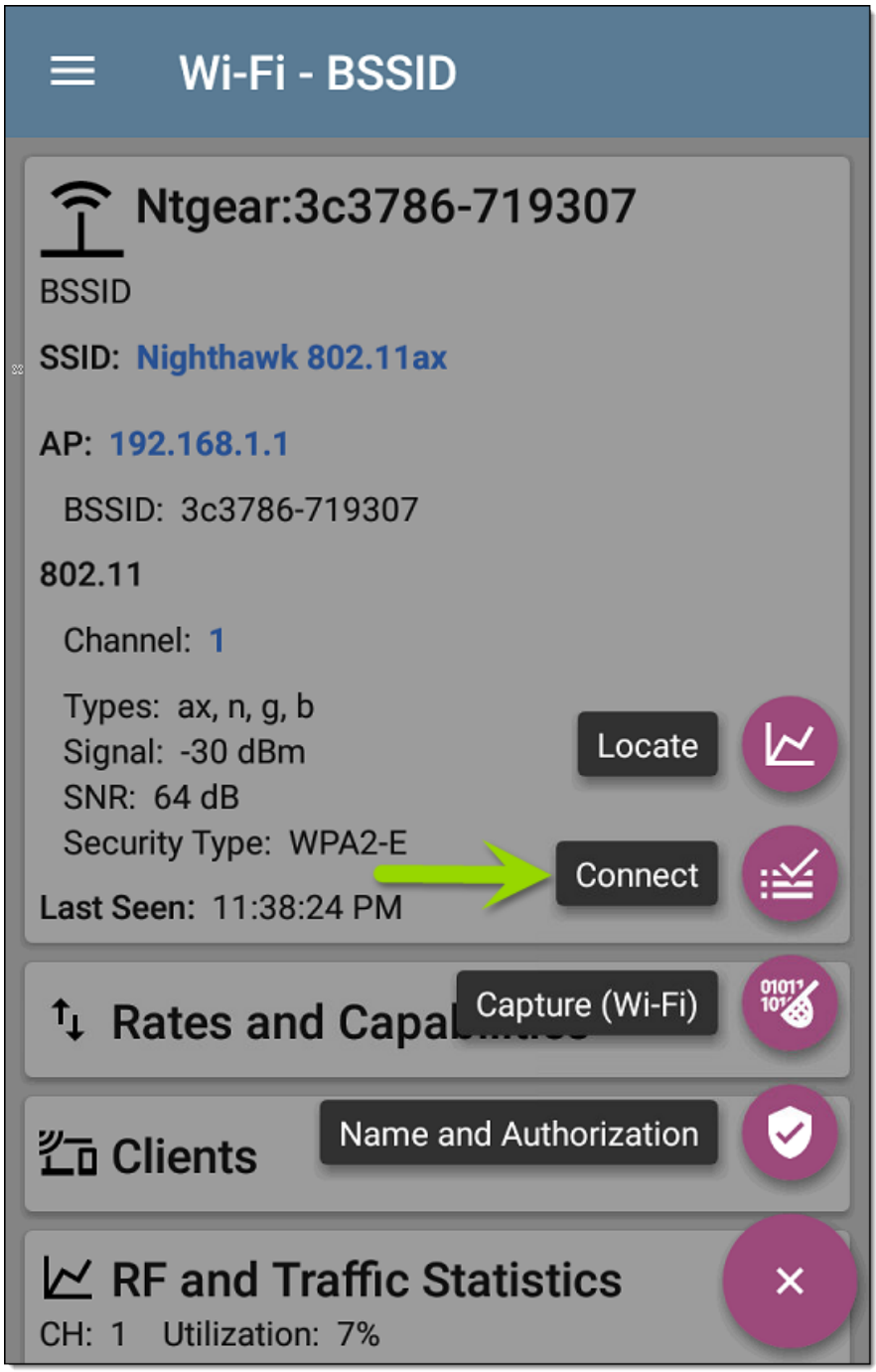
Open the Wi-Fi app from the Home screen.

Tap the menu button to select the **SSIDs** or **BSSIDs** list screen.



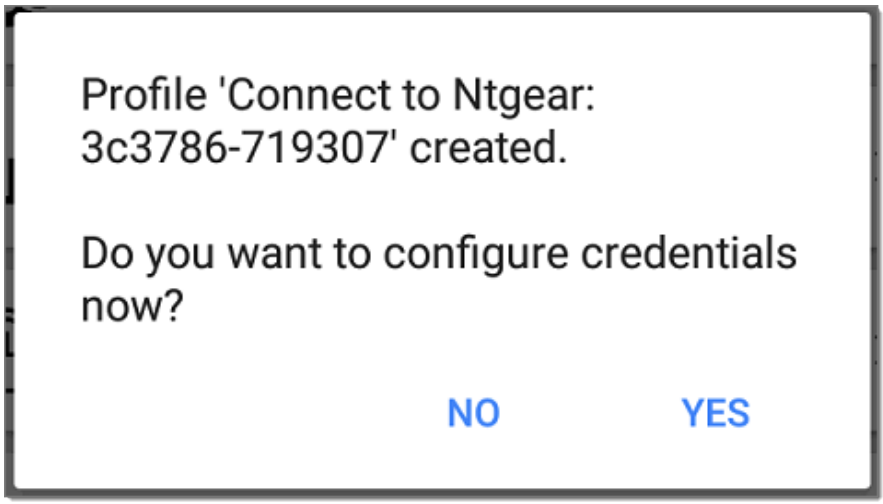
Tap an SSID or BSSID's card to open its Details screen.

Tap the FAB (floating action button) to open the floating action menu.



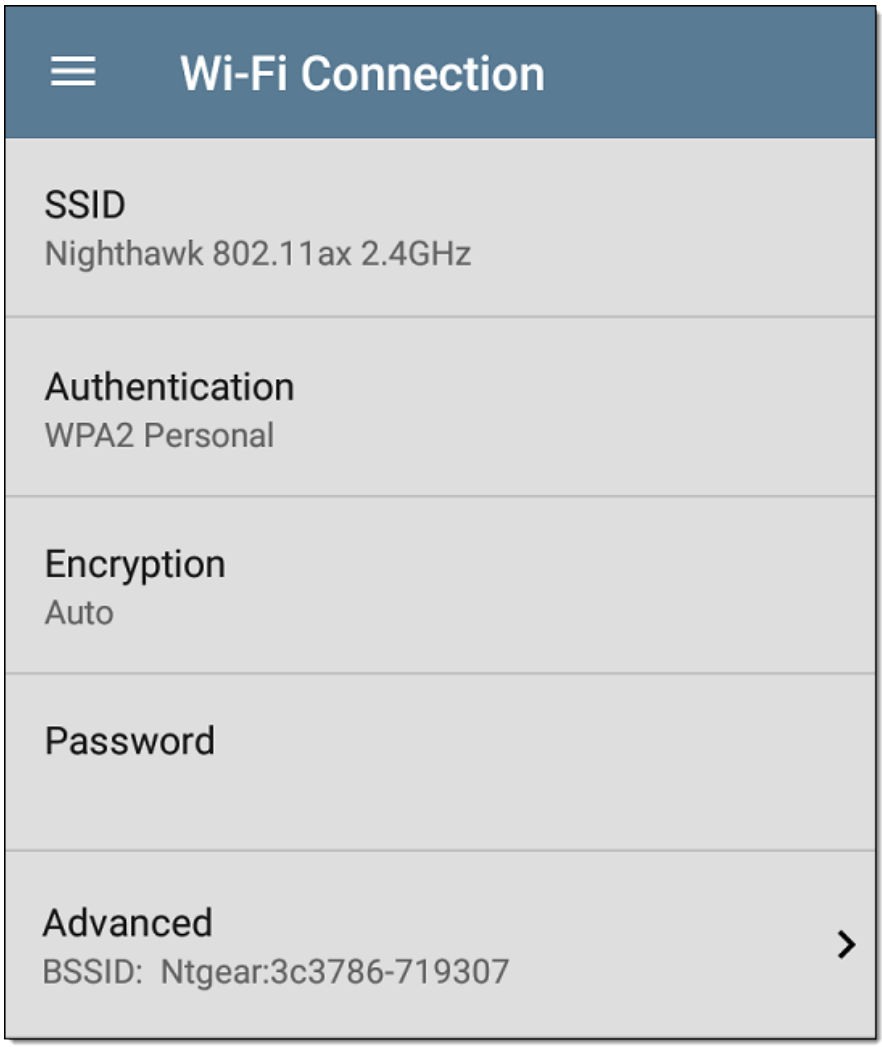
In the floating action menu, tap **Connect**.

A Wi-Fi Profile called "Connect to [SSID/BSSID]" is created in AutoTest.



The SSID, BSSID (if applicable), and Authentication Type are auto-populated in the Wi-Fi Connection settings for the new profile.

Tap **YES** in the pop-up dialog to review and configure additional credentials.



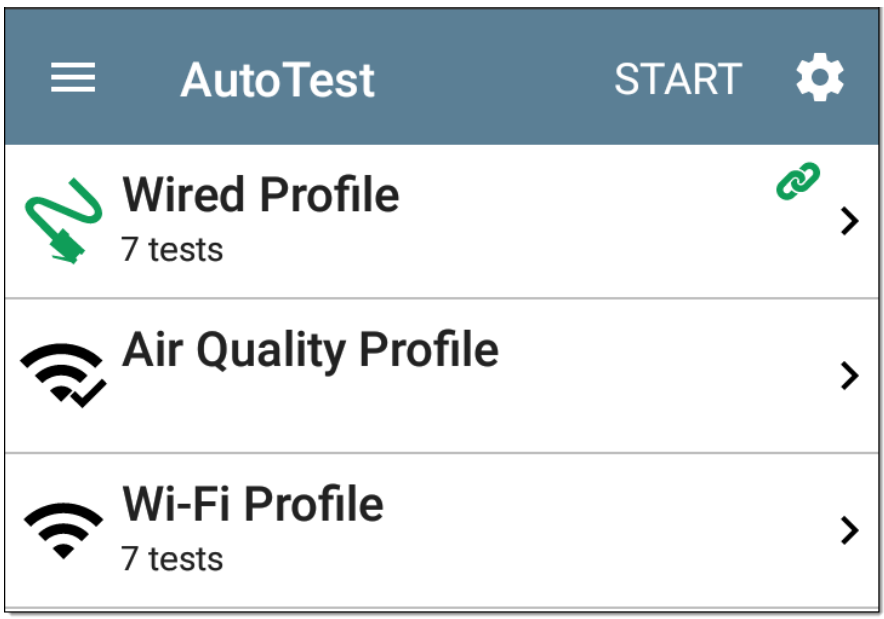
Enter any additional credentials, like the network Password.

After configuring, tap the back button to return to and run the new Profile.

Profile Groups

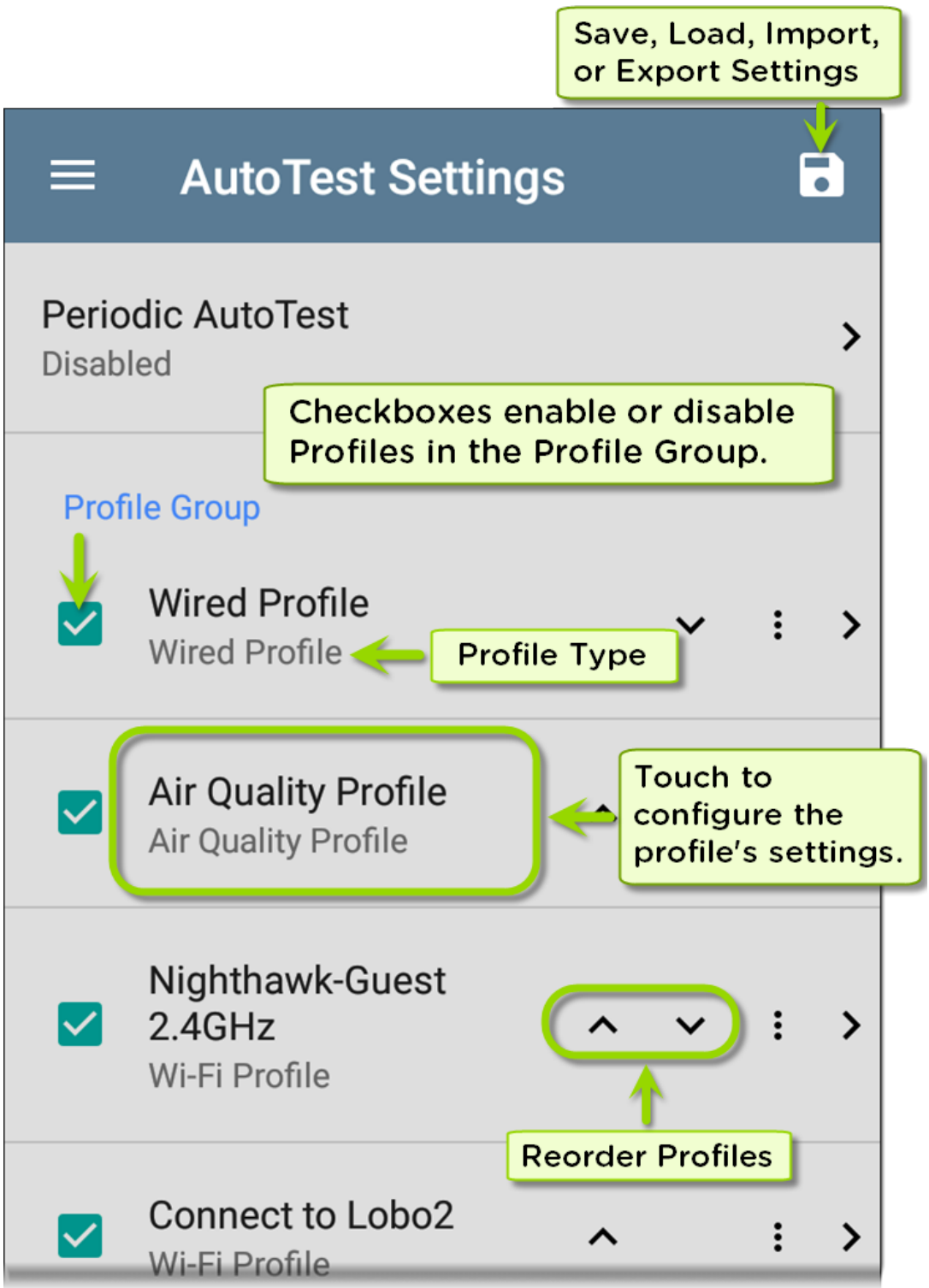
EtherScope nXG also allows you to save Profile Groups. Profile Groups are simply **the included list of test Profiles and the order in which they run** when you start an AutoTest. (See AutoTest Overview for more explanation of Profile Groups.) You can configure and select Profiles and Profile Groups for different locations, jobs, networks, or other purposes.

To manage your Profiles and Profile Groups, tap the Settings button on the main AutoTest screen (with the list of Profiles).



AutoTest Settings Screen

The AutoTest Settings screen contains the Periodic AutoTest and Profile Group settings.



You can perform these actions on the AutoTest Settings screen:

- Check or uncheck the boxes to include or exclude a test Profile from the currently active Profile Group.
- Tap the up and down arrows  to reorder the test Profiles on this and the main AutoTest screen for the Profile Group.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a Profile.
  CAUTION: When you delete a Profile, it is deleted from all Profile Groups. To remove a Profile from the current group, simply uncheck it.
- Tap any Profile's name to open the test and connection settings for the Profile.
- Tap the save icon  to perform the following actions:
  - **Load**: Open a previously saved settings configuration, which includes the Profile Group.

- **Save As**: Save the current settings and Profile Group with an existing name or a new custom name.

  See also Saving App Settings Configurations.

- **Import**: Import a previously exported settings file.

- **Export**: Create an export file of the current settings, and save it to internal or connected external storage.

  See Exporting and Importing App Settings for more details.

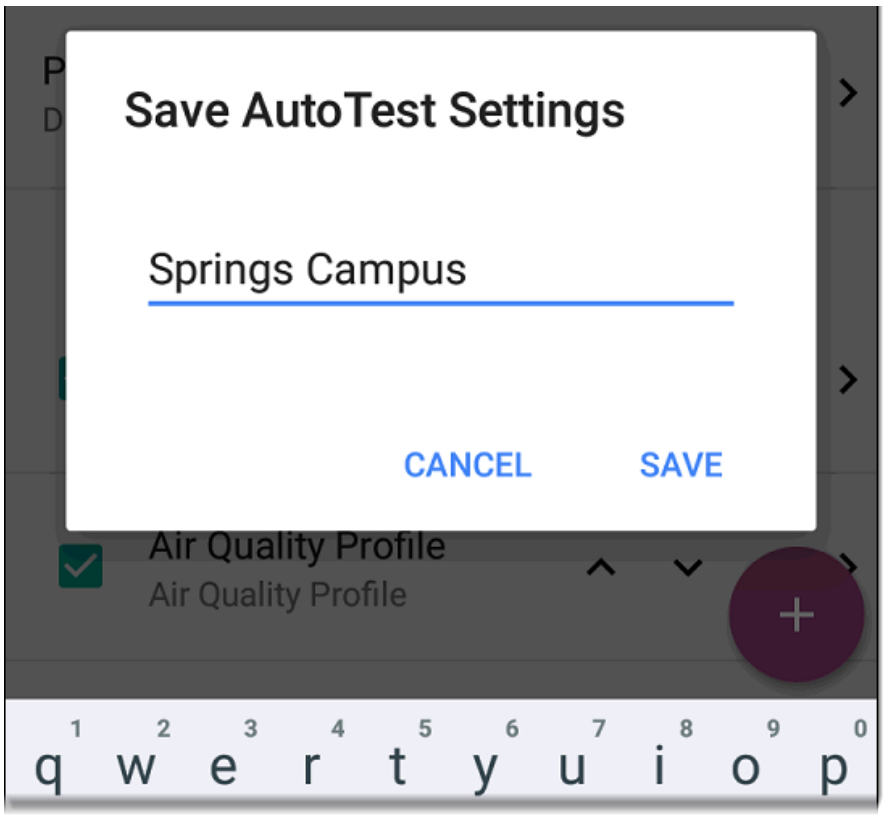
Each Profile Group can run one or many of the three Profiles types. Your saved Profiles are available across all of your Profile Groups.

Custom AutoTest Settings/Profile Group Names

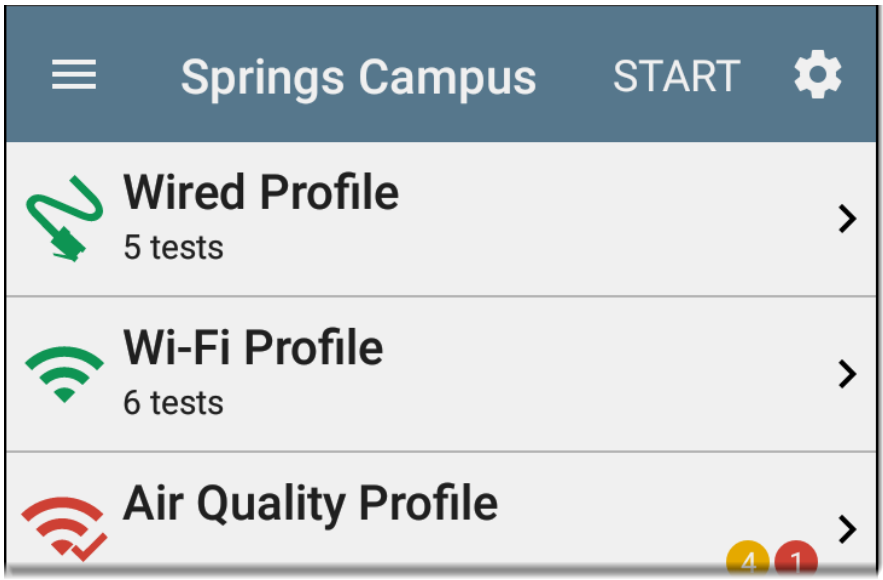
By default, the AutoTest app screen shows "AutoTest" in the header, and the AutoTest Settings screen header is "AutoTest Settings." Once you save a custom name, the name

displays in the AutoTest app header and in the AutoTest Settings screen header.

In the example below, the user saves a custom AutoTest configuration named "Springs Campus."



The main AutoTest app screen now displays the custom name in the header.



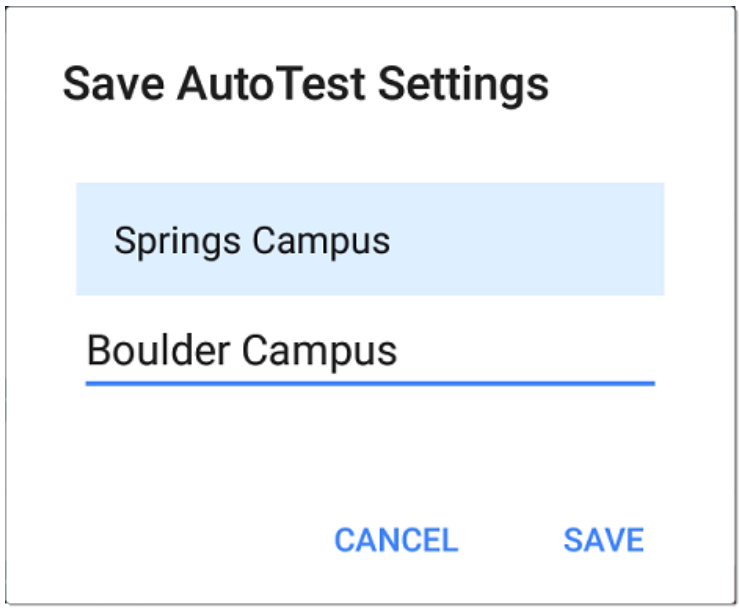
Creating New Profile Groups

To create a new Profile Group, follow these steps:

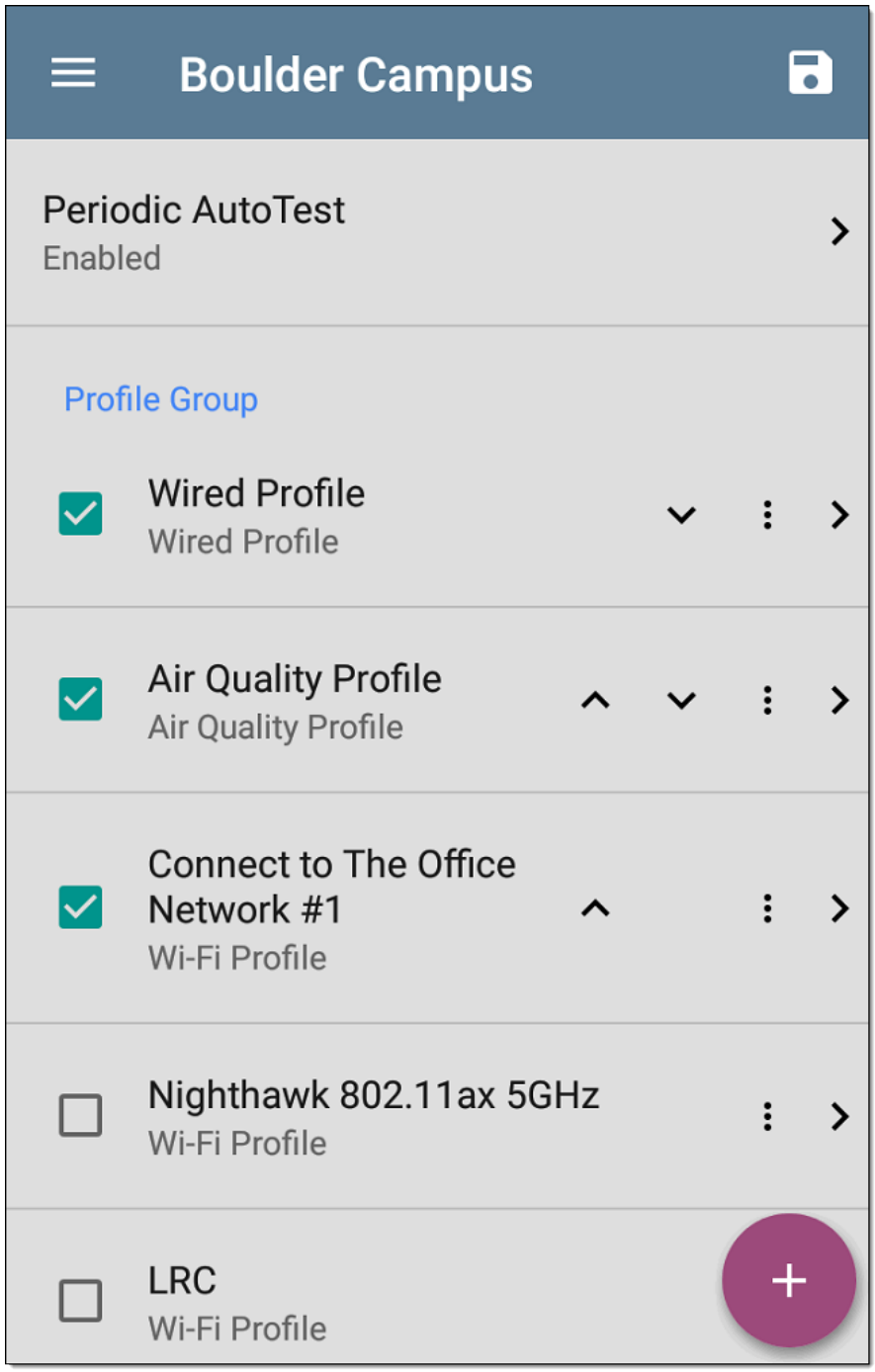
1. Go to the AutoTest Settings and Profile Group screen by tapping on the main AutoTest screen.
2. Uncheck the boxes for any Profiles you do not want included in the new Profile Group.
3. Tap the FAB to add new test Profiles to be included in your new Profile Group.
4. Tap the up and down arrows to change the order in which the test Profiles run. Unchecked profiles automatically move

to the bottom of the list once you leave and revisit this screen.

5. Tap , and select **Save As**. A dialog box opens, where you can enter the new name.



6. Enter a new Profile Group name, and tap **SAVE**. The EtherScope returns to the Profile Group screen with the new group name shown as the title.


Boulder Campus
Periodic AutoTest
Enabled
Profile Group
Wired Profile
Wired Profile
Air Quality Profile
Air Quality Profile
Connect to The Office Network #1
Wi-Fi Profile
Nighthawk 802.11ax 5GHz
Wi-Fi Profile
LRC
Wi-Fi Profile

When running the "Boulder Campus" configuration shown above, AutoTest first runs the Wired Profile over the Ethernet connection, next scans the wireless channels for Air Quality results, and then connects to "The Office Network #1" and remain connected to that network. This Profile Group will *not* connect to or test the "Nighthawk..." or "LRC" networks.

Importing and Exporting AutoTest Profiles

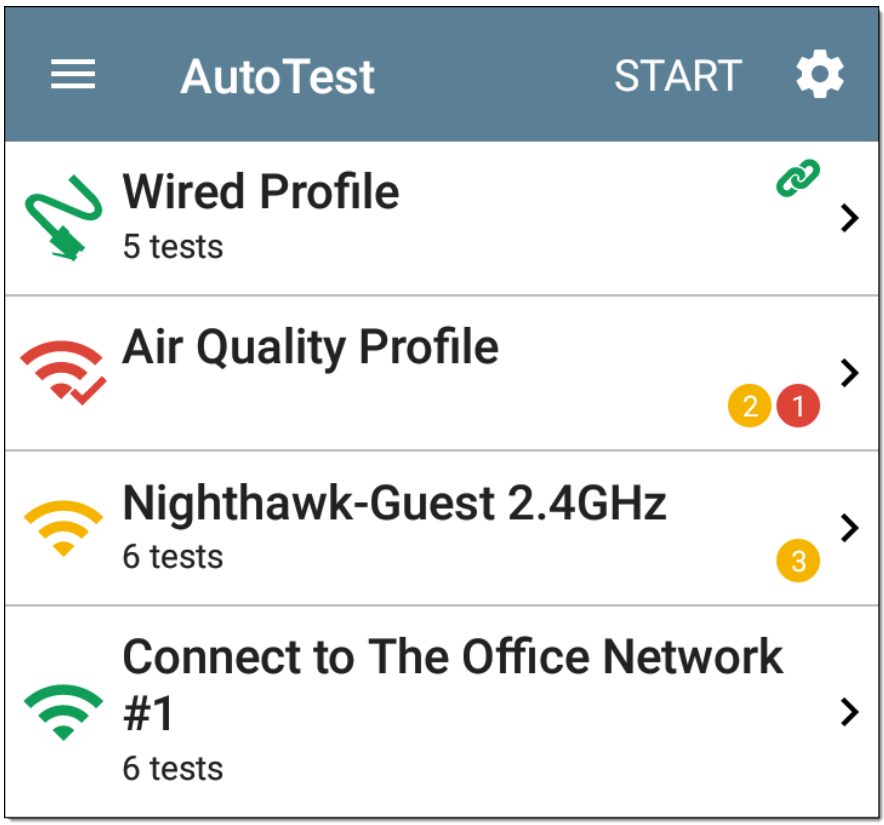
In addition to creating new profiles or using defaults, you can also:

- Import and export profile settings to any connected external or internal storage. See "Importing and Exporting Settings" on page 149.
- Use the Link-Live cloud service to transfer profile settings to other devices in near-real time. See "Transferring AutoTest Settings to Other Devices Using Link-Live" on page 153.

Main AutoTest Screen

To open the AutoTest app, tap the AutoTest icon on the Home screen.

Tap the **START** button on the main AutoTest screen to run all the Profiles in the currently active Profile Group.



The AutoTest screens display icons that correspond to the type of profile, test, or measurement. After running, these icons change color to indicate the status of the test:

- **Green** indicates a successful test or measurement within the set threshold.
- **Yellow** indicates a Warning condition.
- **Red** indicates test Failure.

The number of warnings or failures within each test profile is also displayed in a colored circle to the right of each profile card: 2 1 (2 Warnings, 1 Failure). The thresholds that control the colored test gradings are adjustable in the settings screens for each profile and test type.

The green link icon indicates an active network connection.

Each profile and test is summarized on a card. Tap a profile's or individual test's card to open and view test result details, including the causes of any Warnings or Failures.

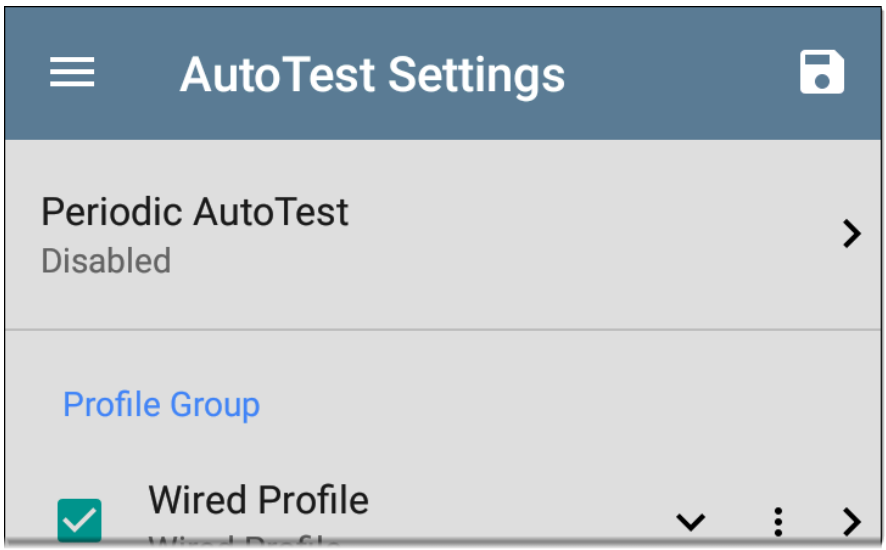
Back to Title and Contents

Periodic AutoTest

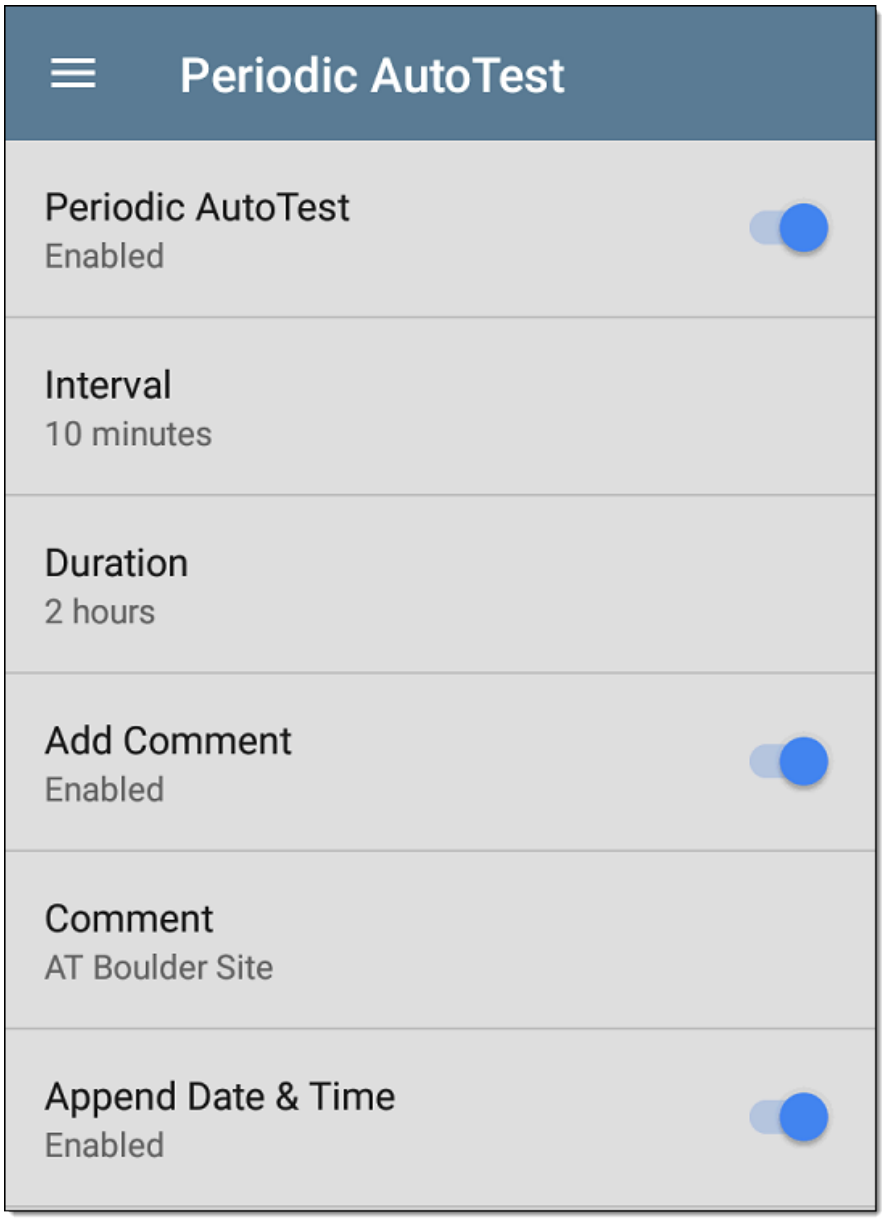
The Periodic AutoTest feature allows you to run AutoTests at set time intervals.

Periodic AutoTest Settings

To enable and configure Periodic AutoTest, open the AutoTest Settings and Profile Group screen, and tap **Periodic AutoTest**.



The Periodic AutoTest settings screen displays.



Tap the **Periodic AutoTest** field to enable, and adjust the settings below as needed.

Interval: Amount of time between each AutoTest run

Duration: Total length of time Periodic AutoTests run

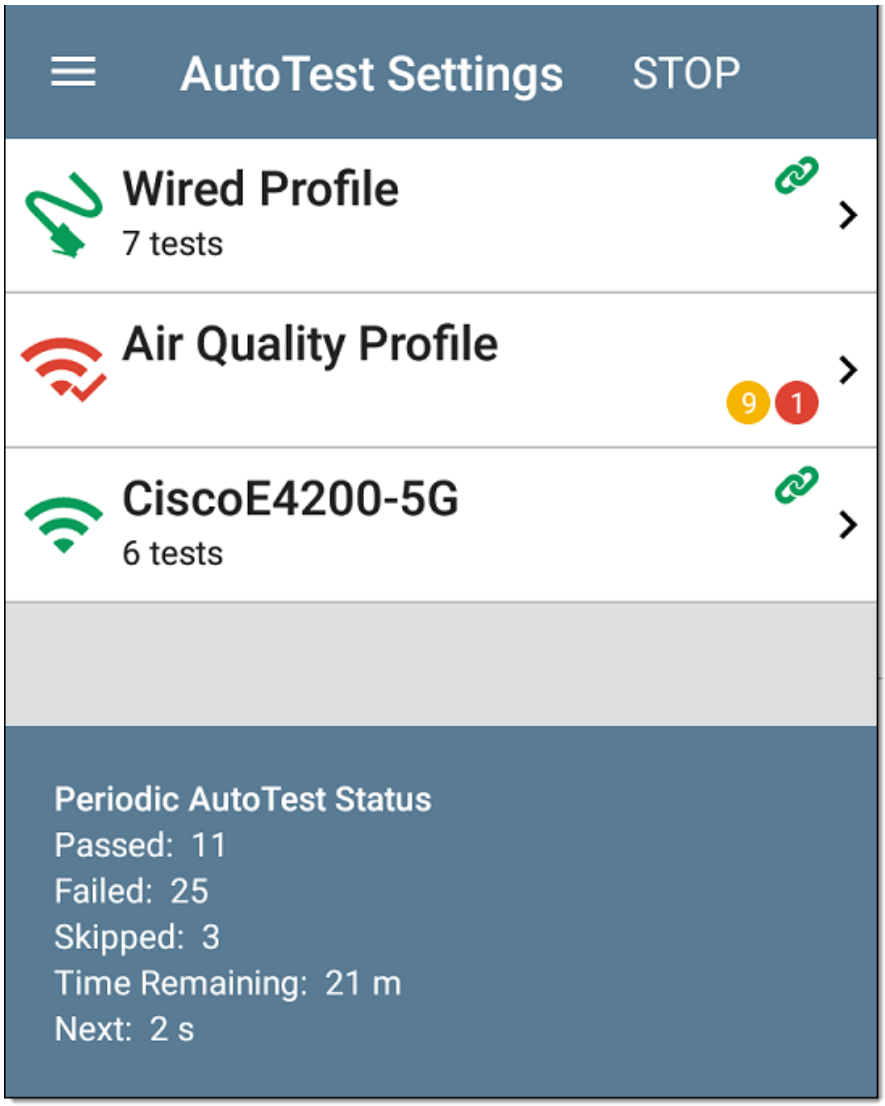
Add Comment: Enabling this setting allows you to attach a comment to the Periodic AutoTest result in Link-Live Cloud Service. The comment appears as a label on the Link-Live.com Results page. This setting and the **Comment** setting below are enabled by default.

Comment: This field appears if the **Add Comment** setting is enabled. Enter the label you want to be attached to the uploaded Periodic AutoTest result on Link-Live. The default is "Periodic AutoTest."

Append Date & Time: This field appears if the **Add Comment** setting is enabled and adds a numeric date and time to the end of the **Comment** above.

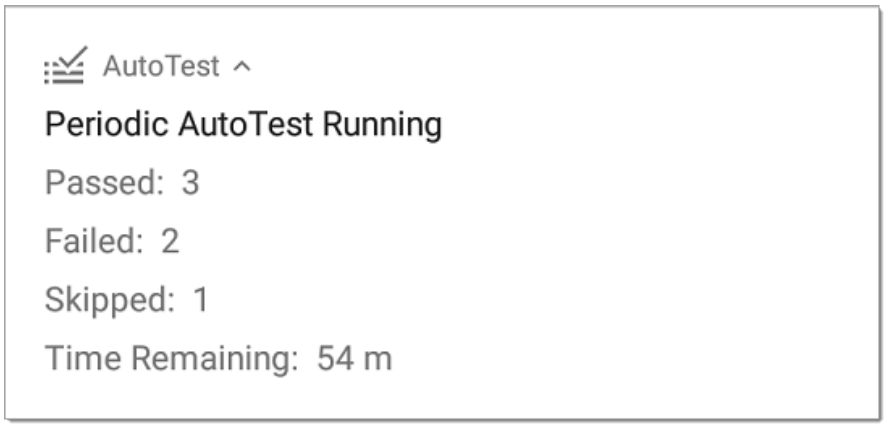
Running Periodic AutoTest

Tap **START** on the main AutoTest screen to begin Periodic AutoTests. AutoTests continues to run at the set Interval for the selected Duration or until you tap **STOP** in AutoTest.



The Periodic AutoTest Status is summarized at the bottom of the AutoTest screens. Passes and failures are reported for each run of the entire Profile Group, rather than individual Profiles. Periodic AutoTests are skipped if the previous interval's test is still running when the next time interval occurs, such that the next run could not start.

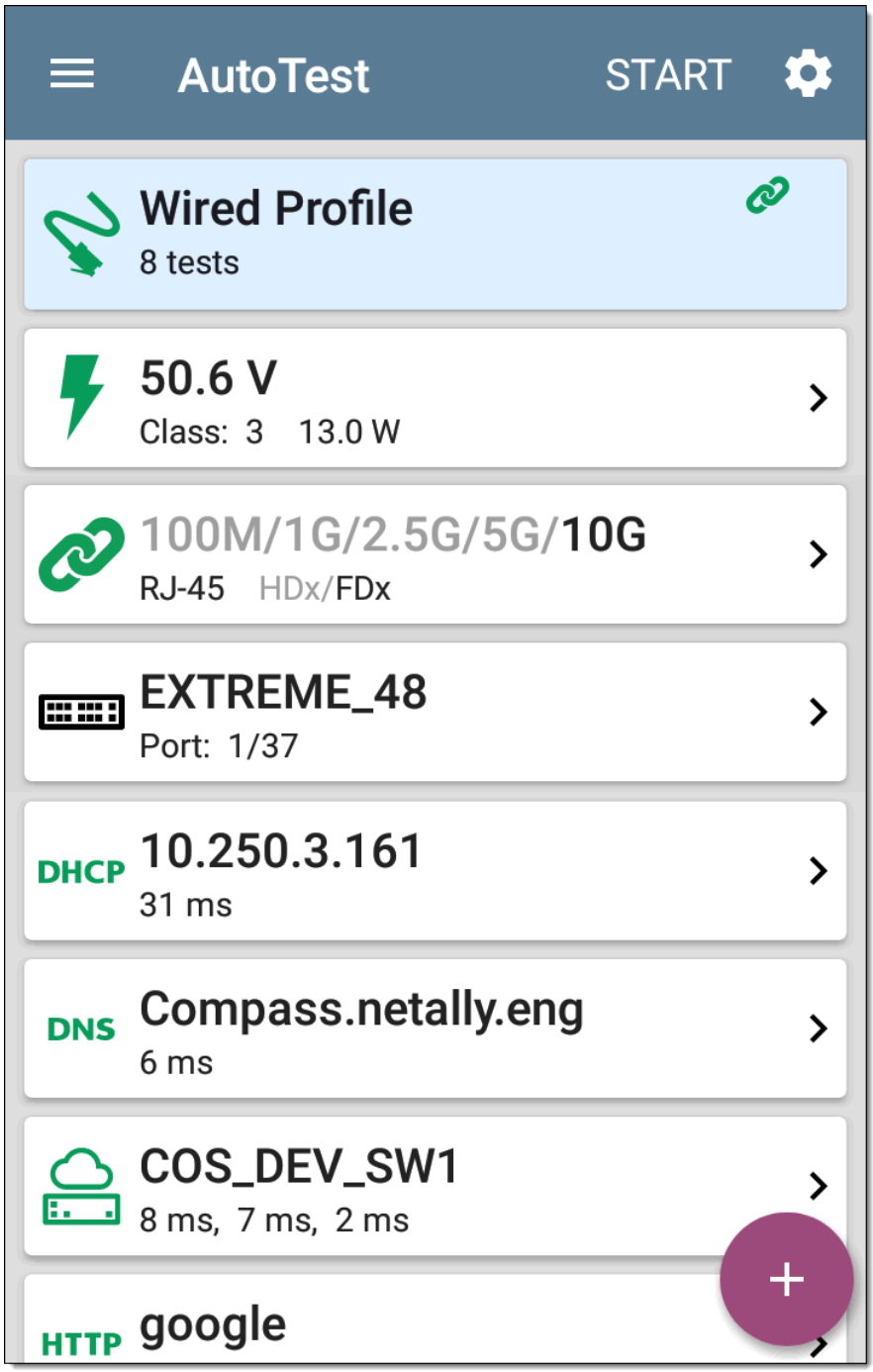
The Periodic AutoTest icon  appears in the top Status Bar when Periodic AutoTest is running or has completed. Drag down on the Status Bar to view the corresponding notification.



NOTE: AutoTest has priority control of the Test Ports, so other apps, including Discovery, Wi-Fi, Wi-Fi Capture (but not Wired Capture), and AirMapper, are paused while AutoTest completes.

Wired AutoTest Profiles

A Wired Profile runs a series of tests over your copper or fiber network connection.



Like the main AutoTest screen, Wired Profile tests are summarized on cards. Tap a card to view individual test screens.

Each test icon (except the switch) displays green, yellow, or red to indicate the status of the completed test step: **Success**/**Warning**/**Fail**. The Switch Test card shows the name and port of the nearest switch, but does not turn green to indicate success.

When Wired Profiles Run Automatically

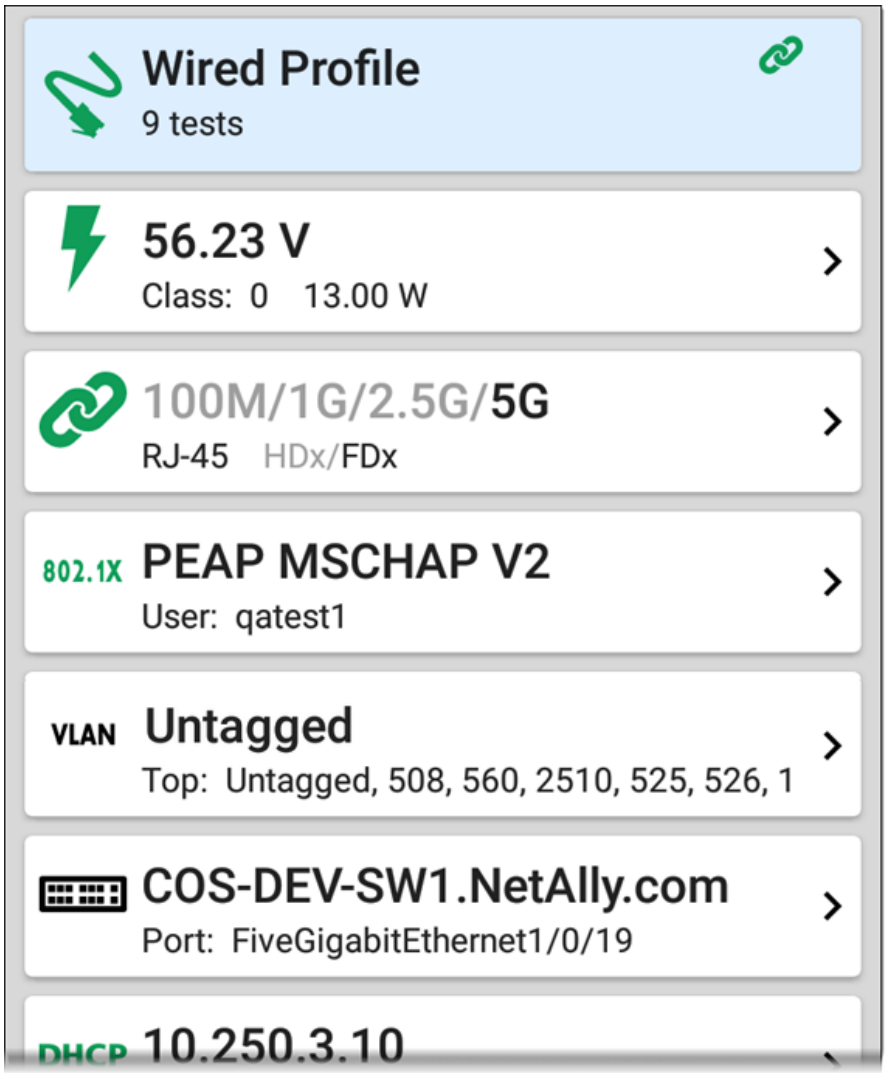
The last enabled Wired Profile in the currently active Profile Group runs automatically when a copper cable is connected or energy is detected to the top RJ-45 port, unless the AutoTest app is open in the foreground and there is more than one enabled Wired Profile. A Wired Profile does not start automatically if Periodic AutoTest is running.

After a Wired Profile runs, a wired network link is maintained for further testing. Wired Test Port linkage is indicated in the top Status Bar with this notification icon:  .

Wired-Profile-Specific Tests

The following tests are specific to a Wired Profile:

- PoE
- Wired Link
- 802.1X
- VLAN
- Switch



The 802.1X card only appears if the **802.1X** setting is enabled for the Wired Profile.

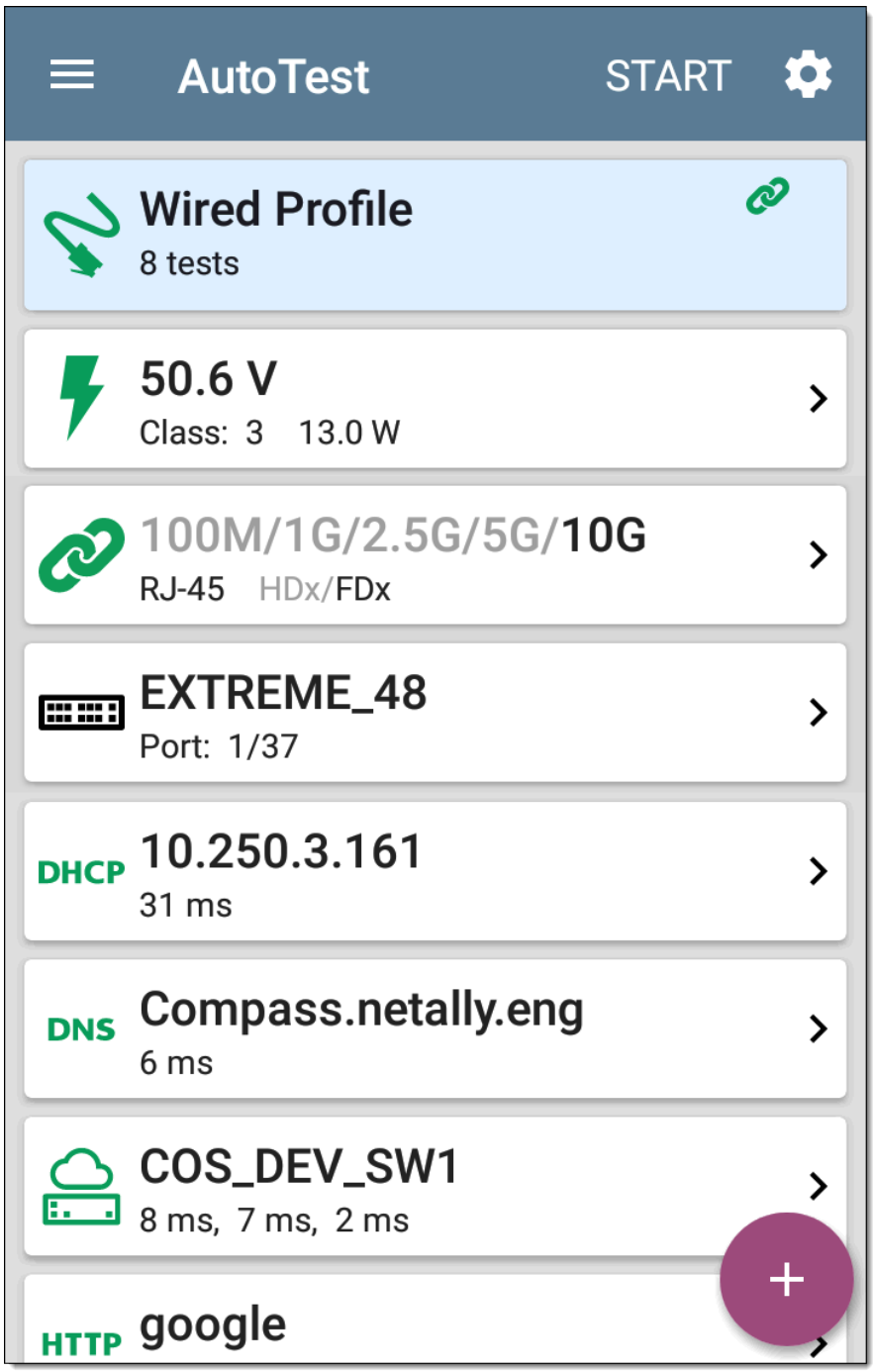
The VLAN test card appears if the **VLAN** setting is enabled or if VLAN-tagged traffic is detected during the AutoTest.

PoE, Wired Link, 802.1X, VLAN, and Switch Results are described next.

- Skip to Wired Profile Settings.
- Skip to DHCP, DNS, and Gateway Tests.
- Skip to Test Targets.

Wired Profile Results

The image below shows a completed AutoTest Wired Profile.



On the Wired Profile screens, you can perform these actions:

- Tap any of the test result cards, like PoE, Link, or Switch to open the individual test result screens.
- From any individual test screen, tap the settings icon to go directly to the settings for the current test.
- On the individual test screens, tap **blue underlined links** to open a Discovery app Details screen showing the selected device or ID.

  NOTE: You may need to Configure SNMP settings in the Discovery app to see all the available information about a network component, such as name and port information.
- Tap other **BLUE LINKS** or the blue action overflow icon ••• at the bottom of the test results screens for additional actions.

  NOTE: Blue links and action icons do not appear on every test results screen, and if the active connection is dropped, you may

need to rerun the Profile to re-establish link and enable additional actions.

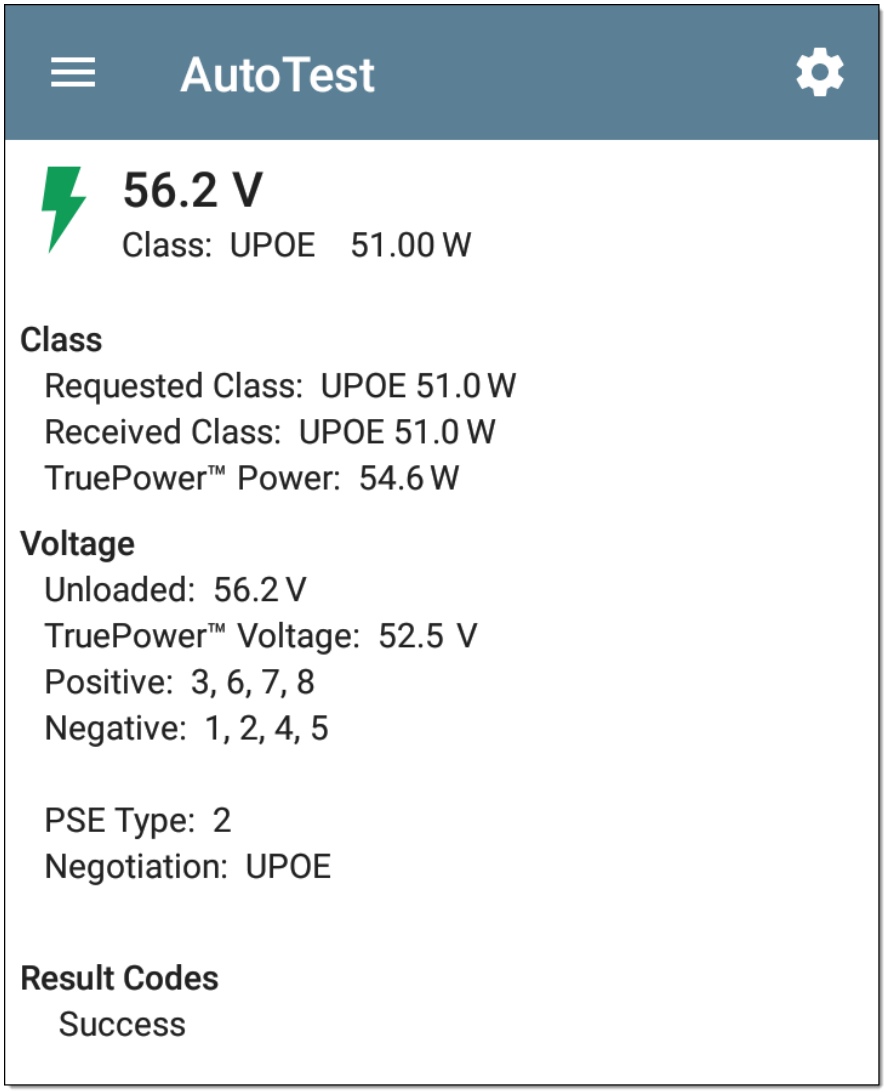
PoE Test Results

The card for the Power over Ethernet (PoE) test displays the measured Voltage, Class, and Wattage.

Refer to PoE Settings if needed.

Tap the card to open the PoE results screen.

PoE Test Results Screen



In addition to the information from the PoE card, the PoE test screen shows these results:

Class

Requested Class: Class selected in the PoE test settings

Received Class: Class acknowledgment received from the switch

TruePower™ Power: Measured wattage with load.

NOTE: The PoE card displays additional TruePower™ results only if TruePower is enabled in the Wired Profile PoE Settings.

Voltage

Unloaded: Measured voltage without load

TruePower™ Voltage: Measured voltage with load

Positive: Positive PoE cable pair IDs

Negative: Negative PoE cable pair IDs

PSE Type: Switch's advertised Power Sourcing Equipment (PSE) type. Recognized types are 1 – 4, LTPoE++, Cisco UPOE, and PoE Injectors. PSE supporting UPOE are classified under Type 2. If the type cannot be determined, "1/2" is displayed.

Negotiation: Negotiation status for UPOE and Class 4 (UPOE or LLDP)

Result Codes: Final status of the test (Success or Failure)

Wired Link Test Results

The Wired Link card indicates whether you can connect to an active network switch.

The Link test card for a copper Ethernet connection displays the advertised speed and duplex capabilities in gray text and the detected speed and duplex in **black text**.

EtherScope can test and display information for link speeds up to 10G.

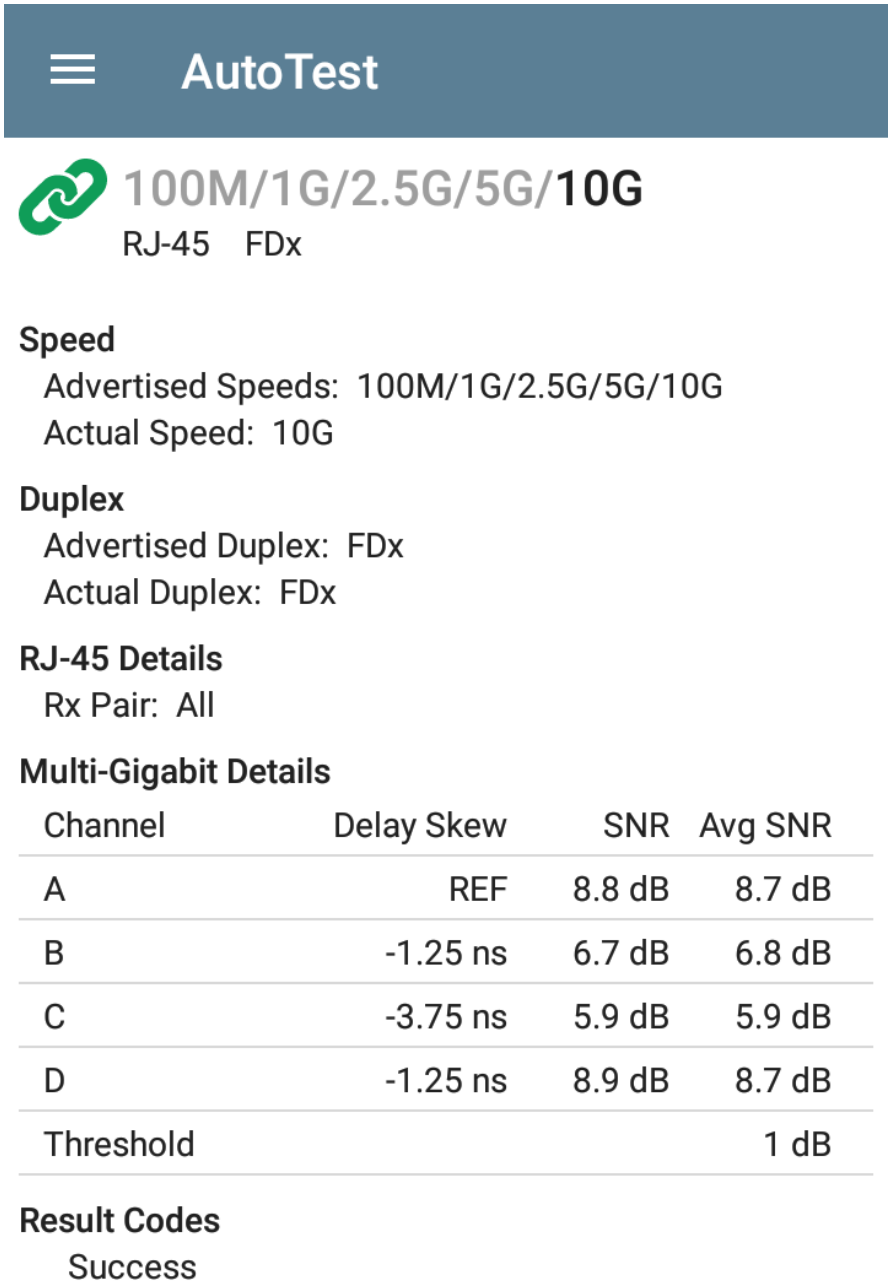
For a Fiber connection, the Link test card shows the connection speed and duplex.

The link icon turns yellow (displays a Warning) under the following conditions:

- EtherScope has linked at a speed slower than the maximum advertised speed.
- The link is using half duplex.
- For links faster than 1G, EtherScope has detected a minimum SNR value below the set threshold.

Tap the card to open the Link test screen.

Wired Link Test Screen



The Wired Link test screen shows the following:

Speed

Advertised Speed: Speed capability as reported by the switch

Actual Speed: Link speed as measured by EtherScope nXG

Duplex

Advertised Duplex: Duplex capabilities reported by the switch

Actual Duplex: Duplex in use as detected by EtherScope

RJ-45 Details (Copper)

Rx Pair: Link receive pair

Multi-Gigabit Details (Copper)

This table appears only when the Wired Profile is linked at speeds higher than 1G. Each twisted pair channel is graded based on the minimum SNR observed. Data in the table updates each second as long as the link persists.

Channel: Channels A, B, C, and D representing the twisted pairs in the cable

Delay Skew: Difference in propagation delay between sets of wired pairs. Channel A acts as the reference for the other channel measurements.

SNR: Current signal-to-noise ratio on each channel

Avg SNR: The average SNR measurement since link was established

Threshold: Multi-Gigabit SNR Threshold from the Wired Connection settings

SFP Details (Fiber)

The SFP Details are defined as follows:

Wavelength: Wavelength (in nanometers) at which the fiber connection is operating

Temperature: Temperature in degrees Celsius

Voltage: SFP transceiver power supply voltage (~3.3 V)

Tx Bias Current: Transmitter bias current

Tx Power: Transmitter power

Rx Power: Link receiver power

Reference Power: The user can set a Reference Power by pressing the **SET REFERENCE** button. This sets the current Rx Power as the reference. The value is saved until cleared by the **CLEAR REFERENCE** button. It is saved across reboots.

Power Difference: The difference between the current Rx Power and the reference. The number is positive if the current value is greater than the reference value.

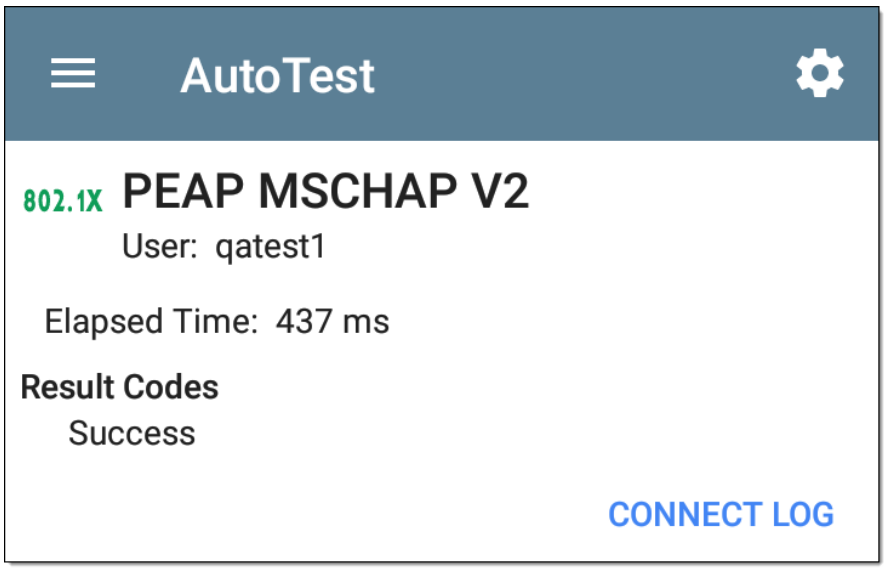
Results Codes: Final status of the test (Success or Failure)

802.1X Test Results

The 802.1X test card only displays if the 802.1X setting is enabled in the Wired Profile Settings.

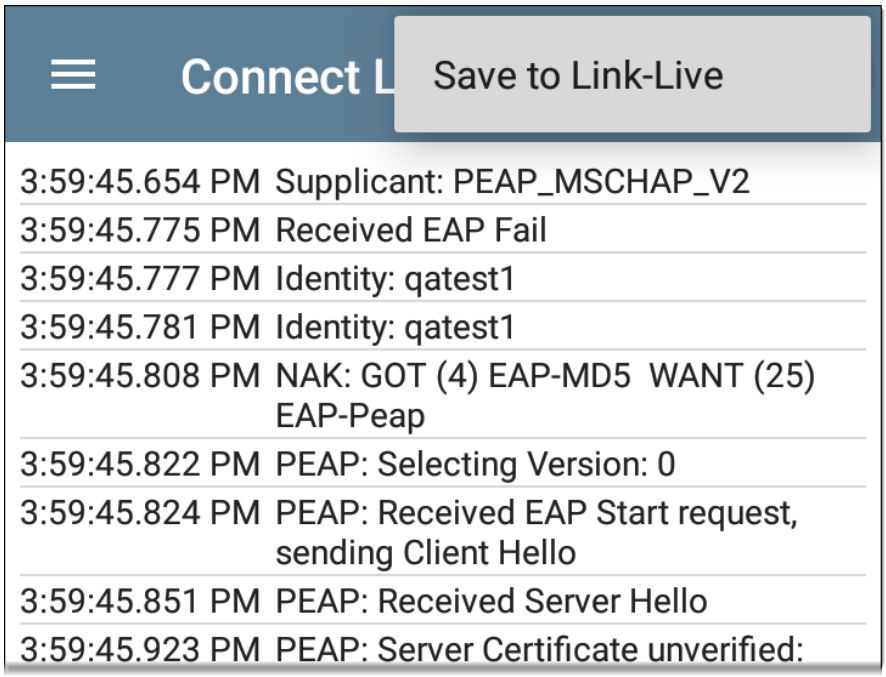
The card shows the EAP type selected in the Wired Connection settings and the username or certificate used. The 802.1X icon turns green if the connection is successful and yellow if 802.1X authentication fails.

802.1X Test Screen



The 802.1X screen also shows the time it took for the authentication process to complete along with Result Codes.

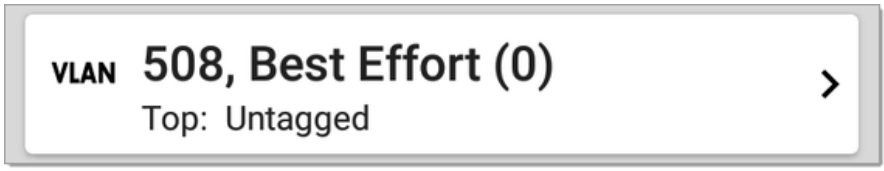
Tap the blue **CONNECT LOG** link to view the 802.1X Connect Log.



Select the action overflow icon ⋮ at the top right on the Connect Log screen to attach the log to its associated AutoTest result on the Link-Live website. You can also attach the Connect Log from the floating action menu + on the main Wired Profile screen.

VLAN Test Results

The VLAN card only displays if the VLAN setting is enabled in the Wired Profile Settings or if AutoTest detects VLAN-tagged traffic.



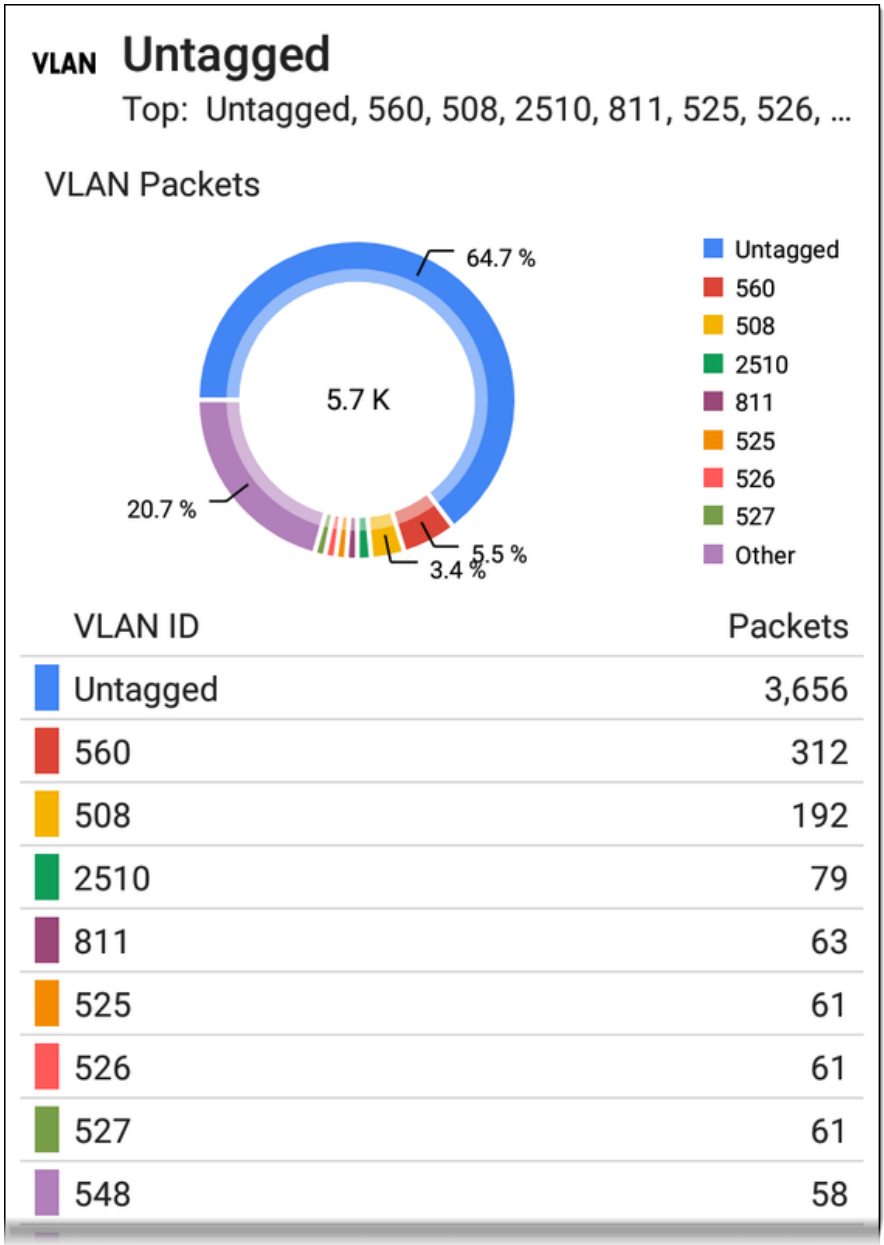
The top line on the VLAN test card shows the configured VLAN settings (image above) or "Untagged" (image below) if VLAN disabled but VLAN-tagged traffic is seen.

Untagged indicates that no VLAN tag is present in either received or transmitted frames, also referred to as the Native VLAN.

The second line on the VLAN card displays the top VLANs with the most detected traffic.

Tap the card to open the full VLAN screen.

VLAN Test Screen

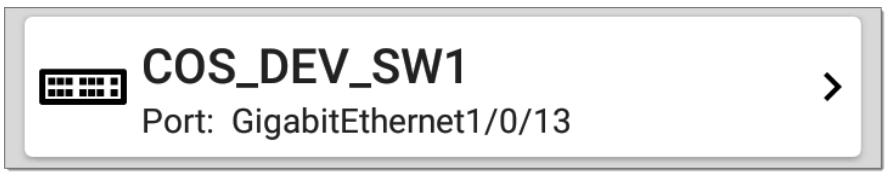


The VLAN test screen displays the real-time traffic the EtherScope detects on the top VLANs. Up to nine VLANs with the highest traffic are displayed as colored portions of the pie chart.

The table on the lower part of the VLAN screen lists all the VLANs seen.

Switch Test Results

The results available for the Switch Test are based on Discovery Protocol advertisements and SNMP system group information. SNMP forwarding table data is used to determine the Nearest Switch. See Discovery Settings for SNMP configuration instructions.



The Switch test card displays the Nearest Switch and the port name. The Switch icon remains black if the test is successful.

- If the EtherScope does not detect any network traffic moving through the switch after 45 seconds, the switch icon turns yellow.

- If the connection is lost while the Wired Autotest is running, the switch icon turns red.

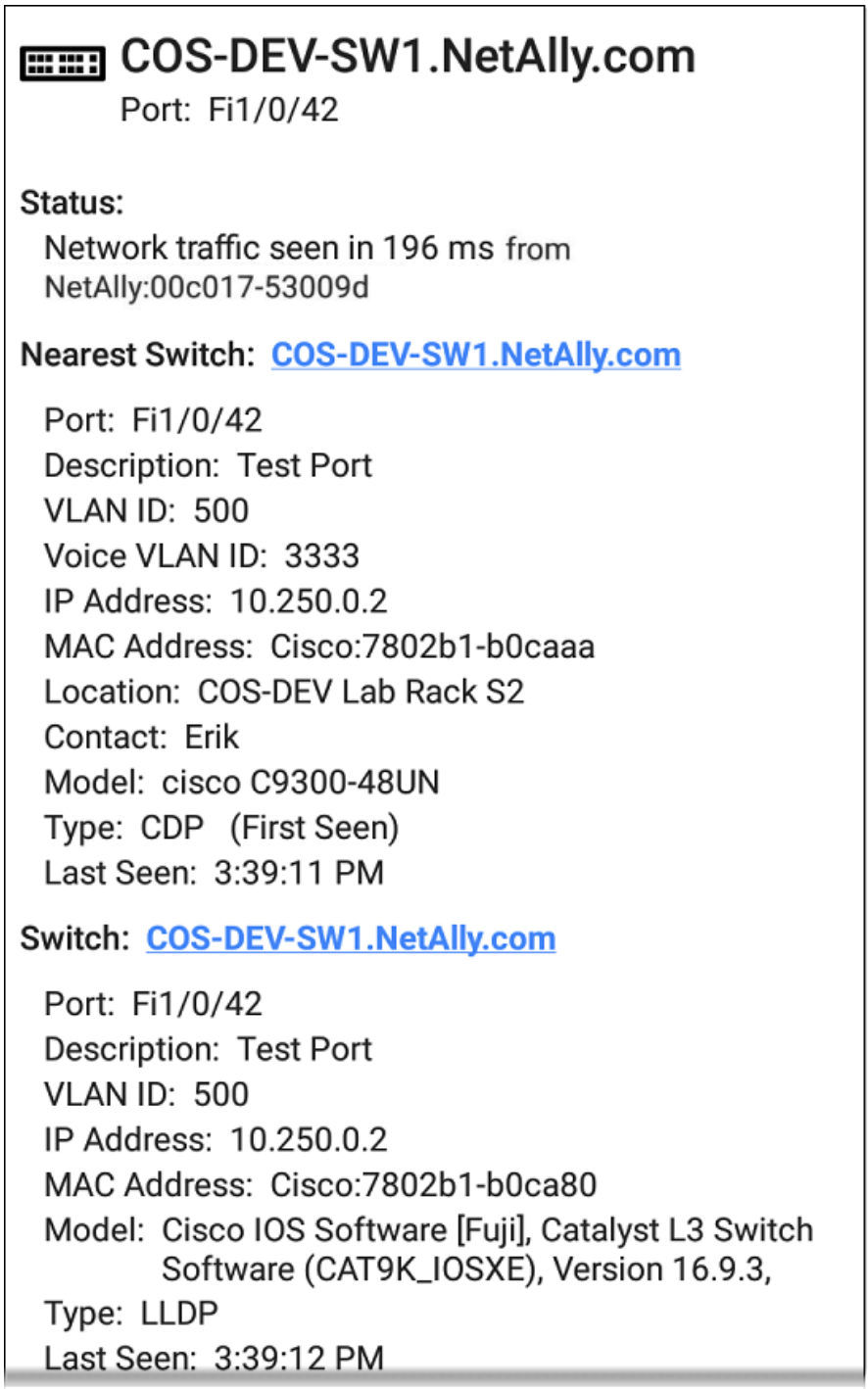
- If the EtherScope was unable to identify the nearest switch, "Nearest Switch Not Found" displays on the Switch card.

The EtherScope continues to search for the nearest switch, even after the AutoTest completes.

Tap the Switch card to open the full switch results screen.

Switch Test Results Screen

Information on the Switch Test screen is organized by the order in which it was received, either via Discovery Protocol advertisements or SNMP.



Each section represents a unique port advertisement as defined by protocol type and MAC address.

The switch results screen shows the following data fields:

Status: Time elapsed after link was established before network traffic was received from the switch. The MAC address of the device that sent the packet is also shown.

Nearest Switch: Name of the switch determined to be closest to the EtherScope

Port: Detected Port name

Description: Configured description reported by the switch

VLAN ID: VLAN ID number (if present)

Voice VLAN ID: Voice VLAN ID number (if present)

IP and MAC Addresses: Discovered switch addresses

Location: Configured location reported by the switch. This field only appears if the EtherScope has SNMP access to the Nearest Switch.

Contact: Configured contact person reported by the switch. This field only appears if the

EtherScope has SNMP access to the Nearest Switch.

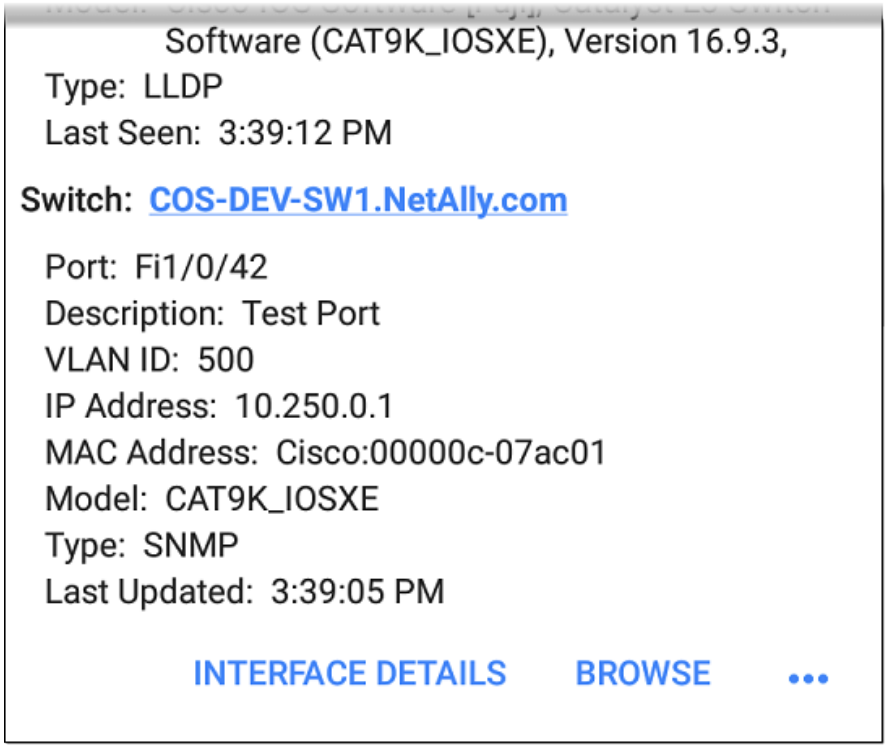
Model: Switch model name and/or number

Type: Discovery Protocol - CDP, LLDP, EDP, FDP, or SNMP. (First Seen) displays next to the protocol type first seen by the EtherScope.

Last Seen: For non-SNMP discovery protocols (CDP, LLDP, EDP, or FDP), the time the advertisement was last received by the EtherScope

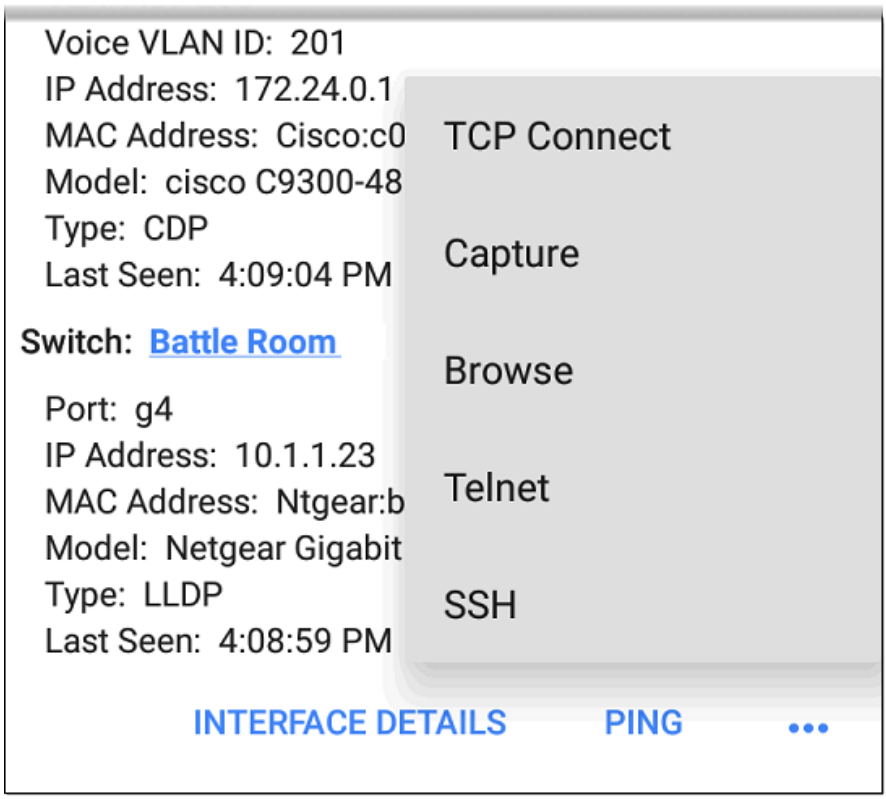
Last Updated: For SNMP only, the time the information was gathered from SNMP tables

SNMP information, if available, appears at the bottom of the screen once the discovery process has acquired relevant data.



Switch: Below the Nearest Switch, other switches seen via advertisements or SNMP

At the bottom of the switch test screen, tap the blue links or the action overflow icon ••• to open other apps or tools with the target (in this case, the **Nearest Switch**) pre-populated.



For example, **INTERFACE DETAILS** opens the Interface Details screen for the Switch Port in the Discovery app.

> NOTE: The **Interface Details** action link only appears in the Switch results if EtherScope has current Discovery data, and AutoTest was able to identify the nearest switch and connected interface.

The **Ping**, **TCP Connect**, and **Capture** selections open the corresponding NetAlly apps, populated with the switch's address. **Browse** opens the

Chromium browser, and **Telnet** or **SSH** opens the JuiceSSH app.

DHCP, DNS, and Gateway Results

Results for these tests operate the same in both Wired and Wi-Fi profiles.

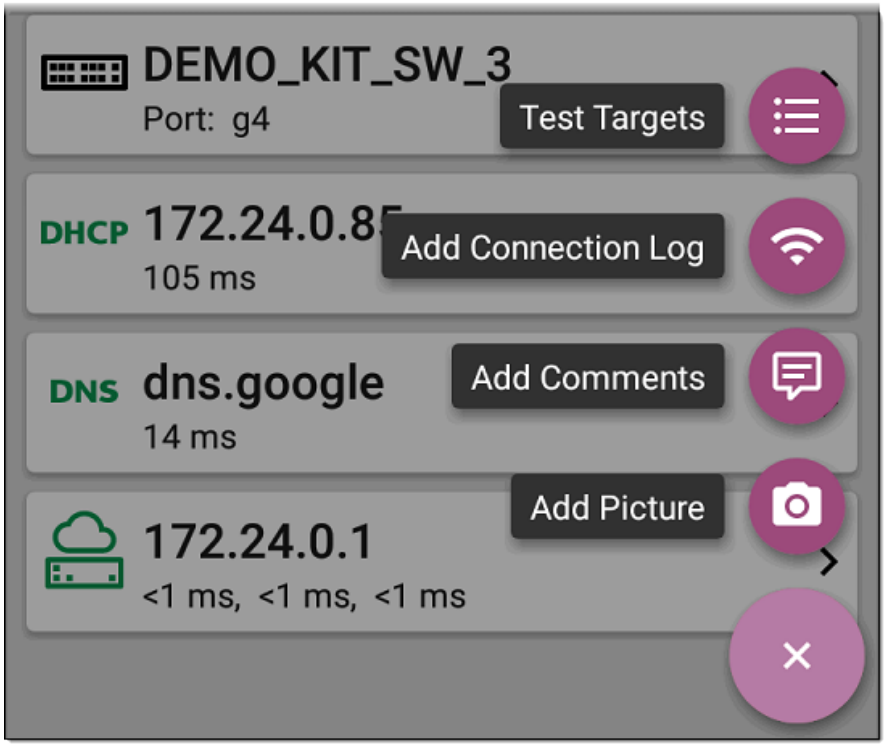
See DHCP, DNS, and Gateway Tests

PING FTP TCP HTTP Target Tests

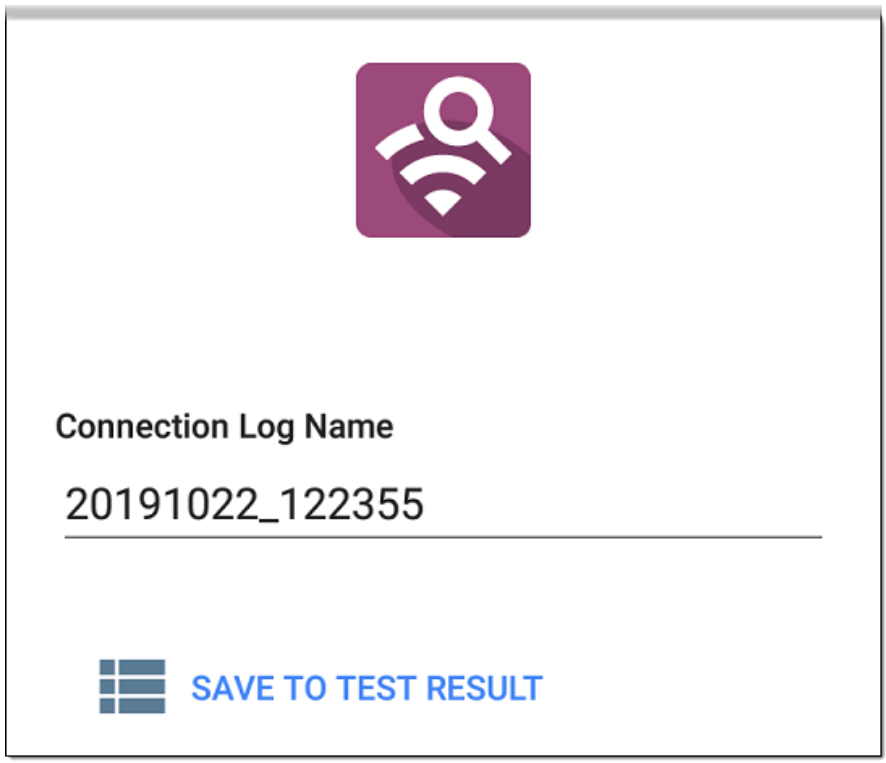
See the Test Targets topic for information on target test results.

Wired Profile FAB

The floating action button (FAB) on AutoTest Profile screens allows you to add Test Targets to the Profile, as well as attach comments, an image, and an 802.1X connect log to this AutoTest result on the Link-Live website.

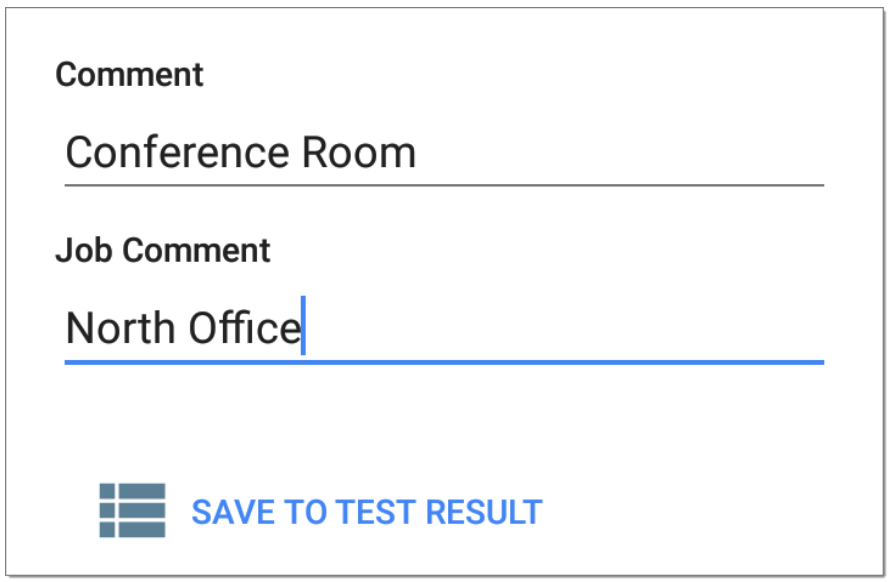


- The **Test Targets** option opens the Test Targets screen, where you can add Ping, TCP Connect, HTTP, and FTP target tests to the current profile.
- **Add Connection Log** opens a Link-Live sharing screen that allows you to custom name the log file before saving to the test result.



Tap the field to enter your desired log name, and tap **SAVE TO TEST RESULT** to upload.

- **Add Comments** also opens a Link-Live sharing screen where you can enter comments.



Tap the fields to enter your desired comments, and tap **SAVE TO LAST TEST RESULT** to upload them.

- The **Add Picture** function lets you open the **Gallery** or **Camera** app to select or take a photo that is then uploaded and attached to your test result.

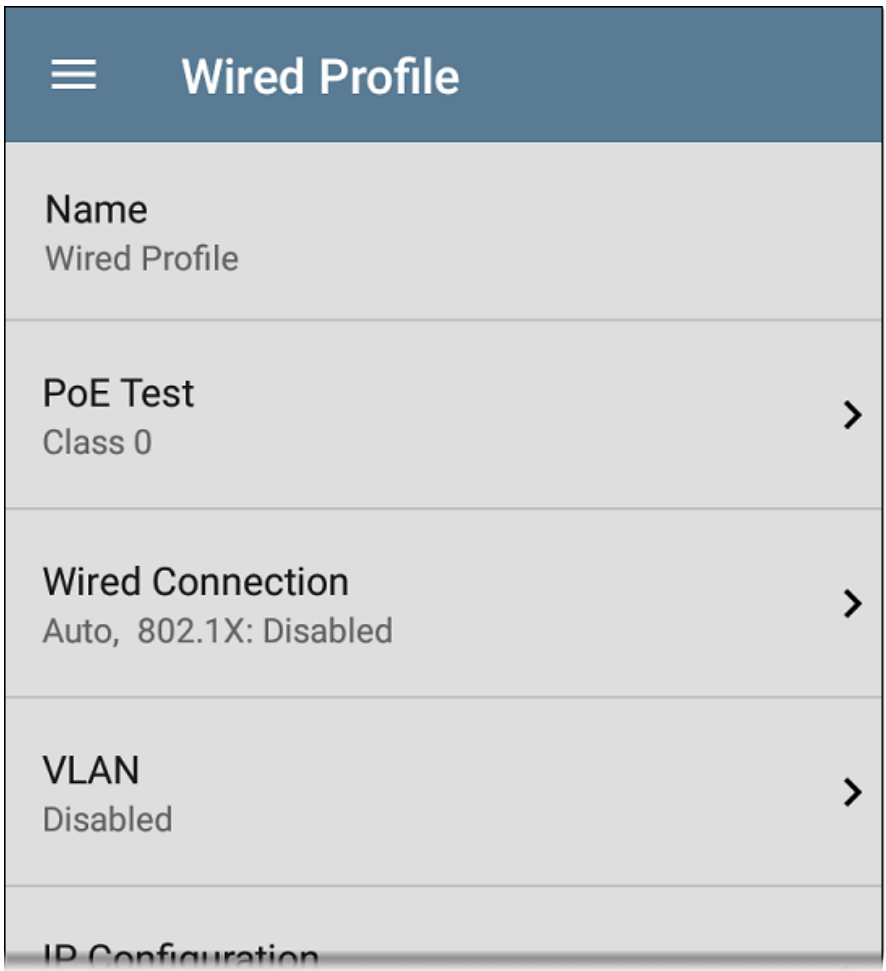
See the Link-Live App chapter to learn about Link-Live and uploading.

Back to Title and Contents

Wired Profile Settings

These settings control the wired test port connection, PoE test, the thresholds for **Pass**/**Warning**/**Fail** results, and any user-added test targets.

Tap the settings icon on the Wired profile screen, or add a new Wired profile, to configure the profile's settings.



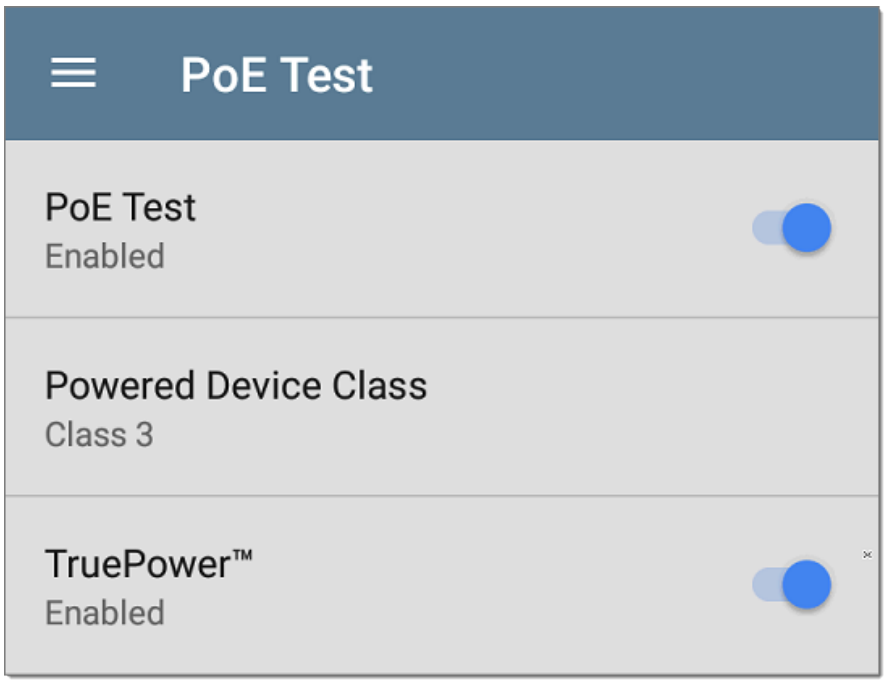
On the **Wired Profile** settings screen, tap each field described below as needed to configure the profile. Changed settings are automatically applied. When you finish configuring, tap the back button to return to the profile.

Name

Tap the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Wired Profile screen header.

PoE Test Settings

Open PoE Test settings to enable or disable PoE and configure the PD Class.



PoE Test

Tap the toggle button to enable or disable the PoE test portion of the current Wired Profile.

Powered Device Class

Tap to select a PoE class setting to match your switch's (or active PoE injector's) available class. EtherScope supports these classes:

- 802.3af Classes 0-3
- 802.3at PoE+ Class 4
- Cisco's UPOE, which can provide up to 51 W
- 802.3bt Classes 5-8

Select **Passive PoE Injector** if you are using a non-IEEE injector.

> NOTE: EtherScope may not receive the total wattage advertised by your switch or injector because of power loss over the cable.
>
> NOTE: EtherScope automatically negotiates Cisco UPOE over LLDP, up to 51 W. LLDP must be enabled on the switch for negotiation to succeed. If the UPOE Class is selected on your EtherScope but LLDP is not

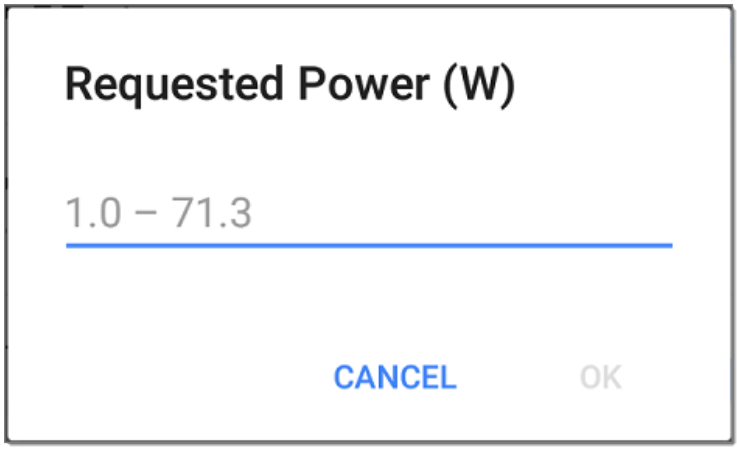
enabled on your Cisco switch, negotiation fails.

LLDP

This toggle button appears if Class 4 (25.50 W) is selected. Enable this setting if LLDP is enabled on the switch you are testing. Class 4 LLDP must be enabled on the switch for AutoTest to detect it successfully. If the LLDP setting is enabled but your switch does not support LLDP, negotiation fails.

Requested Power (W)

This setting appears if **UPOE** is selected in the **Powered Device Class** setting shown above or if the Powered Device Class is set to **Passive PoE Injector** and **TruePower** is enabled. Tap to enter a Requested Power other than the default, if needed. If you tap the backspace button on the pop-up number pad and clear the default value, the valid power range is displayed.



TruePower™

TruePower validates that the Switch (Power Sourcing Equipment) and cabling can provide the requested power under load by applying a load equivalent to the selected class to mimic a Powered Device (PD). Tap the toggle button to enable the TruePower feature.

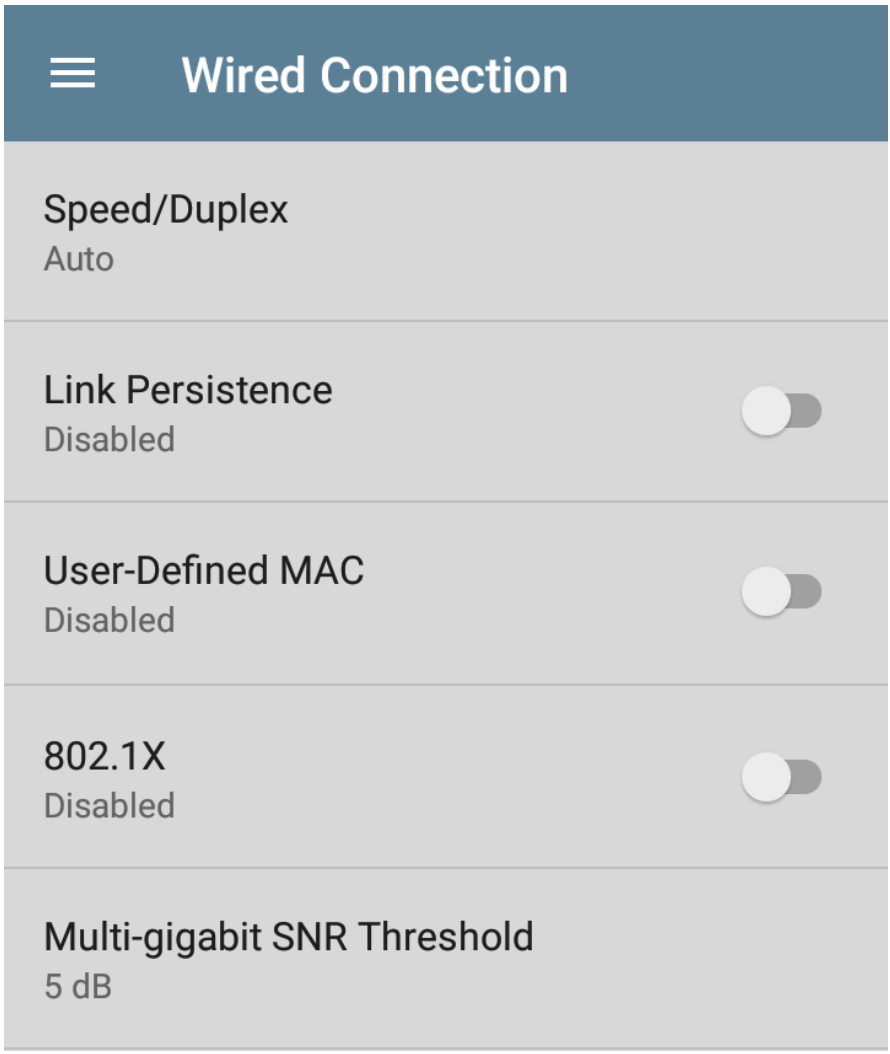
General Settings that Affect PoE

See the Wired section in General Settings for descriptions of the **Test PoE before Link** and **Charge Battery via PoE** settings, which also affects the PoE Test and function.

Wired Connection Settings

Open **Wired Connection** settings to configure speed/duplex, link persistence, user-defined

MACs, 802.1X settings, and multi-gigabit SNR threshold.



Speed/Duplex

Tap to select the speed and duplex option that you want to test your network against. The default is Auto negotiation.

When speed is set to Auto, EtherScope auto-negotiates to the highest possible speed/duplex

supported by the link partner. You can select a fixed speed/duplex for the copper interface. For 10 and 100 Mbps you can optionally force the speed and duplex.

This setting does not force the link speed/duplex on the fiber interface, but does control which speed is attempted first when using a multi-rate SFP. As a result, this setting can enable the test unit to connect faster via fiber.

Link Persistence

Link Persistence controls product behavior prior to link and also after link goes down.

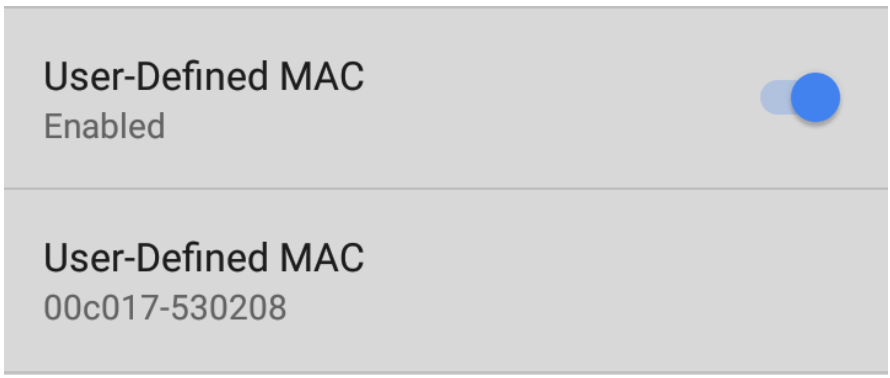
Link Persistence and Establishing Link: When enabled there is no timeout on how long to wait for link to be established. When disabled, the link step fail if not successful in 25 to 30 seconds.

Link Persistence and Link Dropping: When enabled and link drops, the unit attempts to relink. When disabled and link drops, the profile is considered done and no further link attempts are done until a Wired Profile is run again.

The default setting for Link Persistence is disabled.

User-Defined MAC

Tap the toggle field to enable a user-defined MAC for this profile and display the current user-defined MAC definition:



This setting affects the Wired Test Port only. Tap the toggle switch to enable a user-defined MAC address specifically for this profile. When enabled, an additional **User-Defined MAC** field appears under the toggle setting. (If there is no currently value for this profile, the field shows the user-defined MAC address (if any) defined in the " Wired" on page 103 section of the General Settings.) Tap the lower field to enter your desired MAC address for the EtherScope. When this user-defined MAC is enabled, **(User-defined)**

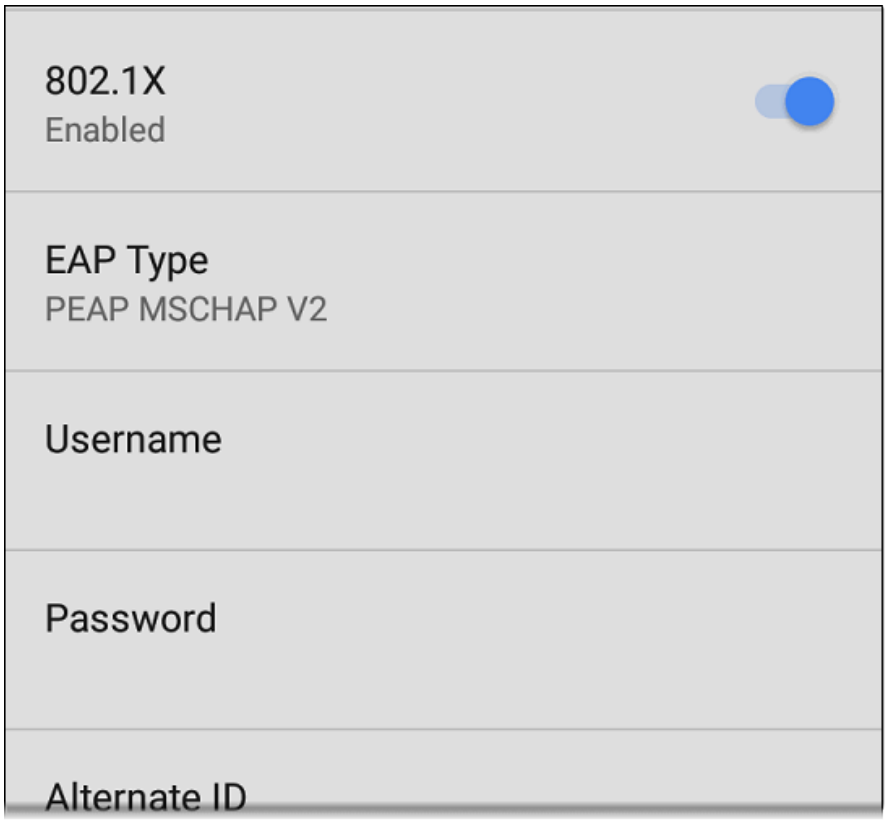
appears next to the MAC address on the About screen and on relevant test result screens.

You can use this feature for tasks such as testing ACL lists (for example, finding out if specific MAC addresses are allowed on the network) or for determining if specific IPv4 addresses should be assigned to specific MAC addresses.

802.1X

Tap the toggle field to enable wired 802.1X authentication in the current Profile. Enabling this setting also enables an 802.1X test card on the Wired AutoTest results screen.

The following settings appear when 802.1X authentication is enabled. Enter all necessary credentials, such as EAP type, username and password, or certificate.



EAP Type

Tap to select a different EAP type if needed. The default is PEAP MSCHAP V2.

Certificate

This setting appears if one of the following EAP types is selected in the setting above: **EAP TLS**, **PEAP TLS**, or **TTLS EAP TLS**.

See How to Import a Certificate.

Username

This field appears along with multiple authentication types. Tap the **Username** field to enter your username.

Password

This field appears along with multiple authentication types. Tap the **Password** field to enter the network password.

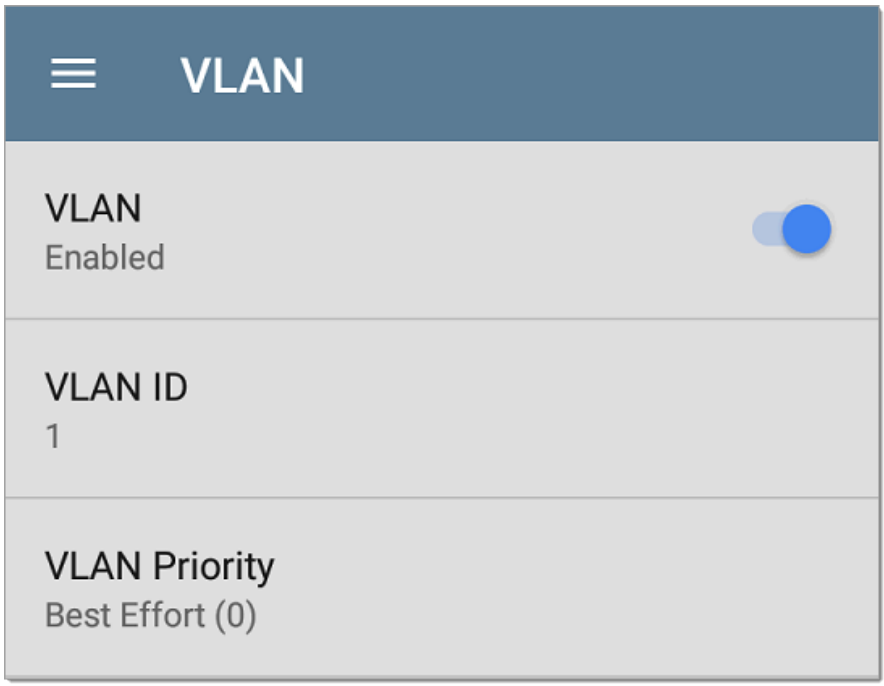
Alternate ID

Enter an Alternate ID if necessary. This is an Advanced Authentication setting.

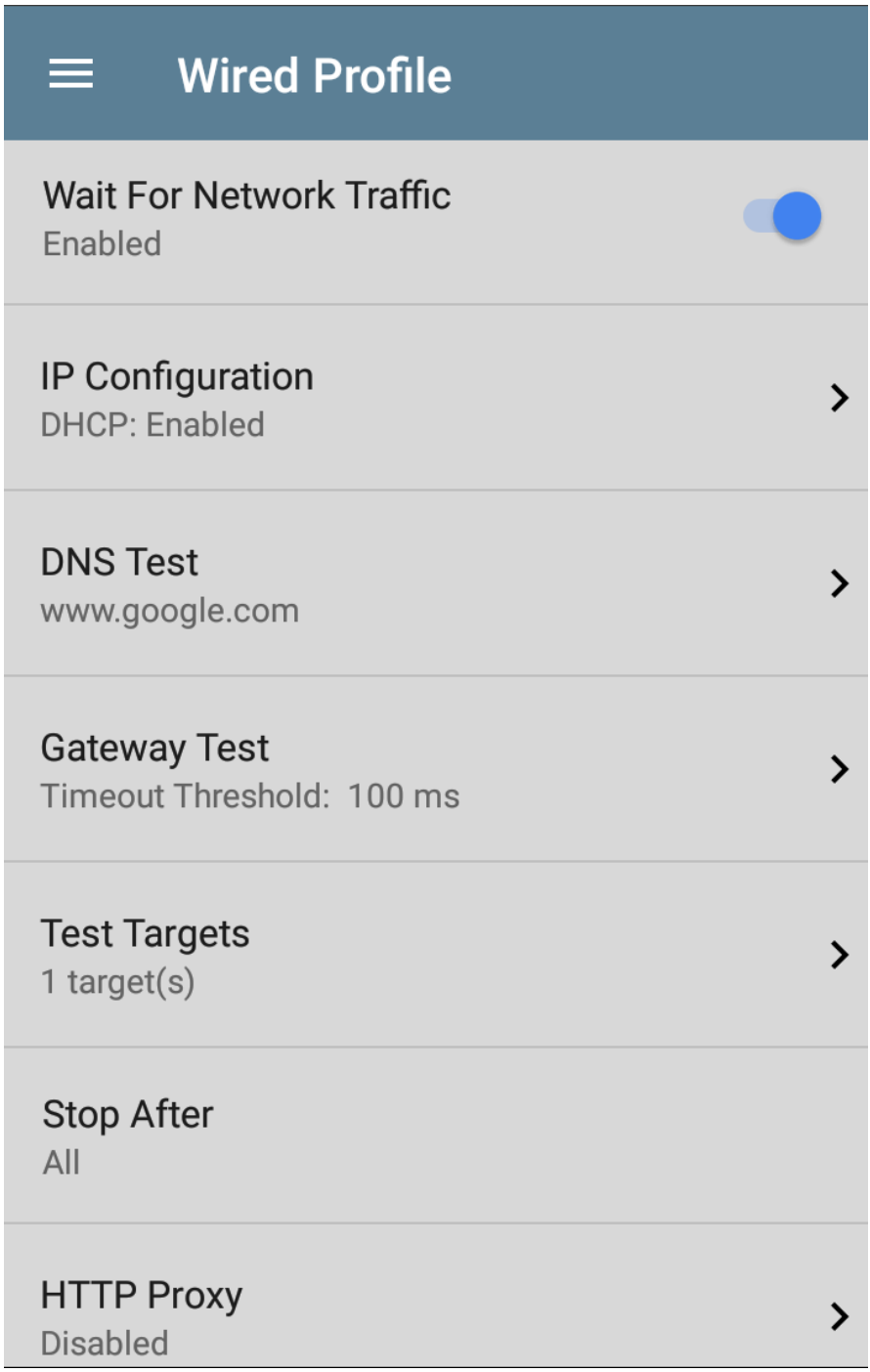
Multi-gigabit SNR Threshold

When a Wired Profile links at speeds higher than 1 Gbps, a table appears on the Link Test screen showing Multi-gigabit Details. This threshold grades SNR measurements on the four twisted pairs. A Minimum SNR below the selected threshold displays a yellow warning condition. The default is 5 dB. If more than one signal is below the Minimum SNR, the signal with the lowest value is shown.

VLAN Settings



Tap to open the VLAN settings screen. Slide the toggle to the right to enable VLAN testing. Enabling this setting also enables a VLAN test card on the Wired AutoTest results screen. Once enabled, **VLAN ID** and **VLAN Priority** fields appear. Tap these fields to open a pop-up number pad and enter the correct ID and priority. Tap **OK** to save them.



Wait For Network Traffic

Wait for Network Traffic controls whether there is any delay after link comes up before proceeding to the next step. When enabled there

is a delay waiting for packets to be forwarded from the network by the nearest switch. This is useful for switches that are configured to search for networking loops prior to forwarding traffic. On networks with very little traffic, the user may choose to disable this delay. The maximum time to delay is 45 seconds.

DHCP, DNS, and Gateway Settings

Settings for these tests operate the same in both Wired and Wi-Fi profiles.

See DHCP, DNS, and Gateway Tests for Wired and Wi-Fi.

PING FTP TCP HTTP Test Targets

Tap the **Test Targets** field to open the Test Targets screen and add custom Ping, TCP Connect, HTTP, or FTP tests to your AutoTest profile.

See Test Targets for Wired and Wi-Fi Profiles.

Stop After

This setting directs the Wired Profile to stop testing after the selected test step (**Link**, **Switch**,

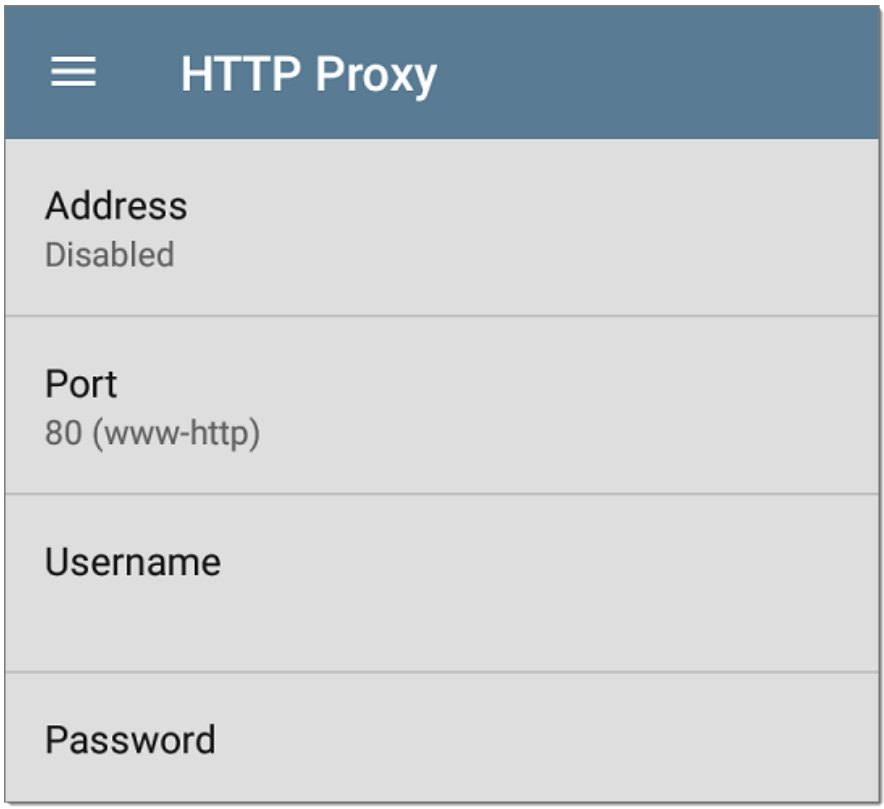
DHCP, **DNS**, **Gateway**, or **All**). The excluded test cards do not appear on the Profile results screen.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the EtherScope establishes a network connection. In AutoTest, these settings are used when HTTP Proxy is enabled in an HTTP or FTP Test Target.

To use the proxy settings with a web browser, run the Profile, and then, open the web browser while the unit remains linked.

Open the **HTTP Proxy** screen to enable proxy settings.

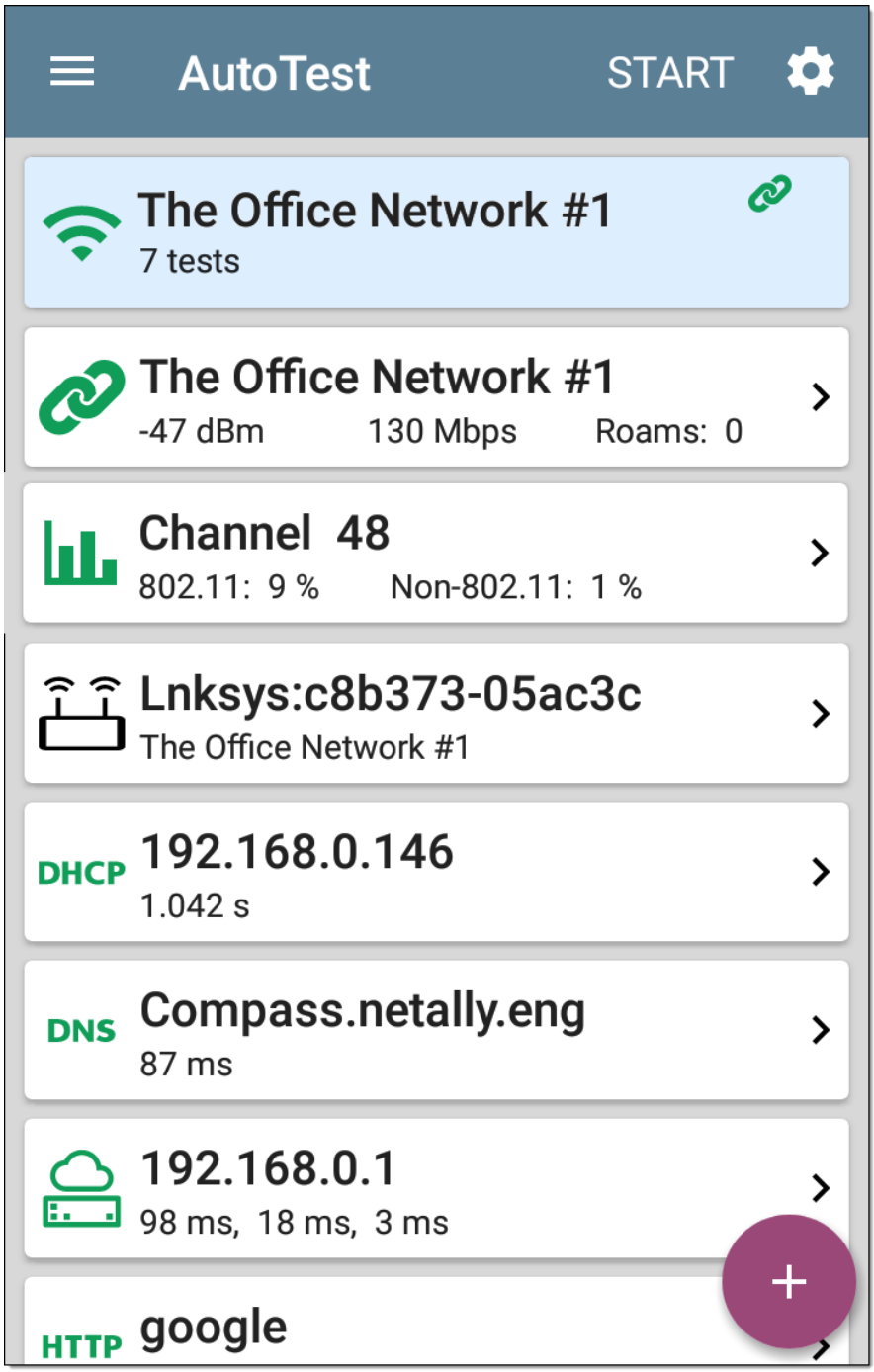


Tap each field to open a pop-up keyboard and enter the appropriate **Address**, **Port**, **Username**, and **Password**. Tap **OK** to save your entries.

Back to Title and Contents

Wi-Fi AutoTest Profiles

A Wi-Fi Profile runs a series of tests by connecting to a selected wireless network.



Like the main AutoTest screen, Wi-Fi Profile tests are summarized on cards. Tap a card to view individual test screens.

Each test icon (except the AP) displays green, yellow, or red to indicate the status (or grade) of the completed test step: **Success**/**Warning**/**Fail**. The AP Test card shows the name and SSID of the connected AP. The AP test is not graded, so the icon stays black.

Wi-Fi Profiles do not run automatically. The factory default Wi-Fi Profile cannot run until you have configured an SSID with the proper credentials. (By default, AutoTest starts in Wi-Fi passive scanning mode if you do not have a profile set up.)

See the Wi-Fi Profile Settings topic for instructions.

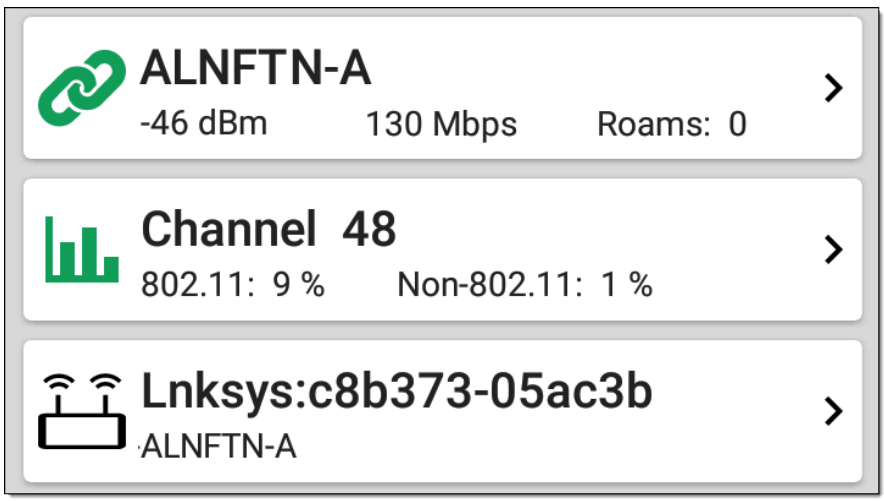
After connecting to a network during a Wi-Fi connection test, EtherScope nXG remains connected until you run another Wi-Fi or Air Quality Profile or open the Wi-Fi app. Wi-Fi Test

Port linkage is indicated in the top Status Bar with this notification icon,  , which also shows the connected channel.

> NOTE: When running an AutoTest Profile that connects to a network with a Captive Portal, a system notification icon  appears in the top Status Bar. Open and select the notification to open a web browser window where you can enter the required information for the captive portal.

Wi-Fi-Profile-Specific AutoTests

The tests that are specific to a Wi-Fi Profile include the wireless Link, Channel, and AP tests.



The link and channel cards update in real time to display the connection measurements for as

long as EtherScope remains connected to the wireless network.

Link (Connection), Channel, and AP Results are described next.

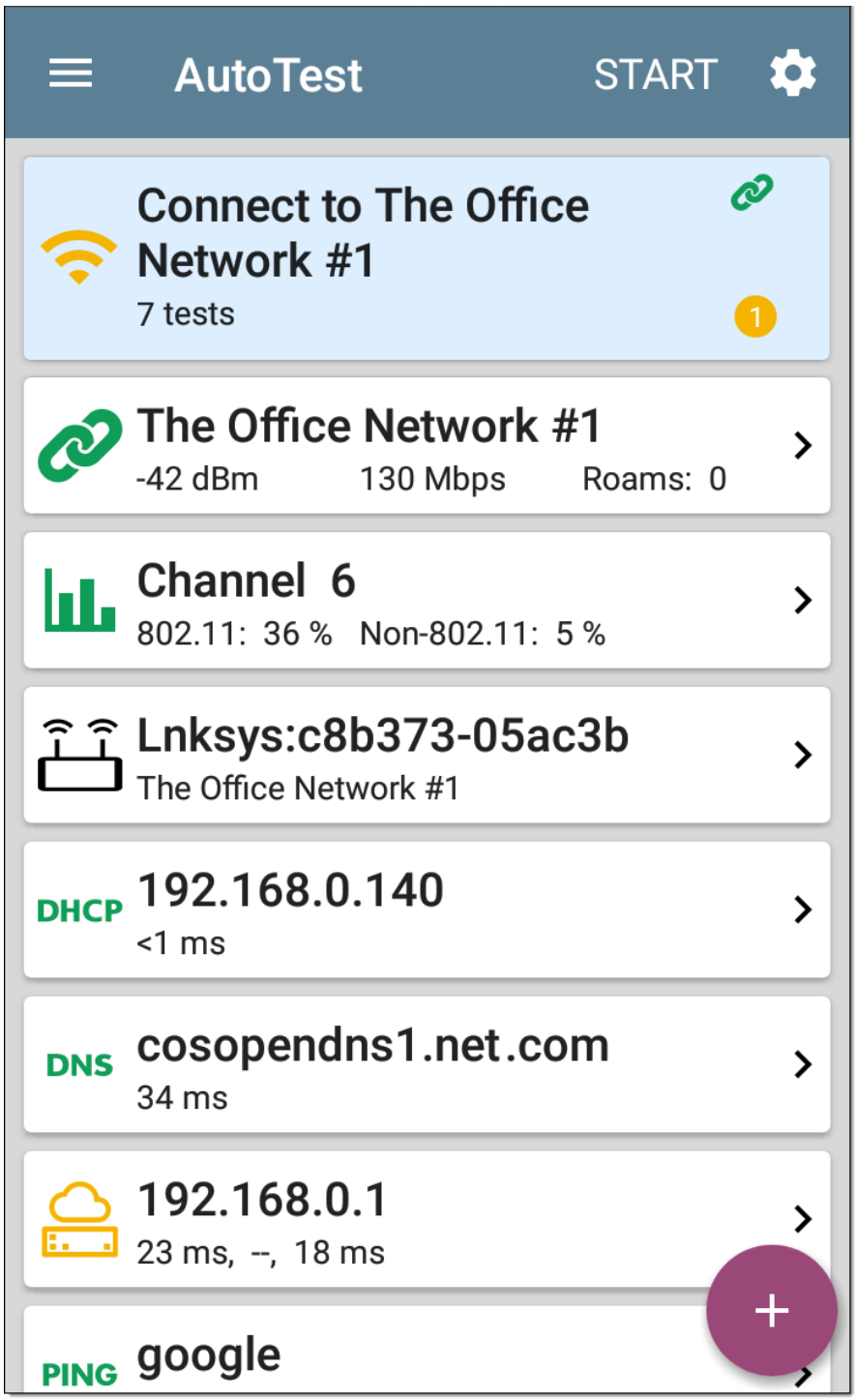
Skip to Wi-Fi Profile Settings.

Skip to DHCP, DNS, and Gateway Tests.

Skip to Test Targets.

Wi-Fi Profile Results

The image below shows a completed AutoTest Wi-Fi Profile.



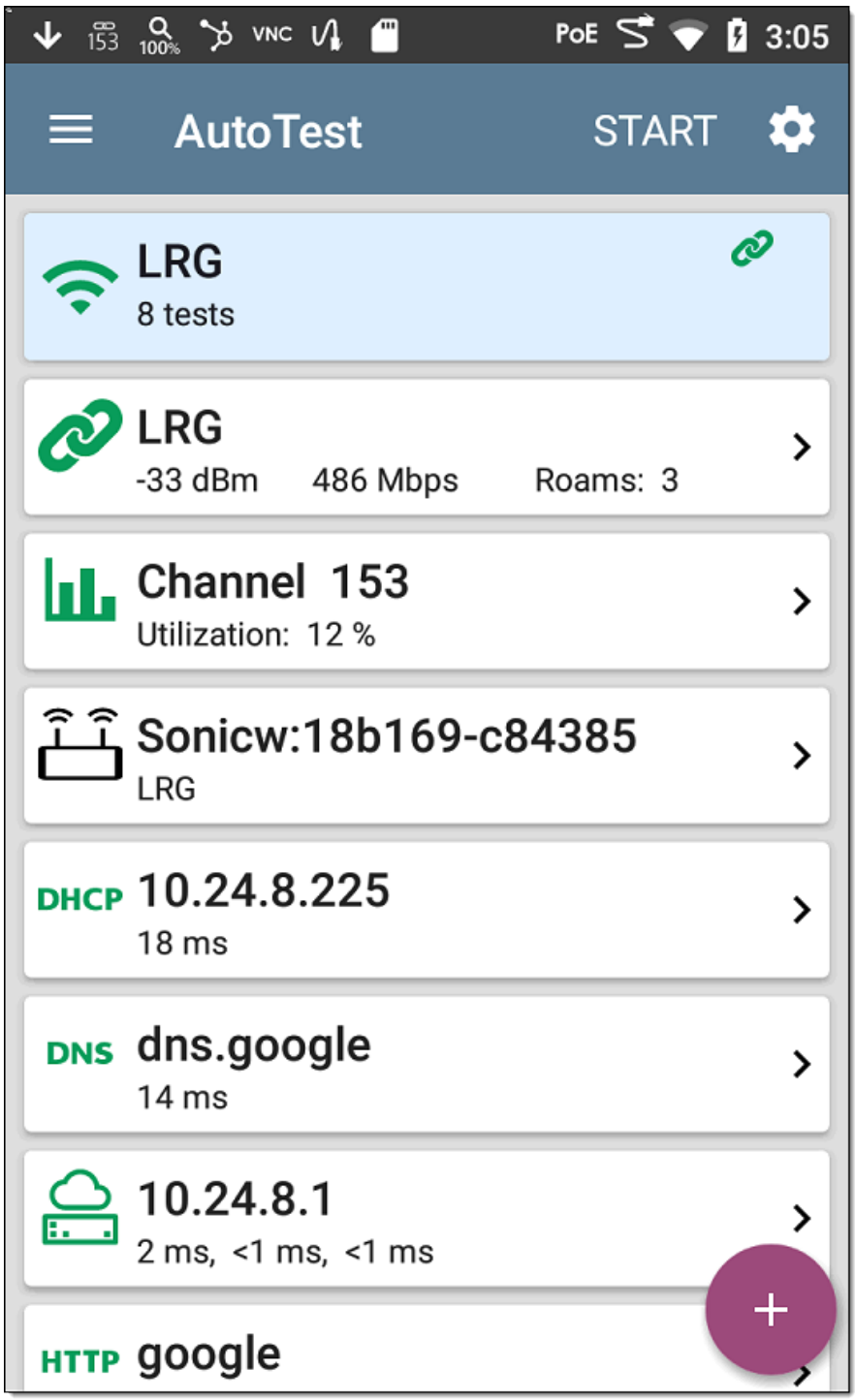
This Profile connects to SSID "The Office Network #1." The Profile is displaying one **Warning** condition from a timeout of the second Gateway ping.

On the Wi-Fi Profile screens, you can perform these actions:

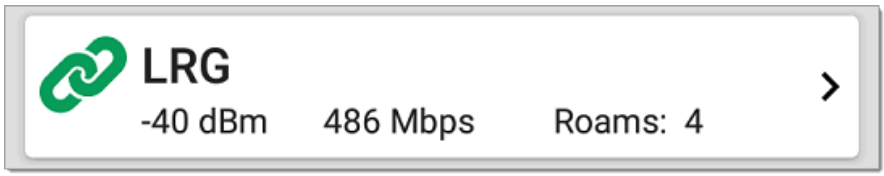
- Tap any of the test result cards, like Link , Channel, or AP, to open the individual test result screens.
- From any individual test screen, tap the settings icon to go directly to the settings for the current test.
- On individual test screens, tap **blue underlined links** to open a Wi-Fi app Details screen showing the selected device or ID.
- Tap other **BLUE LINKS** or the action overflow icon ••• at the bottom of test results screens for additional actions.

  NOTE: Blue links and action icons do not appear on every test screen, and if the network connection is dropped, you may need to rerun the Profile to re-establish link and enable additional actions.

The rest of this topic describes the individual test cards and screens using the Wi-Fi Profile results for the "LRG" SSID shown below.



Wi-Fi Link Test Results

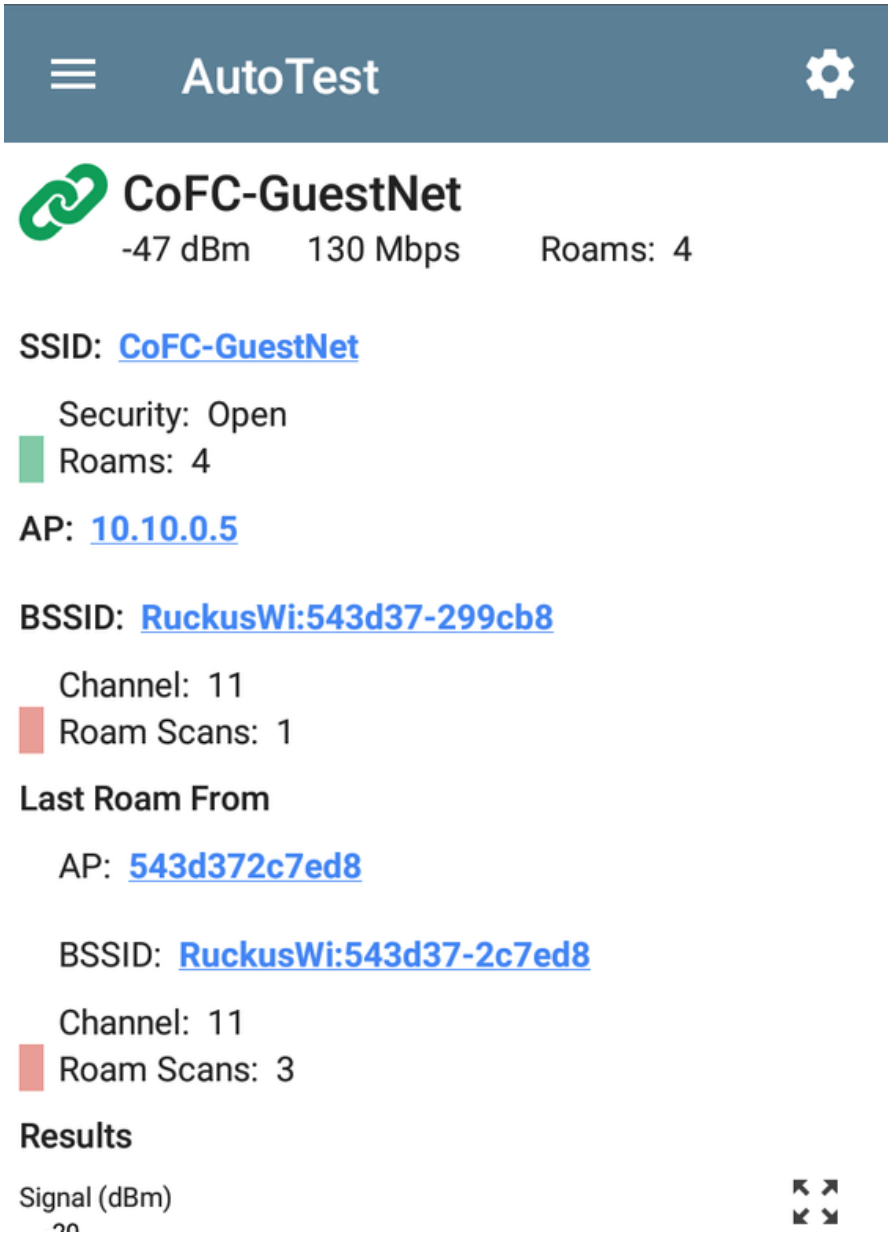


The Wi-Fi link test card indicates whether you can connect to the configured network at your current location. The Wi-Fi Link card displays the SSID, current signal strength (dBm), link speed (Mbps), and number of roams.

Refer to Wi-Fi Connection Settings if needed.

Tap the card to open the Link test screen.

Wi-Fi Link Test Screen



The Wi-Fi Link test screen shows these results:

SSID

Security: Security protocol in use on the network

Roams: Number of times the unit has disconnected from the previous AP and connected to a different AP with a better signal strength. This behavior is partly controlled by the **Roam Threshold** in the Wi-Fi Connection settings.

AP: Name, IP, or MAC address of the AP to which the Tester is connected, depending on the information EtherScope can see about the AP. This field shows the custom User Name if one has been entered. See Assigning a Name and Authorization to a Device in the Wi-Fi app chapter.

BSSID: BSSID of the access point

Channel: Channel number on which the AP is operating

Roam Scans: (EXG-200 only) Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause EtherScope to scan for another AP, such as low signal strength or high retry rate.

Last Roam From: If the EtherScope has roamed to a new AP, the previous AP's name, BSSID, and Channel display.

AP: Channel number on which the AP is operating

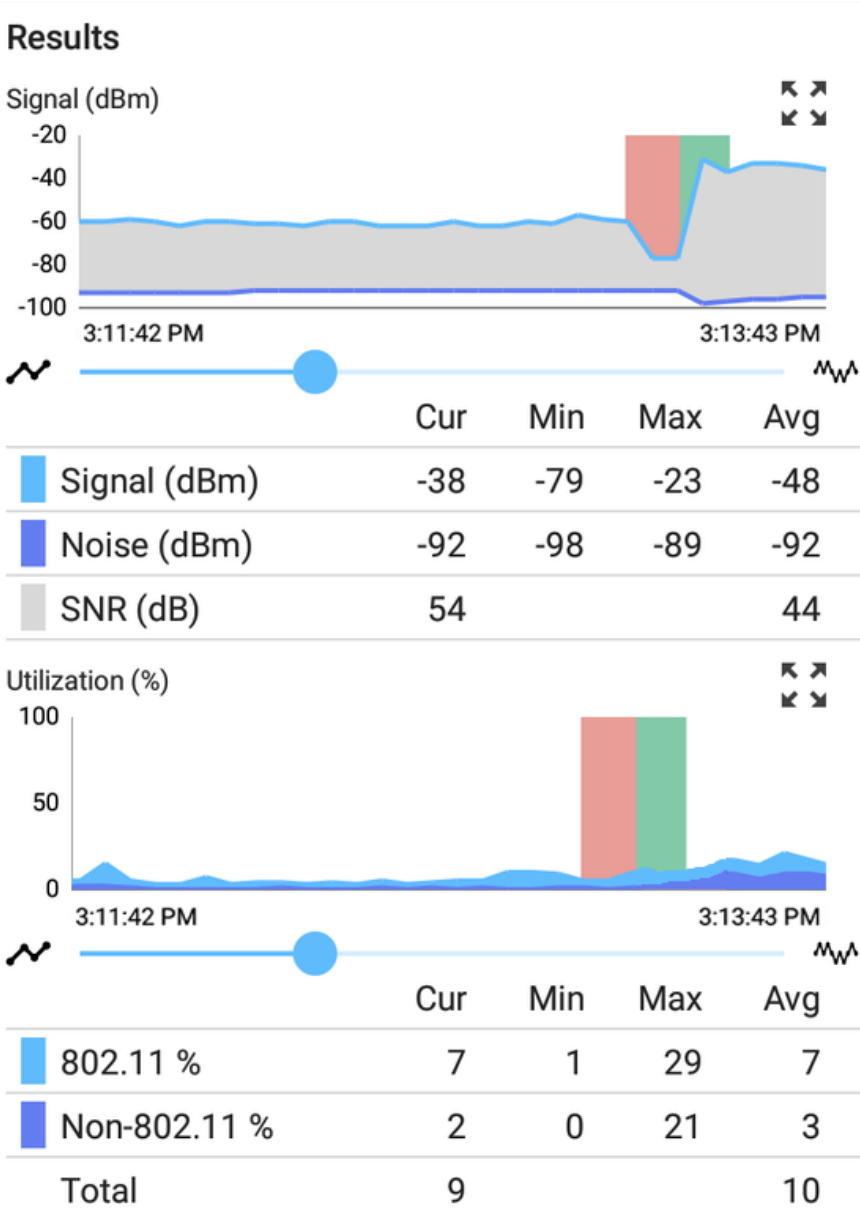
BSSID: BSSID of the access point

Channel: Channel number on which the AP is operating

Roam Scans: (EXG-200 only) Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause EtherScope to scan for another AP, such as low signal strength or high retry rate.

Wi-Fi Link Trending Graphs

EtherScope's trending graphs operate similarly across different testing apps, allowing you to pan and zoom to view different time intervals. Swipe, double tap, and move the slider to adjust the graph views. See the Trending Graphs topic for an overview of the controls.



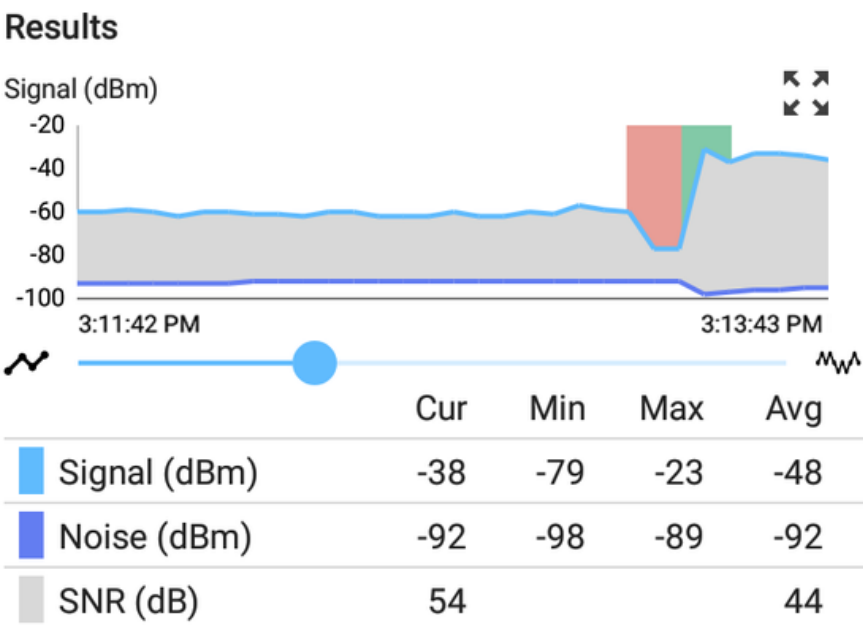
The Wi-Fi Link Test graphs save and display data for up to 24 hours in the past if the unit stays linked. The default time interval shown is 2 minutes.

Under each graph, a legend table displays the Current, Minimum, Maximum, and Average measurements. The Current column contains

measurements from the last second. Min, Max, and Avg columns show cumulative measurements.

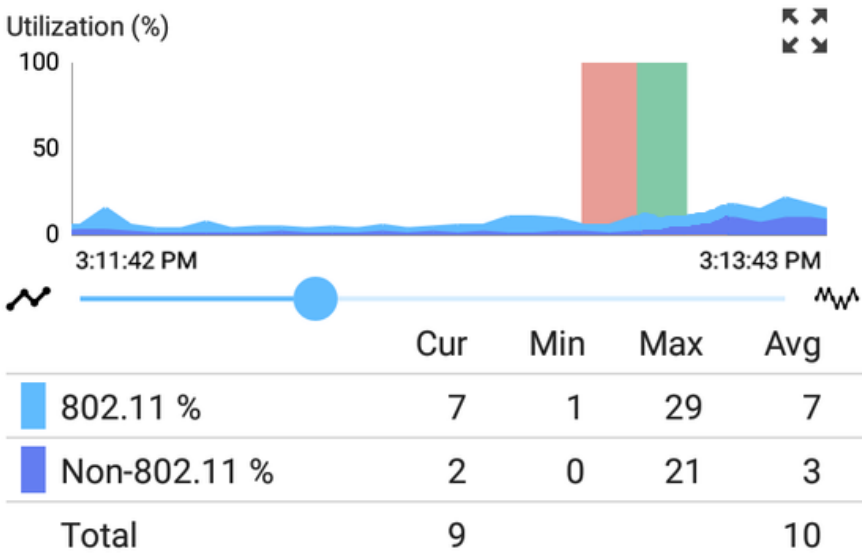
Signal (dBm) graph: Plots the signal strength in dBm of the connected AP.

- Green vertical bars - The tester roamed to a new AP.
- Red vertical bars - (EXG-200 only) The tester made a roam scan.
- Signal - The AP's signal strength in dBm.
- Noise - The noise level in dBm on the channel used.
- SNR - The network's signal-to-noise ratio in decibels (dB).



Utilization (%) graph: Plots percentage of the connected channel's capacity being used by 802.11 devices and by non-802.11 interference.

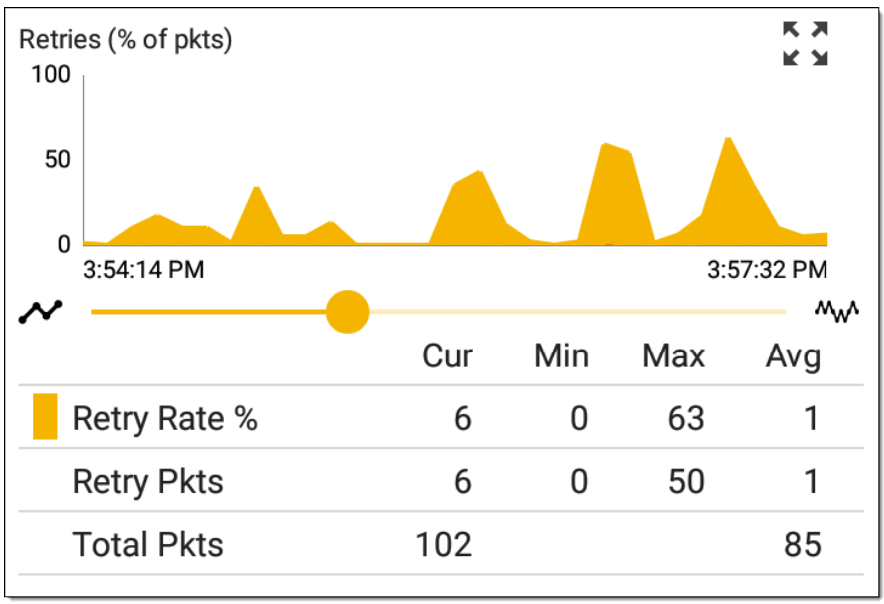
- Green vertical bars - The tester roamed to a new AP.
- Red vertical bars - (EXG-200 only) The tester made a roam scan.
- (EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows only combined 802.11 and non-802.11 channel utilization. See the General Settings topic for more information.



	Cur	Min	Max	Avg
802.11 %	7	1	29	7
Non-802.11 %	2	0	21	3
Total	9			10

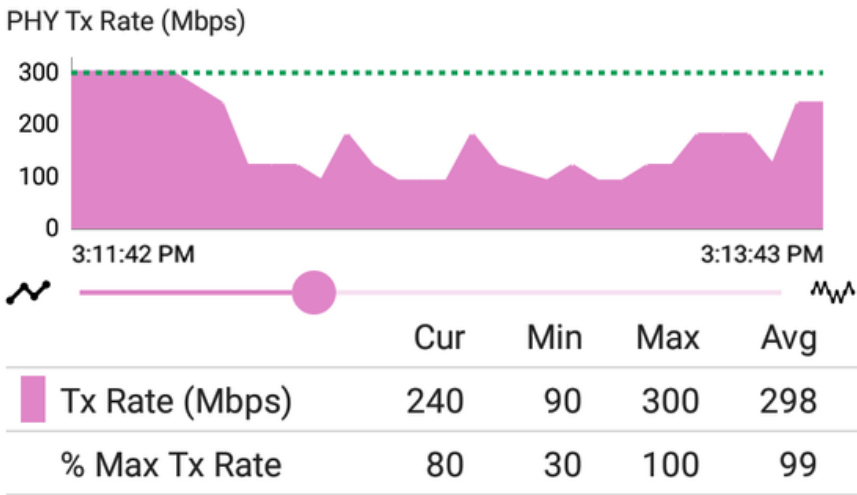
Retries (% of packets) graph: Plots percentage of transmitted packets that are retry packets

- Retry Rate % - The percentage of total packets that are retry packets.
- Retry Pkts - The number of retry packets seen in the current sample cycle.
- Total Pkts - The total number of packets transmitted in the current sample cycle.



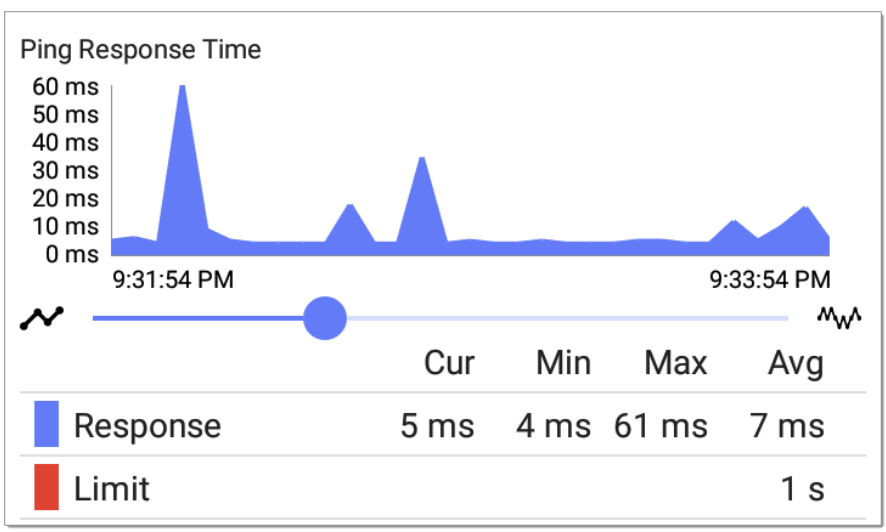
	Cur	Min	Max	Avg
Retry Rate %	6	0	63	1
Retry Pkts	6	0	50	1
Total Pkts	102			85

PHY TX Rate (Mbps) graph: Plots the physical transmission rate. The green horizontal dotted line shows the AP's maximum TX rate.



	Cur	Min	Max	Avg
Tx Rate (Mbps)	240	90	300	298
% Max Tx Rate	80	30	100	99

Ping or TCP Connect Response Time graph: This graph displays on the Link test screen if you run a Ping or TCP Connect test, using the Ping/TCP app, over the Wi-Fi test port connection while the Profile is linked.



	Cur	Min	Max	Avg
Response	5 ms	4 ms	61 ms	7 ms
Limit				1 s

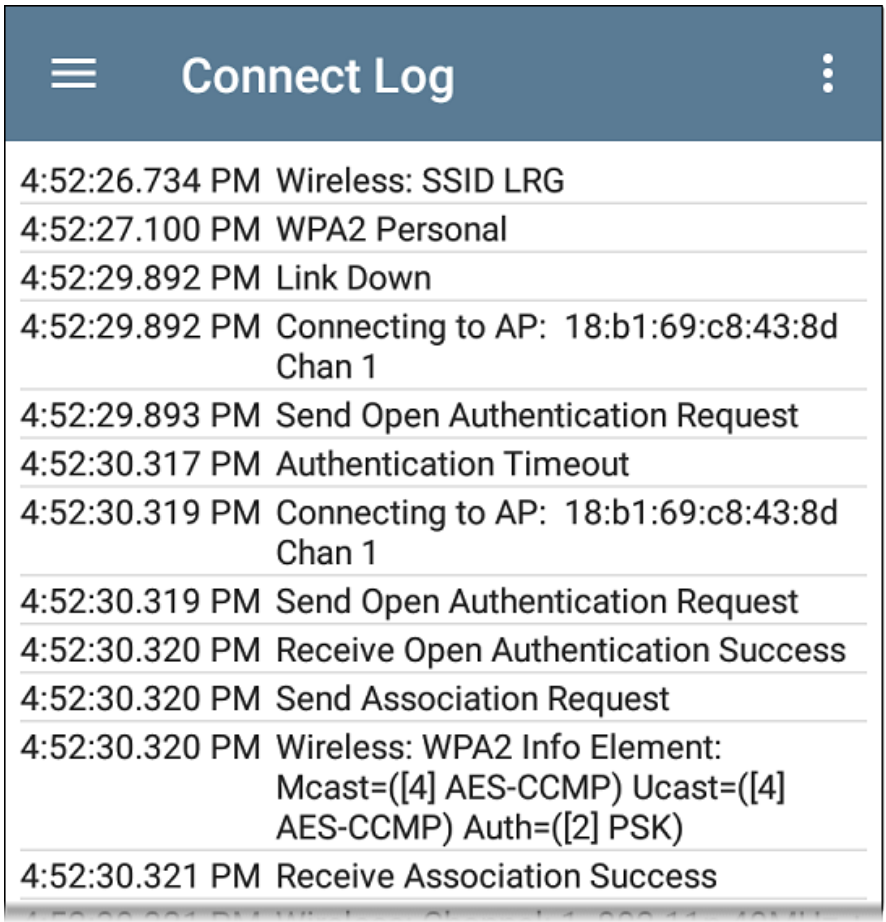
Follow these steps to view the Response Time graph:

1. Tap the blue **PING** hyperlink at the bottom of the Link test screen. This opens the Ping/TCP app with the **Interface** set to Wi-Fi Port and **Protocol** set to Ping.
2. Access and adjust the Ping/TCP settings as desired.
3. **START** the Ping or TCP Connect test.
4. Tap back  to go back to the AutoTest Wi-Fi Link screen. The Response Time graph appears near the bottom of the screen and updates in real time along with the other graphs for the duration of the Ping/TCP test.

Result Codes: Final status of the test (Success or Failure)

Tap the blue links at the bottom of the link test screen to open the Ping/TCP app, view the **CONNECT LOG**, or run a Wi-Fi packet **CAPTURE** on the connected channel and AP.

Connect Log



The Connect Log shows the Wi-Fi connections, including driver activity, supplicant, and the DHCP process. The Connect Log can be especially helpful for identifying linking or roaming problems.

Select the action overflow icon ⋮ at the top right on the Connect Log screen to attach the log to its associated AutoTest result on the Link-Live website, or attach the Connect Log from the

floating action menu + on the main Profile screen. See Wi-Fi Profile FAB below.

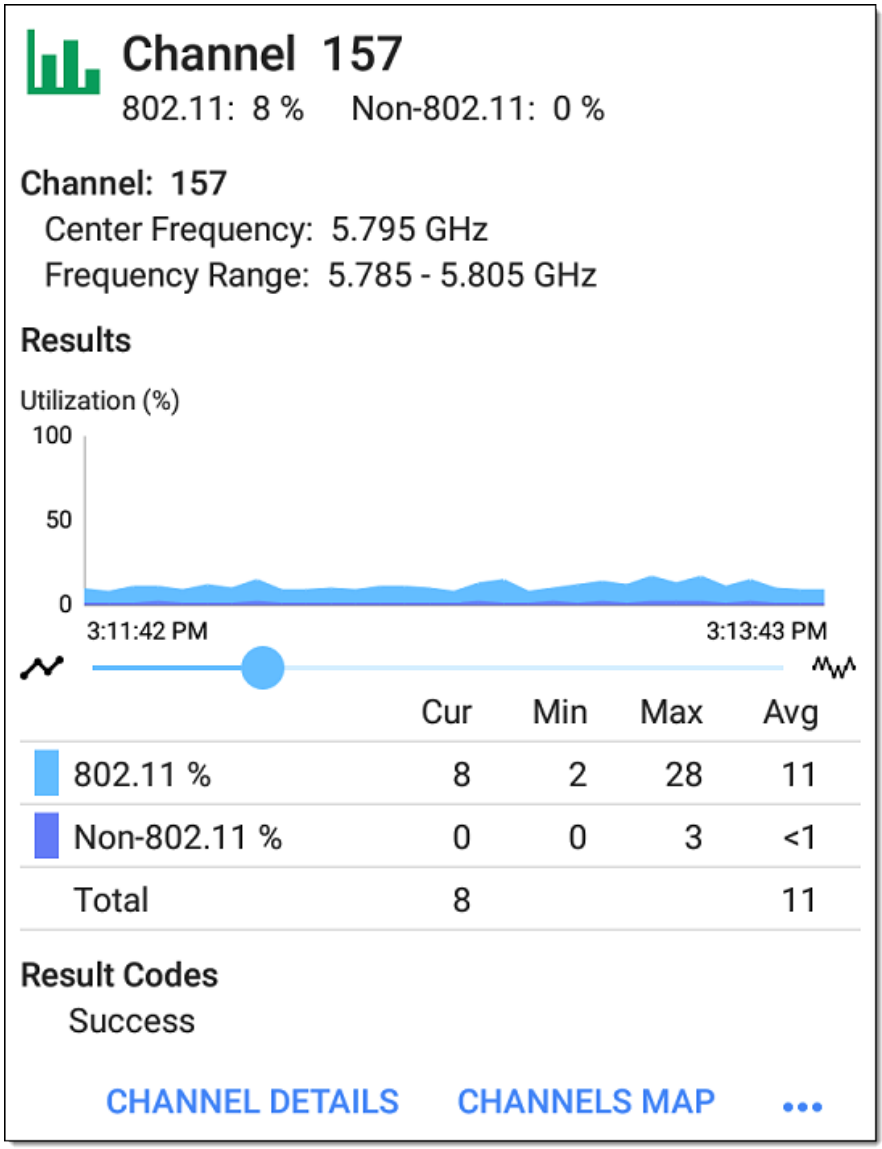
Channel Test Results

The Channel card shows the channel on which the AP is operating and the current 802.11 and Non-802.11 utilization.

(EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, the card shows only combined 802.11 and non-802.11 channel utilization. See the General Settings topic for more information.

Refer to Channel Test Settings if needed.

Channel Test Screen



The Channel Test results screen indicates the **Center Frequency** and **Frequency Range** of the connected channel along with a real-time Utilization graph.

Results: The channel Utilization (%) graph updates in real time for as long as the unit is still

connected to the network. The graph saves and displays data for up to 24 hours if the unit stays linked.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

Utilization (%) graph: Plots percentage of the connected channel's capacity being used by 802.11 devices and by non-802.11 interference

- **802.11 %**: Percentage of channel capacity being used by 802.11 devices
- **Non-802.11 %**: Percentage of channel capacity being used by non-802.11 interference
- **Utilization**: (EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows only combined 802.11 and non-802.11 channel utilization.
- **Total**: Total percentage of both 802.11 and non-802.11 channel utilization

Results Codes: Final status of the test (Success or Failure)

Tap the blue links at the bottom of the channel test results to open the Wi-Fi app's **CHANNEL DETAILS** or **CHANNELS MAP** screens, or to run a Wi-Fi packet **CAPTURE** on the connected channel.

AP (Access Point) Test

The AP card shows the AP's name and the SSID of the network it is supporting. The AP name or address shown is based on what the EtherScope is able to gather from the device and network. If the AP has a custom user name, that name is shown on the card and test screen.

The AP test is not graded, so the icon remains black.

Back to Title and Contents

AP Test Screen

In addition to the AP name and SSID, the AP test screen shows the following:

Device Name: AP's name or address

IP Address: The AP's assigned IP address. If none could be determined, the field displays dashes --.

MAC Address: The AP's MAC address

SSID: Name of the network on which the AP is operating

Security: Security protocol in use on the network

Roams: Number of times the unit has roamed and connected to a different AP

802.11

Channel(s): Channel or channels the AP is operating on. If the BSSID is on multiple channels, the **bold** channel number indicates the primary channel.

Type: 802.11 type in use on the current link

Supported Types: 802.11 types that the BSSID supports. If none could be determined, the field displays dashes --.

Client Associations: The number of client devices connected to the AP

Roam Scans: (EXG-200 only) Number of times the EtherScope has scanned for a new AP supporting the same SSID. Multiple triggers may cause EtherScope to scan for another AP, such as low signal strength or high retry rate.

Tap the blue links at the bottom of the link test screen to view the **CONNECT LOG** or run a **PATH ANALYSIS** to the AP.

Open the overflow menu ••• for additional actions, such as to run a Wi-Fi packet **CAPTURE** on the connected channel and AP, or start a Telnet or SSH session using the AP's IP address.

DHCP, DNS, and Gateway Results

Results for these tests operate the same in both Wired and Wi-Fi profiles.

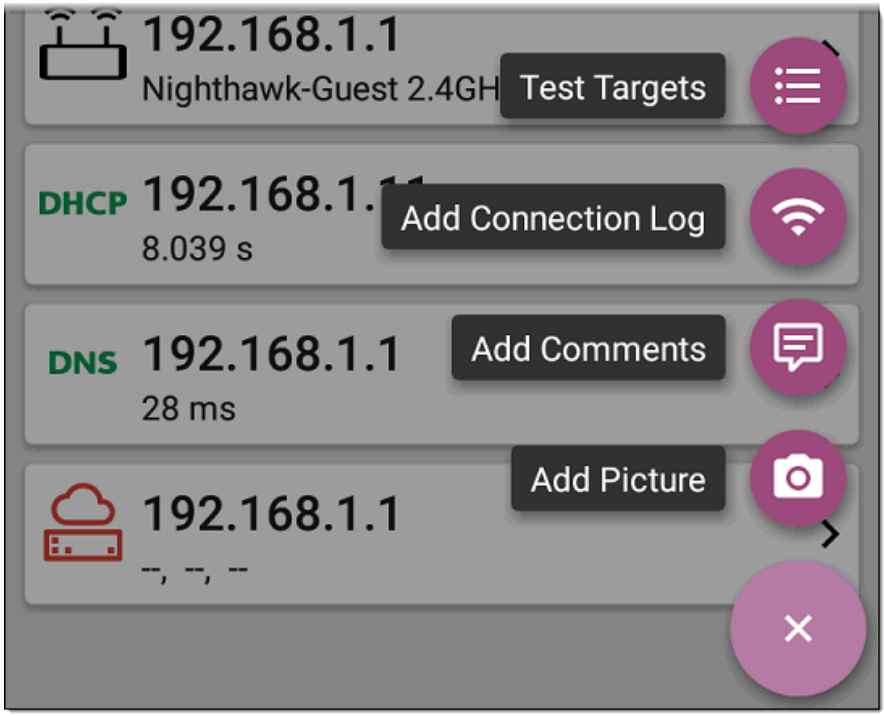
See DHCP, DNS, and Gateway Tests.

PING FTP TCP HTTP Target Tests

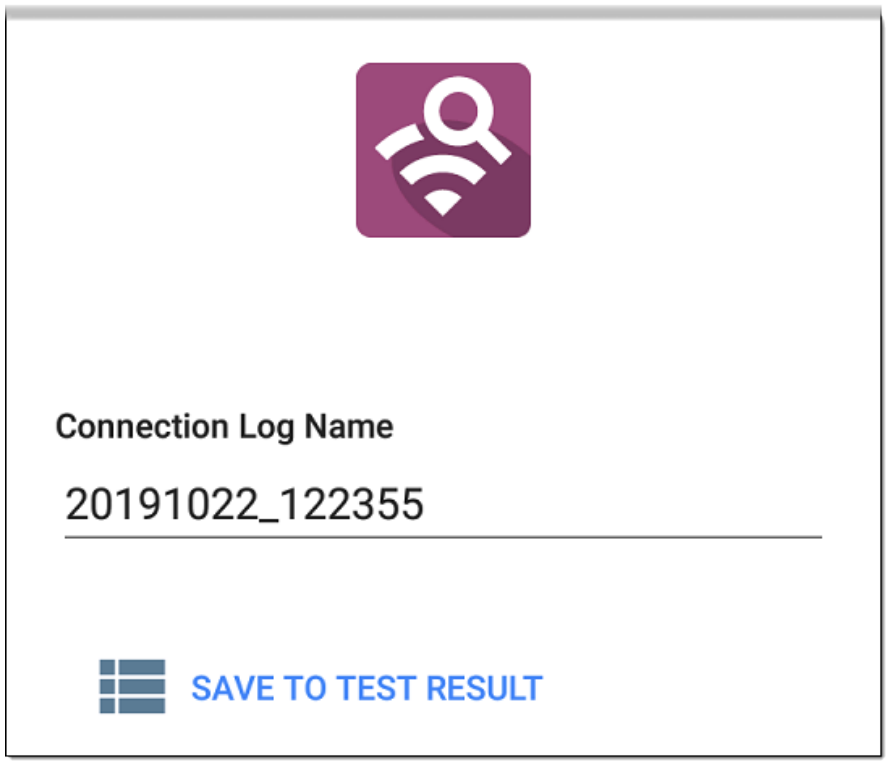
See the Test Targets topic for information on target test results.

Wi-Fi Profile FAB

The floating action button (FAB) on the Wi-Fi Profile AutoTest Profile screens allows you to attach comments, an image, and the Connect Log to this AutoTest result on the Link-Live website.

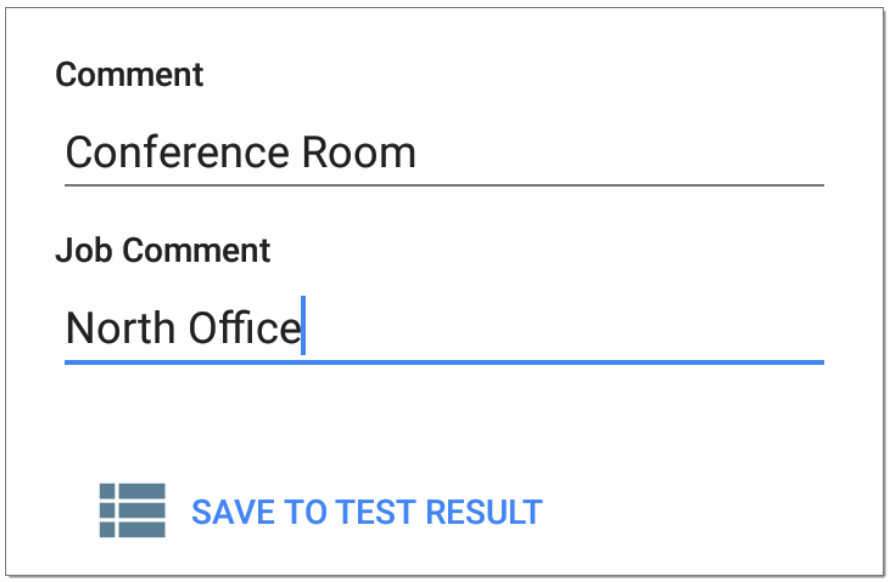


- The **Test Targets** option opens the Test Targets screen, where you can add Ping, TCP Connect, HTTP, and FTP target tests to the current profile.
- **Add Connection Log** opens a Link-Live sharing screen that allows you to custom name the log file before saving to the test result.



Tap the field to enter your desired log name, and tap **SAVE TO TEST RESULT** to upload.

- **Add Comments** also opens a Link-Live sharing screen where you can enter comments.



Tap the fields to enter your desired comments, and tap **SAVE TO LAST TEST RESULT** to upload them.

- The **Add Picture** function lets you open the **Gallery** or **Camera** app to select or take a photo that is then uploaded and attached to your test result.

See the Link-Live App chapter to learn about Link-Live and uploading.

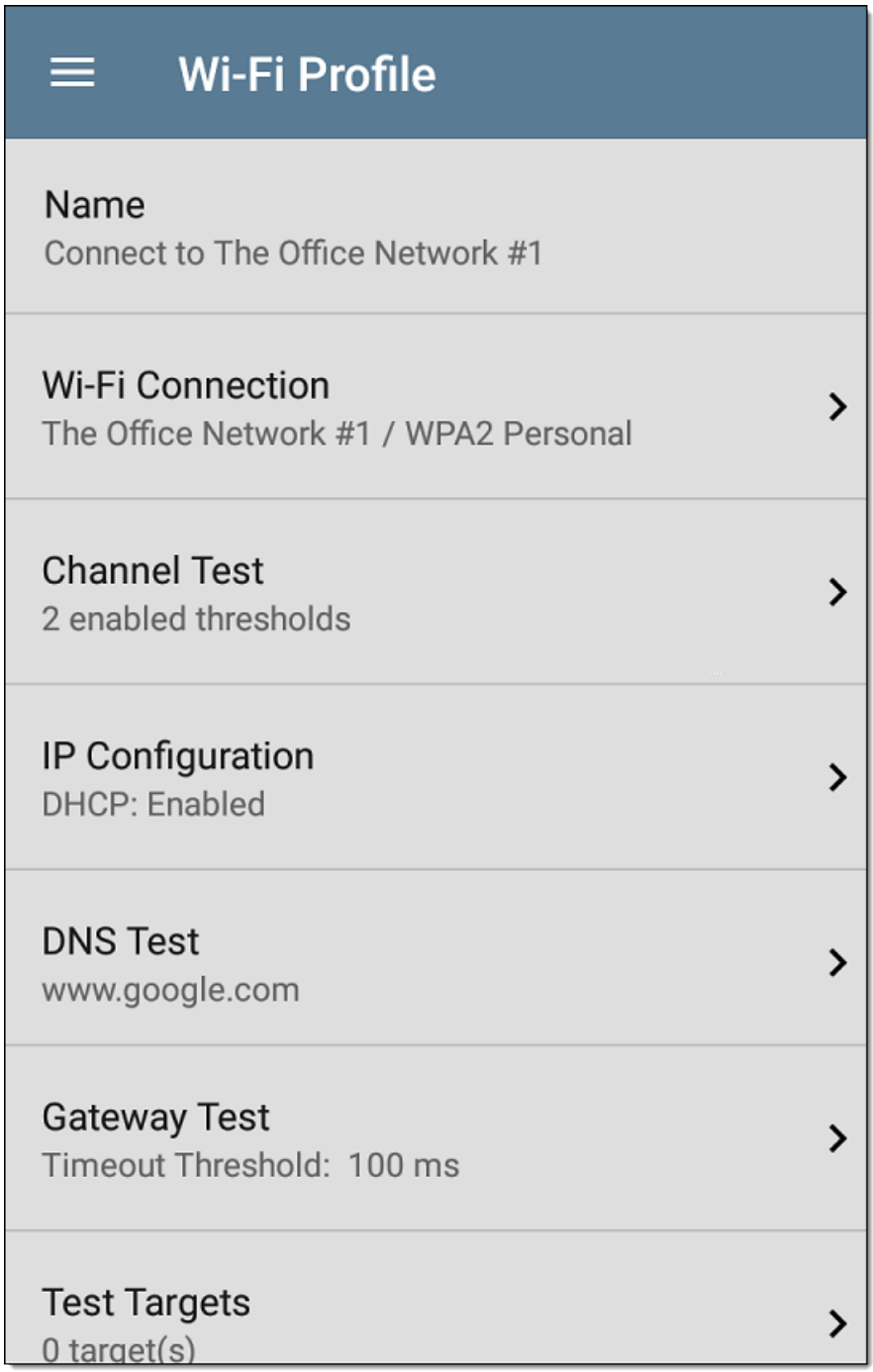
Back to Title and Contents

Wi-Fi Profile Settings

These settings control which network is tested, how the EtherScope nXG connects, thresholds for **Success**/**Warning**/**Fail** results, and any user-added test targets.

To configure the profile settings, tap the settings icon  on the Wi-Fi Profile screen, or add a new Wi-Fi Profile to AutoTest.

Tap the links below to skip to later sections in this topic:



On the **Wi-Fi Profile** settings screen, tap each field described below as needed to configure the profile. Changed settings are automatically applied.

NOTE: If you add a new Wi-Fi profile from the Wi-Fi Analysis app, the Profile Name, SSID, and Authentication type are auto-populated. See Creating a Wi-Fi Profile from the Wi-Fi Analysis App.

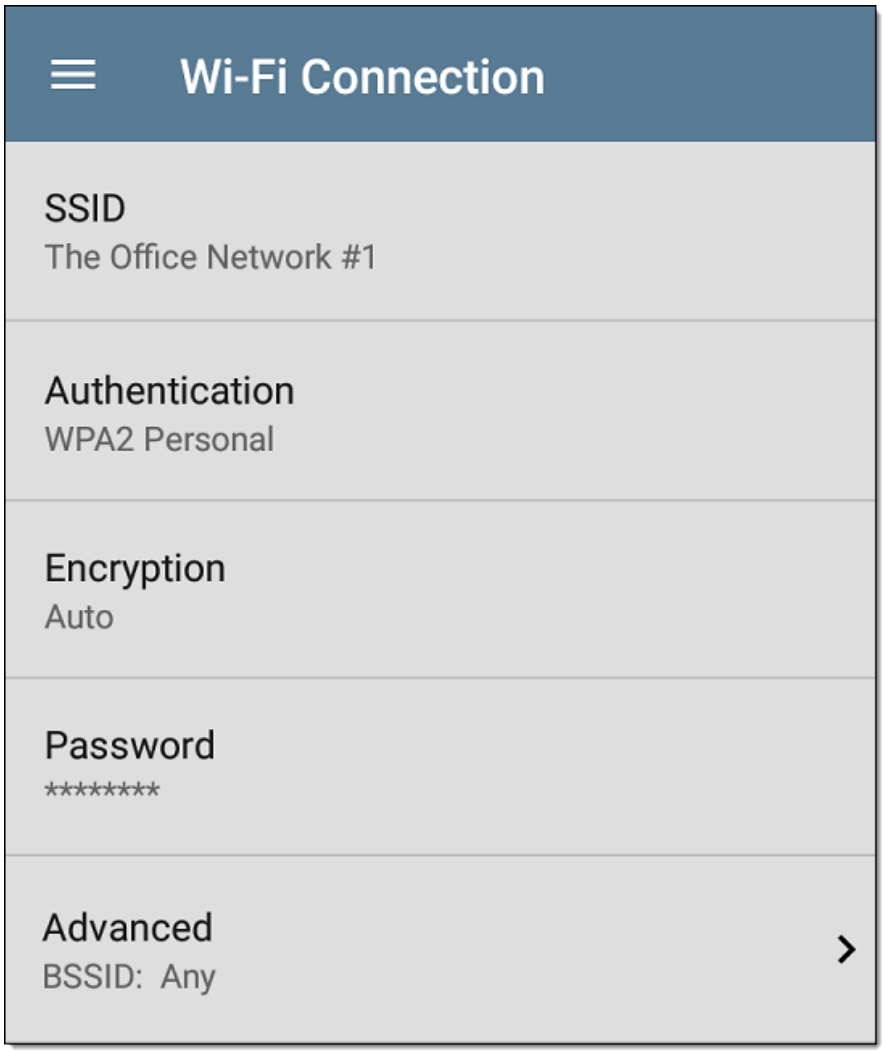
When you finish configuring, tap the back button  to return to the profile.

Name

Tap the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Wi-Fi profile screen header.

Wi-Fi Connection Settings

Open **Wi-Fi Connection** settings to configure network IDs, security credentials, and test thresholds for the Link test. These settings control the Wi-Fi Test Port connection.



SSID

Tap to enter an **SSID** or select from the list of discovered SSIDs. If you do not enter a custom **Name** for the Profile, the SSID is displayed as the Wi-Fi Profile's name.

Authentication

If you selected an **SSID** from the drop-down list of discovered SSIDs in the setting above, or

created a "Connect to [SSID]" profile from the Wi-Fi app, the Authentication type is automatically selected. If needed, tap to open the **Authentication** dialog and select the correct security type for the network.

The following settings depend on the Authentication type. Enter all necessary credentials for the network security type, such as Encryption, Keys, EAP type, username, certificate, and/or password.

WEP Key

This setting appears if the Authentication type is **WEP Shared** or **WEP Auto**. Tap to select the correct key type (ASCII or Hex) and enter the key.

Encryption

Tap to select an encryption type if needed. The default is "Auto."

EAP Type

This setting appears if the Authentication type is **WPA/WPA2/WPA3 Enterprise**. The default is

PEAP MSCHAP V2. Tap to select a different EAP type if needed.

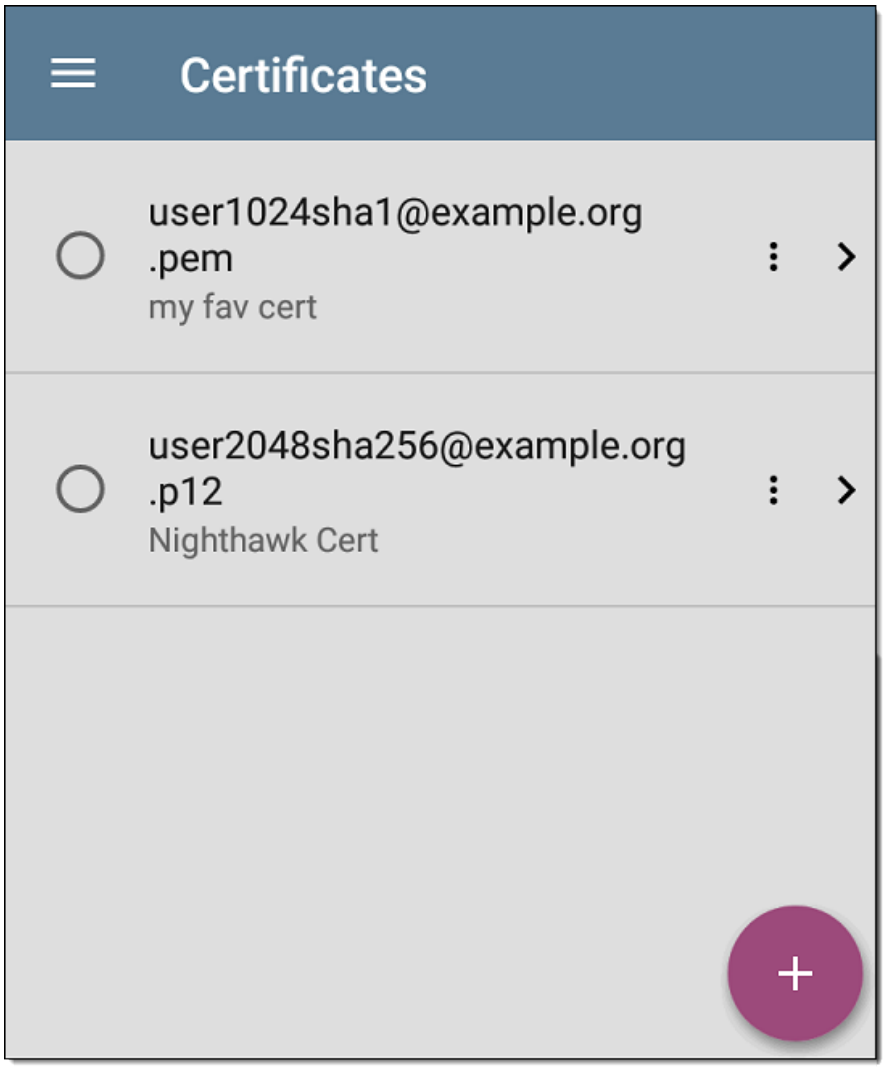
Username

This field appears along with multiple authentication types. Tap the **Username** field to enter your username.

Certificate

This setting appears if you selected one of the following EAP types: **EAP TLS**, **PEAP TLS**, or **TTLS EAP TLS**.

Tap to open the Certificates screen.



This screen displays all the certificates that have been imported to AutoTest via the Wired or Wi-Fi Profile settings.

- Tap the radio button to the left of an imported certificate to select and use it with the current Profile.
- Tap a certificate's row to edit its name and description.

- Tap the action overflow icon ⋮ to **Delete** an imported Certificate.
- Tap the floating action button (FAB) + to import a new certificate file.

EtherScope nXG supports these certificate file extensions:

- .pem
- .p12
- .cer
- .crt

The imported certificate feature is meant for client authentication and must include the private key. The EtherScope supports 1-way client authentication only; mutual authentication, Server, and CA/Root certificates are not supported. While EtherScope can perform a key exchange, it does not authenticate the server certificate.

Tap here to skip the following "How to" section and go to Advanced Wi-Fi Connection Settings.

How to Import a Certificate:

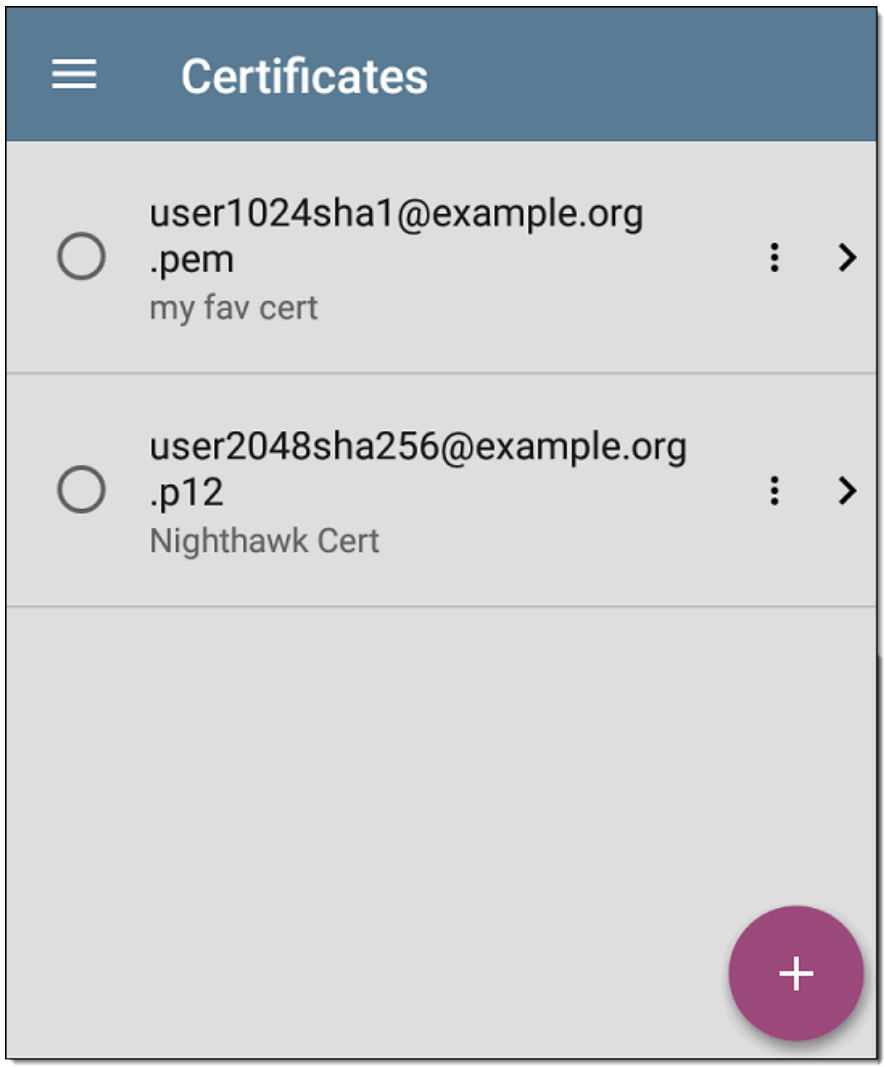
Certificate files can be imported from either an inserted storage device (USB or Micro SD) or the

EtherScope's internal file system.

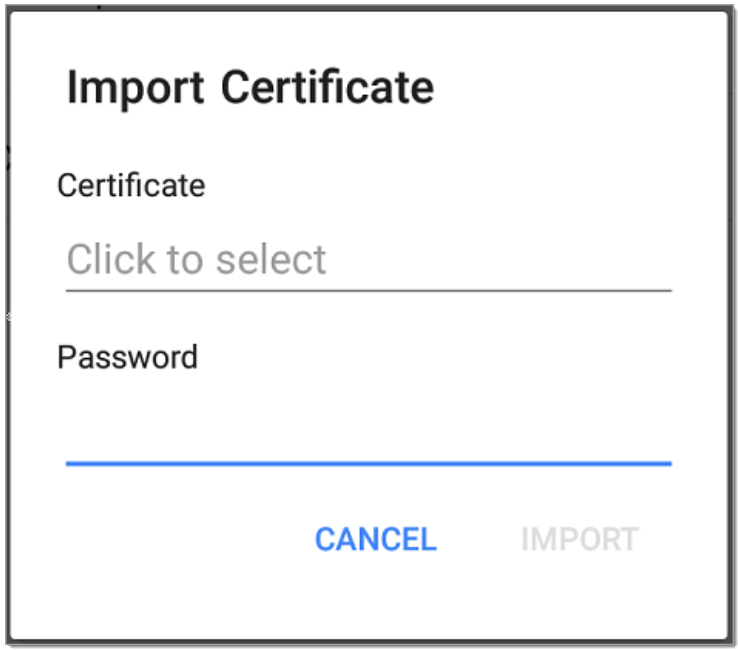
1. Make the certificate file available on your EtherScope unit by saving it to a USB drive or Micro SD card inserted into your unit or by transferring to the file system using a USB-C cable or email. (See Managing Files for help.)
2. To run an AutoTest Wi-Fi Profile using certificate authentication, set up the profile with the following settings:
   a. Authentication: **WPA/WPA2/WPA3 Enterprise**
   b. Encryption: **Auto**
   c. EAP Type: **EAP TLS, PEAP TLS, or TTLS EAP TLS**

   To run an AutoTest Wired Profile using 802.1X with certificate authentication, set up the profile with the following 802.1X test settings:
   a. 802.1X: **Enabled**
   b. EAP Type: **EAP TLS**, **PEAP TLS**, or **TTLS EAP TLS**

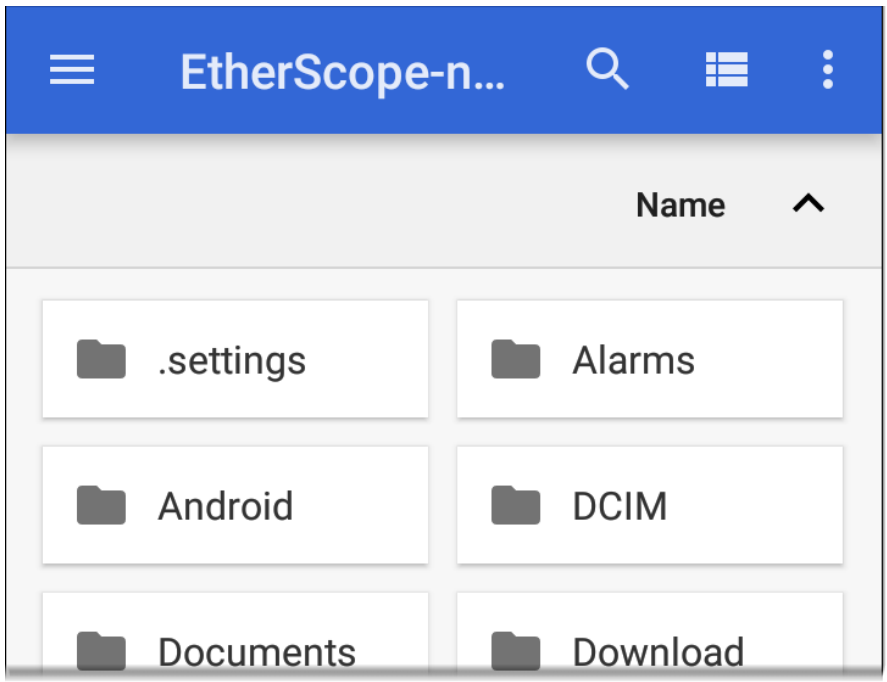
3. In **AutoTest > Wi-Fi Connection** or **Wired Connection** settings, tap the **Certificate** setting to open the Certificates screen.



4. Tap the floating action button (FAB) + to open the Import Certificate dialog box.

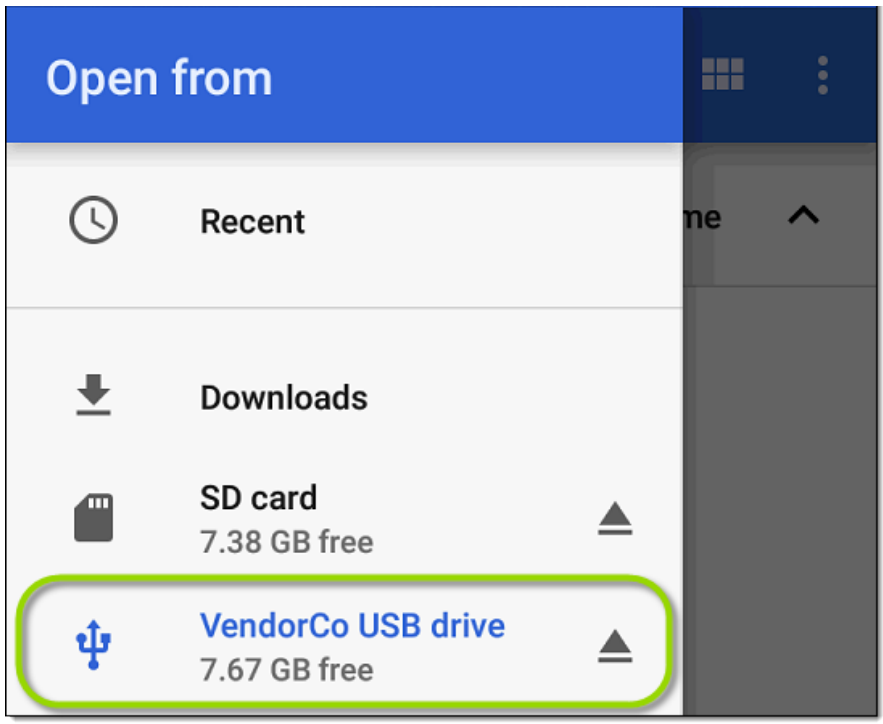


5. Tap **Click to select** beneath the Certificate field to open the Files app.



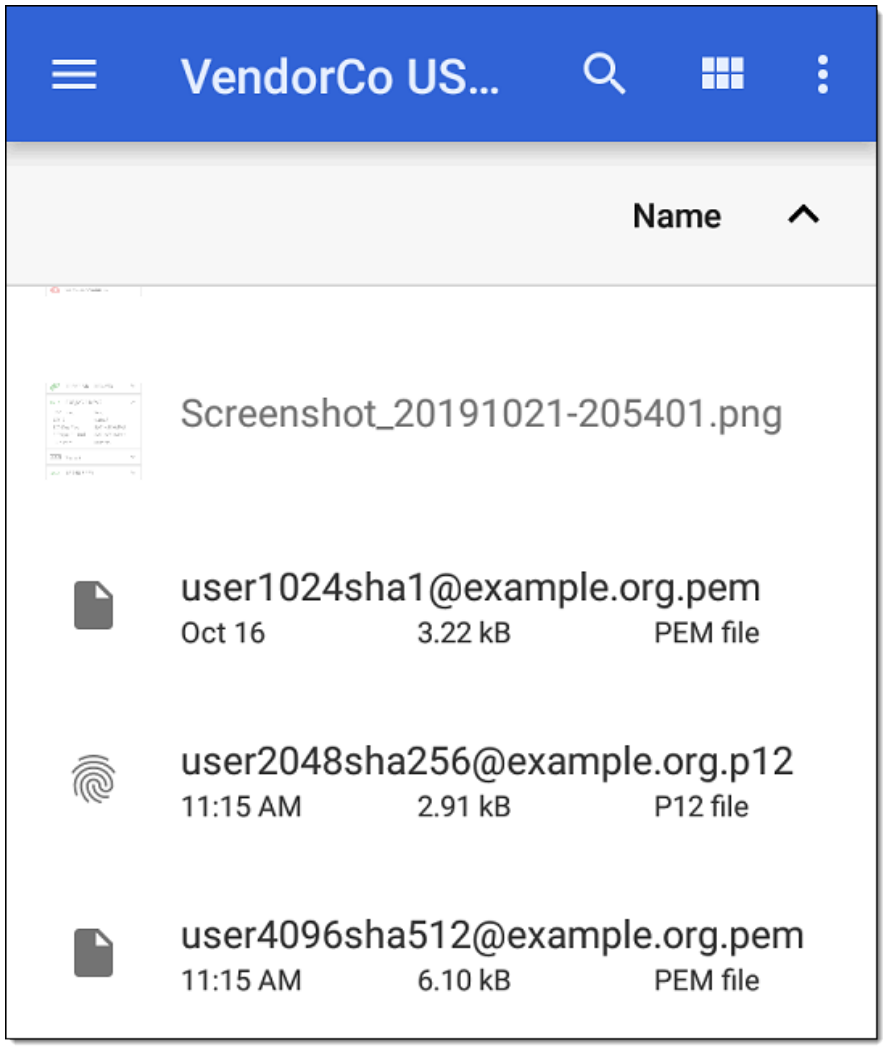
6. In the Files app, navigate to the folder or storage device where your certificate file is

saved. Tap the menu button to open the left-side navigation drawer and access the storage devices.



In the image above, the user is navigating to a USB flash drive.

7. Navigate to the required certificate file, and tap to select it.



After you select the file, the Files app closes, and the Import Certificate dialog displays the chosen certificate file.

8. Enter the certificate's password if it is password protected.
9. Tap **IMPORT**.

10. If desired, tap the fields to edit the **Name** and **Description** of the certificate. The name defaults to the certificate file name.
11. Tap the back button  to return to the Certificates list screen. The newly added certificate appears selected in the list.
12. Tap the back button  to return to the Connection settings.

After running the AutoTest, you can review the **Connect Log** from the Wi-Fi Link Test screen or Wired 802.1X Test screen to verify or troubleshoot certificate authentication.

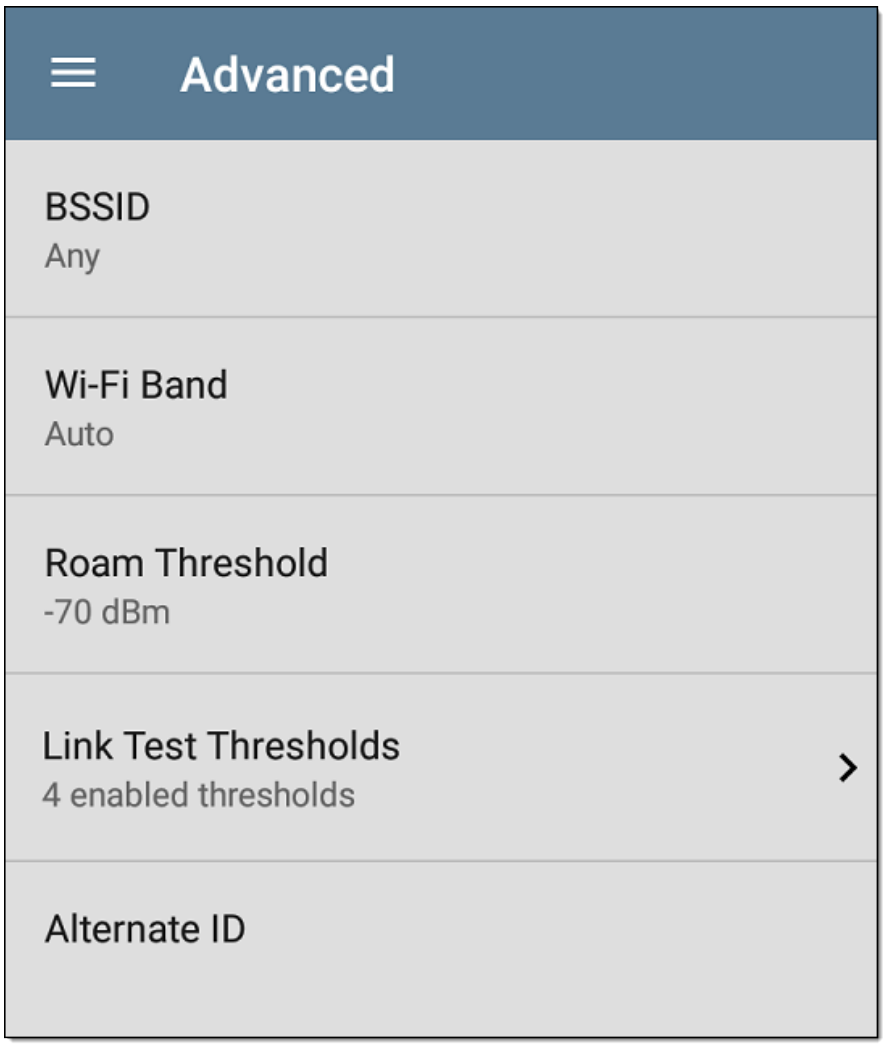
Username

This field appears along with multiple authentication types. Tap the **Username** field to enter your username.

Password

This field appears along with multiple security types. Tap the **Password** field to enter the network password.

Advanced (Wi-Fi Connection) Settings



BSSID

Enter or select a specific BSSID for the Wi-Fi Profile to prevent the EtherScope from roaming to a new AP while linked.

Wi-Fi Band

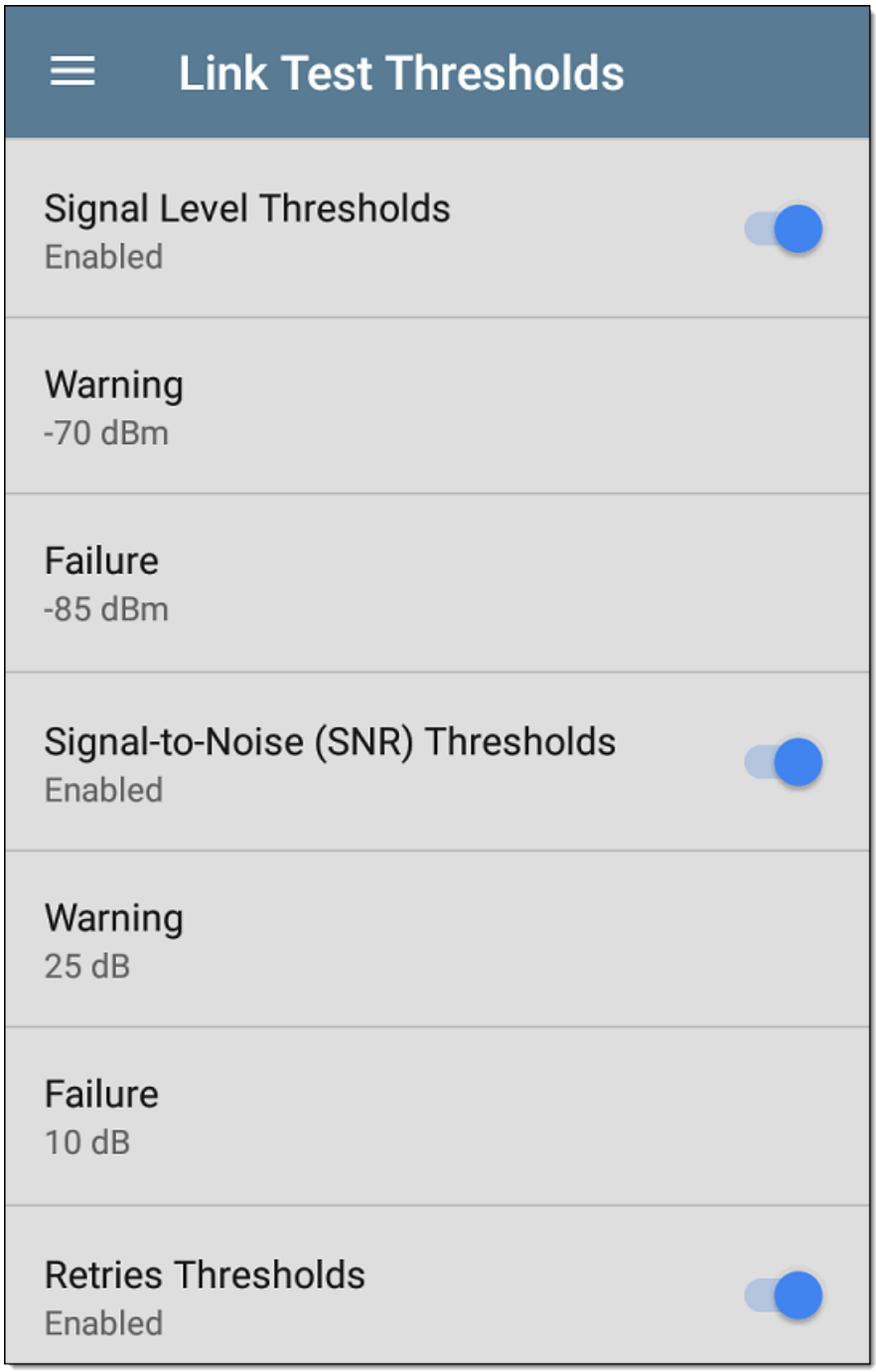
Tap this setting to specify the wireless band(s) on which the Wi-Fi Profile attempts to connect. The default setting of Auto allows the unit to connect on any band. Note that the Profile fails to link if this setting conflicts with the selected bands in General Settings.

Roam Threshold

This threshold controls the Signal Strength (in dBm) at which EtherScope stays connected and looks for another AP on the network with a stronger signal. If found, it disconnects from the current AP and connect to the AP with a stronger signal. Tap the field to select a new value or enter a custom one.

Link Test Thresholds

Open the **Link Test Thresholds** screen to adjust the values that determine **Success**/**Warning**/**Fail** results for the following measurements.



Tap each field to select a new value or enter a custom one. Each threshold also has a toggle button that allows you to disable grading based on that measurement entirely.

Signal Level Thresholds: Measured signal from the AP

Signal-to-Noise (SNR) Thresholds: Ratio of measured AP signal to noise level detected on the channel

Retries Thresholds: Retry frames as a percentage of total transmitted frames

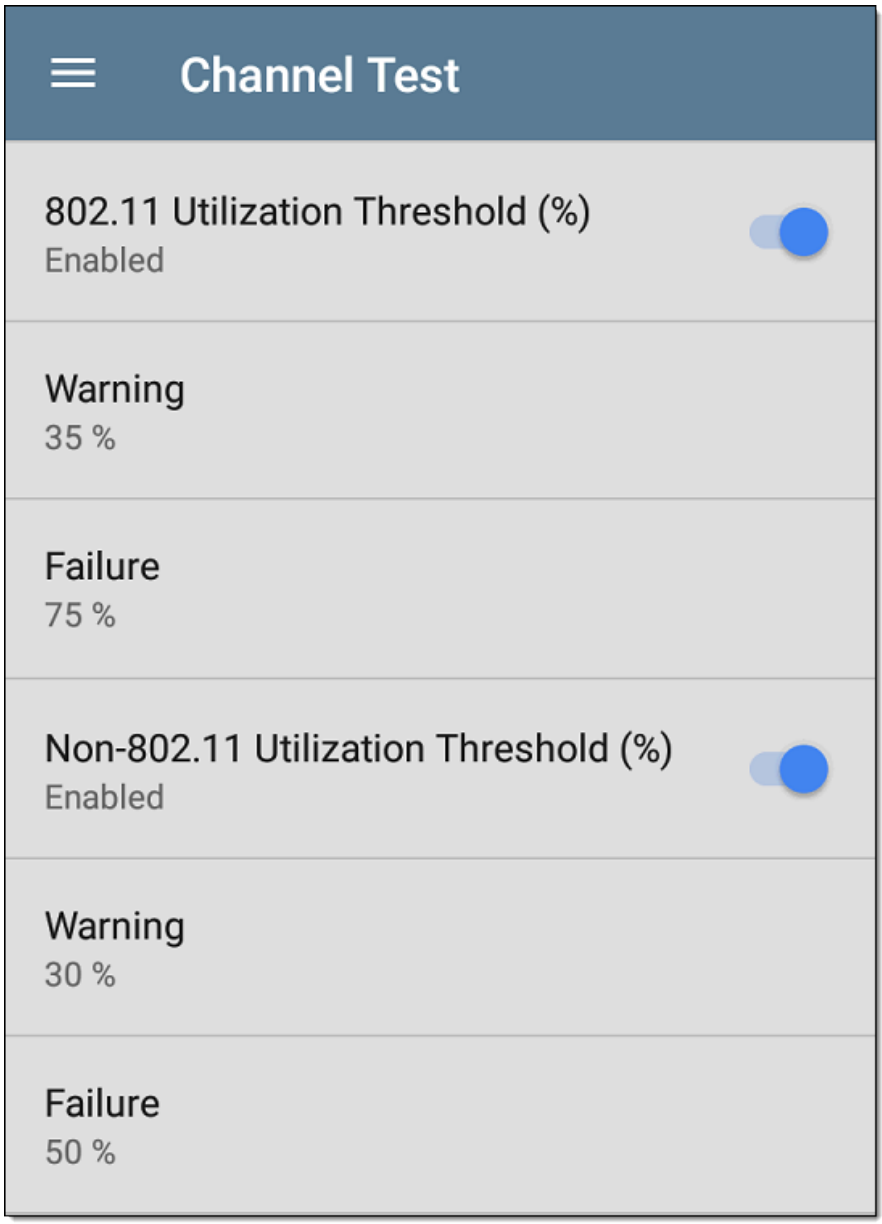
Transmit Rate (TX) Thresholds: Measured rate as a percentage of the AP's maximum throughput rate

Alternate ID

Enter an Alternate ID if necessary. This is an Advanced Authentication setting.

Channel Test Settings

Open **Channel Test** settings to configure Utilization thresholds for the channel test portion of the Wi-Fi profile.



(EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, only a single, combined **Utilization Threshold** setting appears.

802.11 Utilization Threshold (%)

This threshold controls the **Success**/**Warning**/**Fail** gradings for the

percentage of the connected channel's capacity being used by 802.11 devices.

- Tap the toggle button to enable or disable test grading based on 802.11 utilization.
- Tap **Warning** or **Failure** to select or enter custom percentage values for Warning or Failure results.

Non-802.11 Utilization Threshold (%)

This threshold controls the **Success**/**Warning**/**Fail** gradings for the percentage of the connected channel's capacity being used by non-802.11 interference.

- Tap the toggle button to enable or disable test grading based on non-802.11 utilization.
- Tap **Warning** or **Failure** to select or enter custom percentage values for Warning or Failure results.

DHCP, DNS, and Gateway Settings

Settings for these tests operate the same in both Wired and Wi-Fi profiles.

See DHCP, DNS, and Gateway Tests

PING FTP TCP HTTP Test Targets

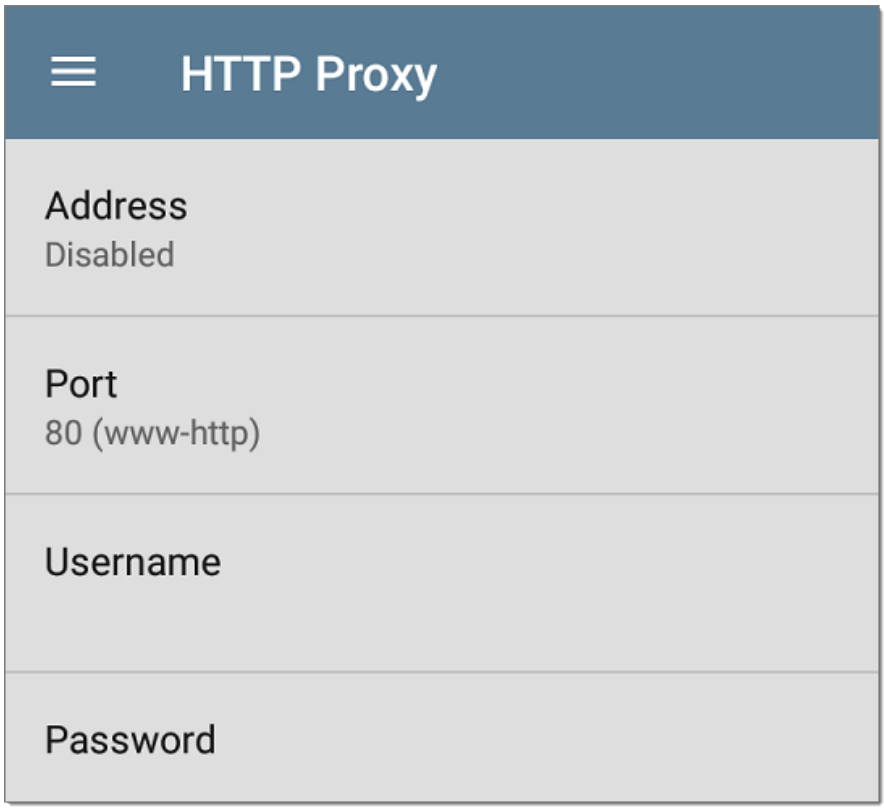
Tap the **Test Targets** field to open the Test Targets screen and add custom Ping, TCP Connect, HTTP, or FTP tests to your AutoTest profile. See Test Targets to learn more.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the EtherScope establishes a network connection. In AutoTest, these settings are used when HTTP Proxy is enabled in an HTTP or FTP Test Target.

To use the proxy settings with a web browser, run the Profile, and then, open the web browser while the unit remains linked. When using a web browser, the Wired Test Port takes priority over the Wi-Fi Test Port, so if you want to browse via Wi-Fi proxy connection, unplug the (top) Wired Test Port.

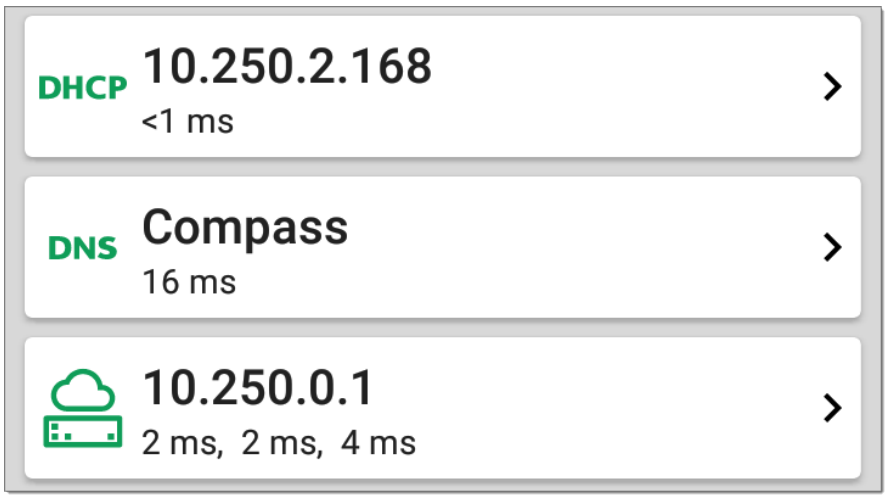
Open the **HTTP Proxy** screen to enable proxy settings.



Tap each field to open a pop-up keyboard and enter the appropriate **Address**, **Port**, **Username**, and **Password**. Tap **OK** to save your entries.

Back to Title and Contents

DHCP, DNS, and Gateway Tests



These tests are included in both Wired and Wi-Fi AutoTest Profiles, and the settings and results fields are the same for each Profile type. Access AutoTest's DHCP, DNS, and Gateway settings from either the Wired or Wi-Fi Profile settings screens, or by tapping the settings button from the full results screen for each test type.

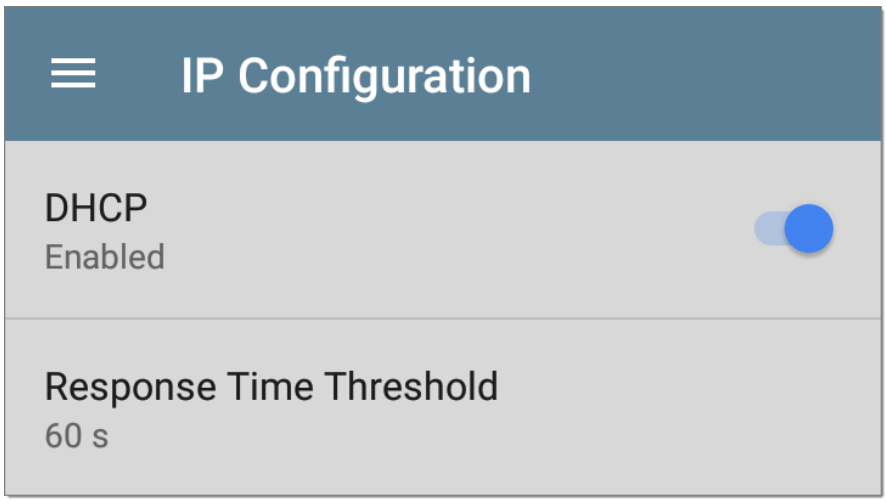
Tap blue links or the blue action overflow icon ••• on the test results screens for additional actions.

DHCP or Static IP Test

The DHCP (Dynamic Host Configuration Protocol) test indicates whether the EtherScope receives an IP address assignment from the DHCP server.

DHCP Settings – IP Configuration

Access the DHCP test settings from the Wired or Wi-Fi Profile settings or by tapping the settings button on the DHCP test results screen.



By default, DHCP is enabled. On the **IP Configuration** screen, you can adjust the **DHCP Response Time Threshold** or configure a **Static IP Address**.

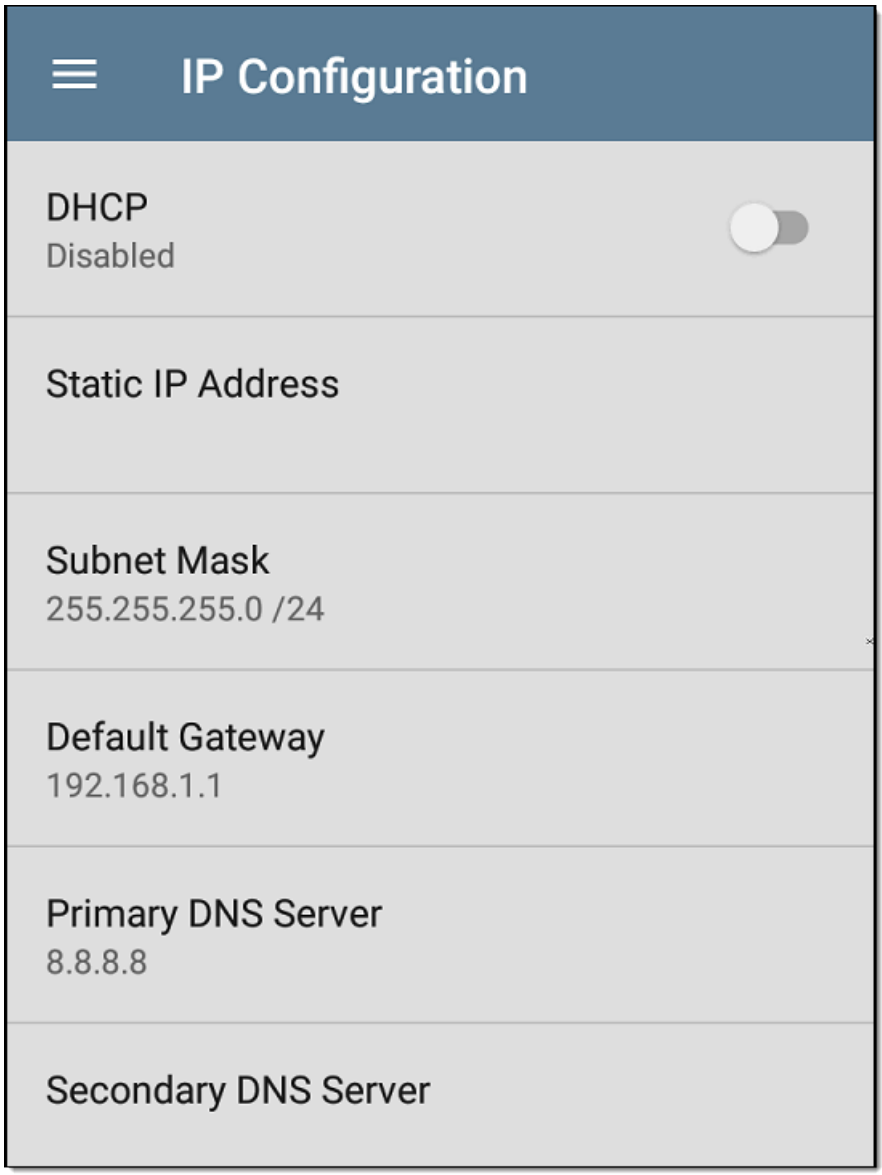
DHCP

DHCP is enabled by default. Tap the toggle button to disable DHCP and enter static IP addresses.

(DHCP only) Response Time Threshold

This field only appears if DHCP is enabled. The Response Time Threshold controls how long the EtherScope waits for a DHCP server response before failing the Link and DHCP tests.

Static IP Address



The Static IP address fields for **Subnet Mask, Default Gateway**, and **Primary** and **Secondary DNS Servers** only appear if DHCP is disabled. Tap each field to open a pop-up number pad and enter the static addresses as needed. Tap **OK** to save your entries.

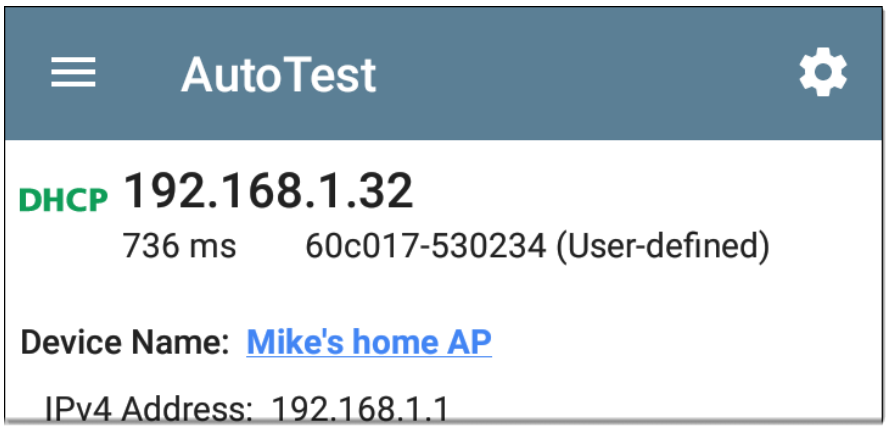
DHCP Test Results

When DHCP is enabled, the DHCP test card and results screen are displayed in the Profile.

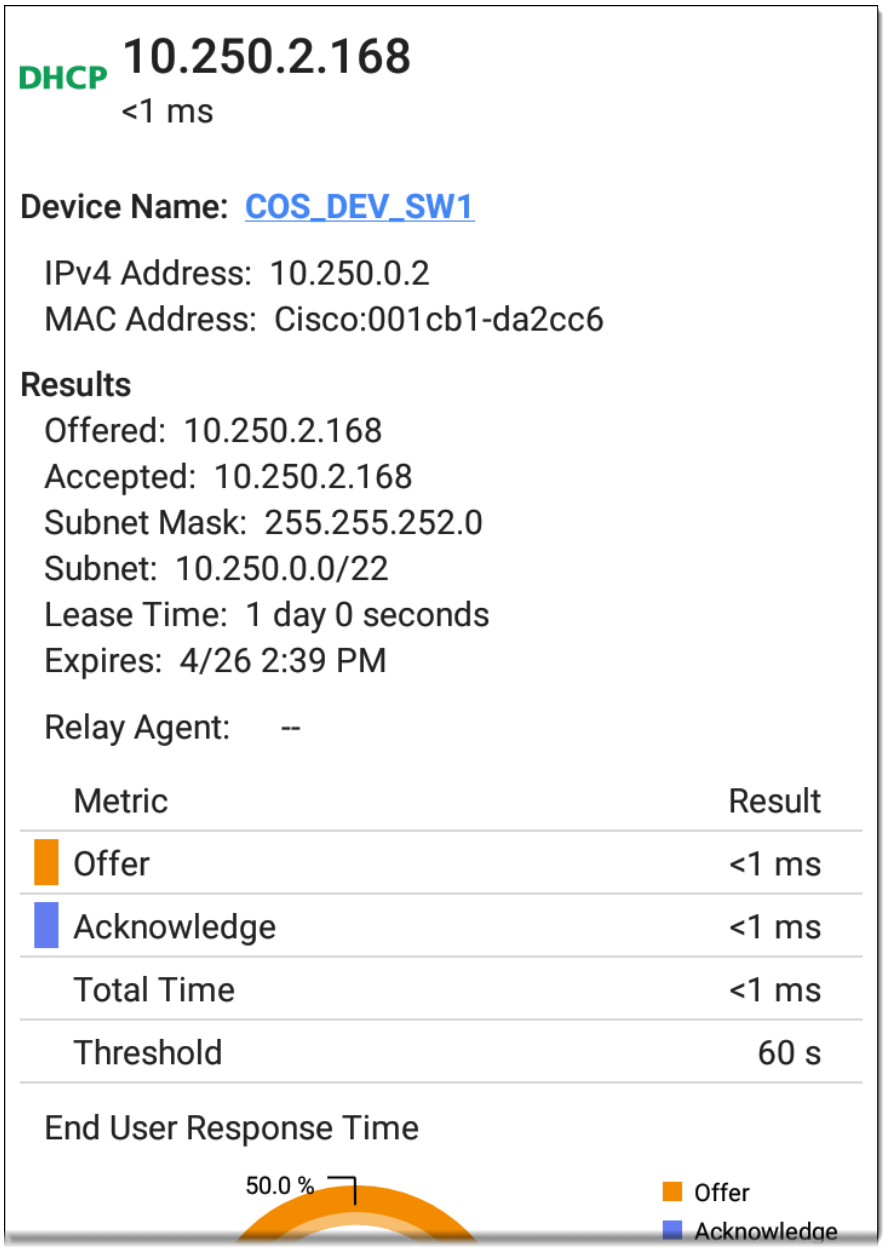
The DHCP Test card displays the DHCP server's IP address and the total time for the discover, offer, request, and acknowledgment to complete.

Tap the card to open the DHCP test screen.

> NOTE: If a **User-Defined MAC** is enabled for this connection in General Settings, (User-defined) appears next to the MAC address beneath the DHCP IP address on results screen.



DHCP Test Results Screen



Device Name: The discovered name of the DHCP Server, or, if no name could be discovered, the IP address

IPv4 Address: IP address of the server

MAC Address: Server's MAC address. Two dashes -- indicate that no MAC address was provided from the server.

Results

Offered: IP address offered by the DHCP server

Accepted: IP address accepted by the Ether-Scope

Subnet Mask: Used to determine which addresses are local and which must be reached via a gateway

Subnet: Combination of the subnet mask and the offered IP address

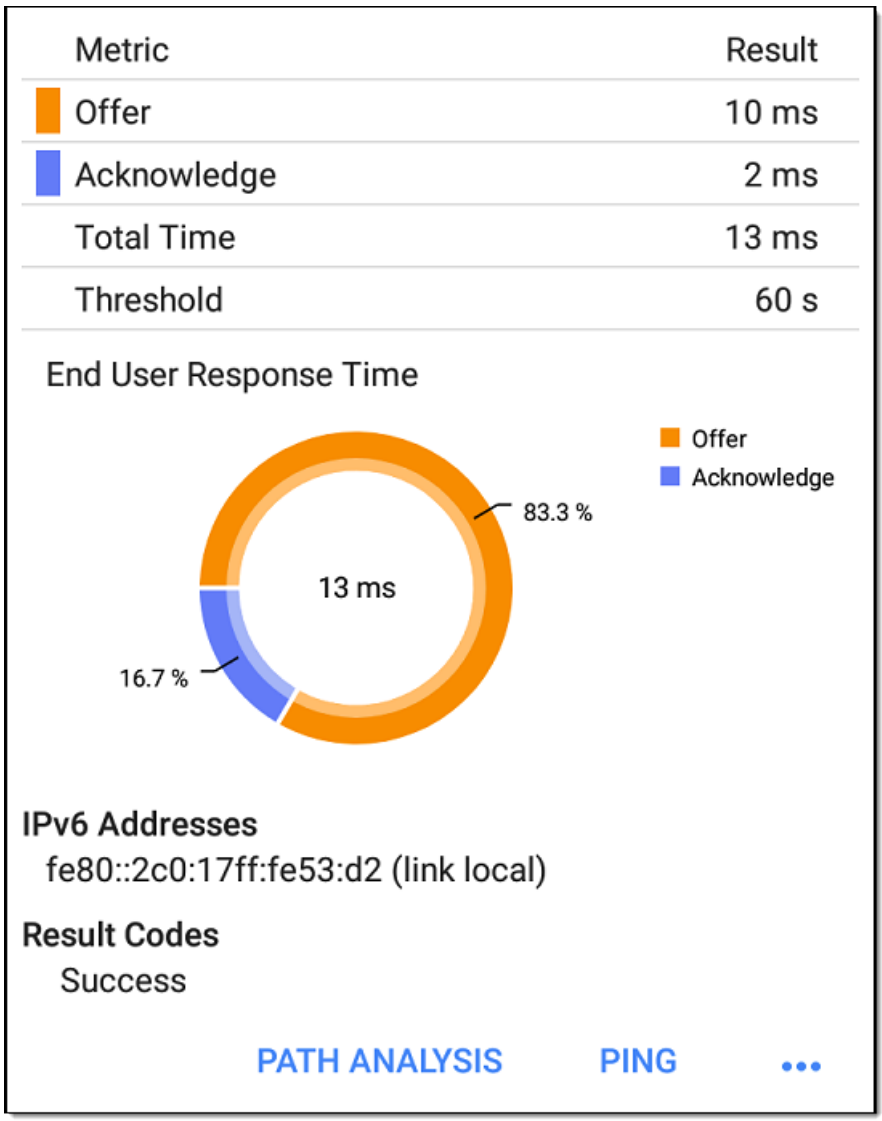
Lease Time: The amount of time the IP address is leased to the EtherScope by the DHCP server

Expires: Expiration date and time of the IP address

Relay Agent: If a BOOTP DHCP relay agent is present, this field shows its IP address. The relay agent relays DHCP messages between

DHCP clients and DHCP servers on different IP networks.

End User Response Time table and chart: Breakdown of the times for the process of acquiring a DHCP IP address



Offer: Time between when the EtherScope sent the discovery and received an address offer from the DHCP server

Acknowledge: Time between EtherScope sending the request and receiving the acknowledgment from the DHCP server

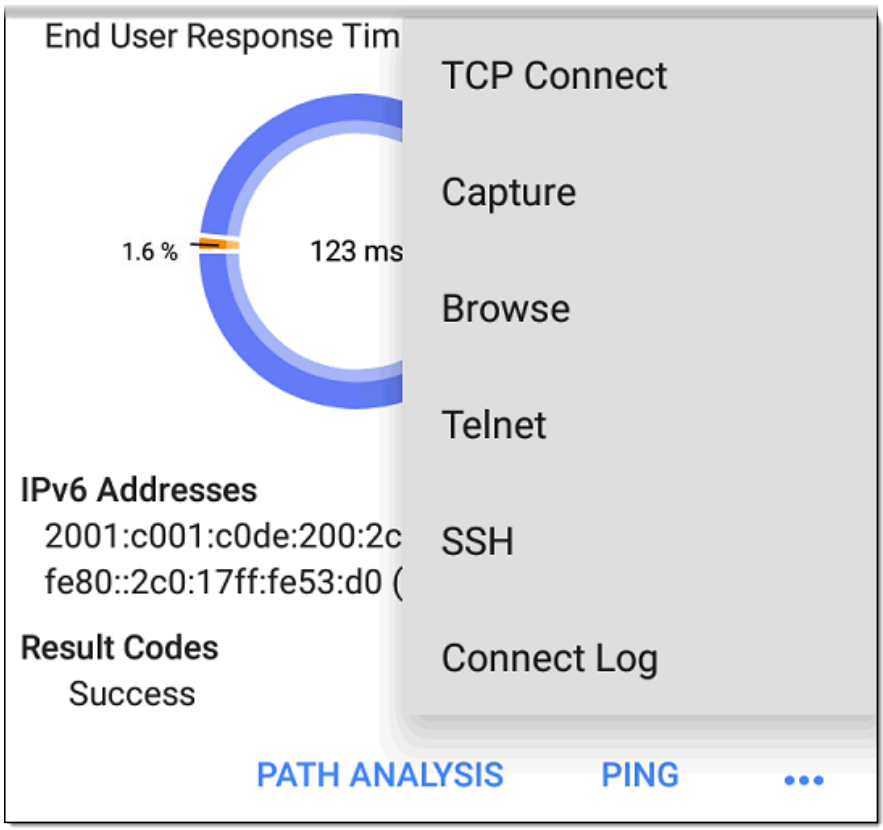
Total Time: Total amount of time consumed by the DHCP process

Threshold: The DHCP Response Time Threshold from the DHCP test settings, which controls how long the EtherScope waits for a DHCP server response before failing the DHCP test.

End User Response Time: A pie chart showing the Offer and Acknowledgment times as percentages

IPv6 Addresses: Addresses obtained via router advertisement

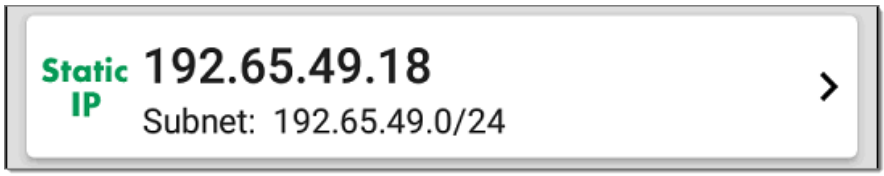
Results Codes: Final status of the test (Success or Failure)



The additional actions available on the DHCP test screen include opening the Path Analysis, Ping/TCP, or Capture apps populated with the DHCP server address, browsing to the IPv4 address in the web browser, starting a Telnet or SSH session, or viewing the Connect Log.

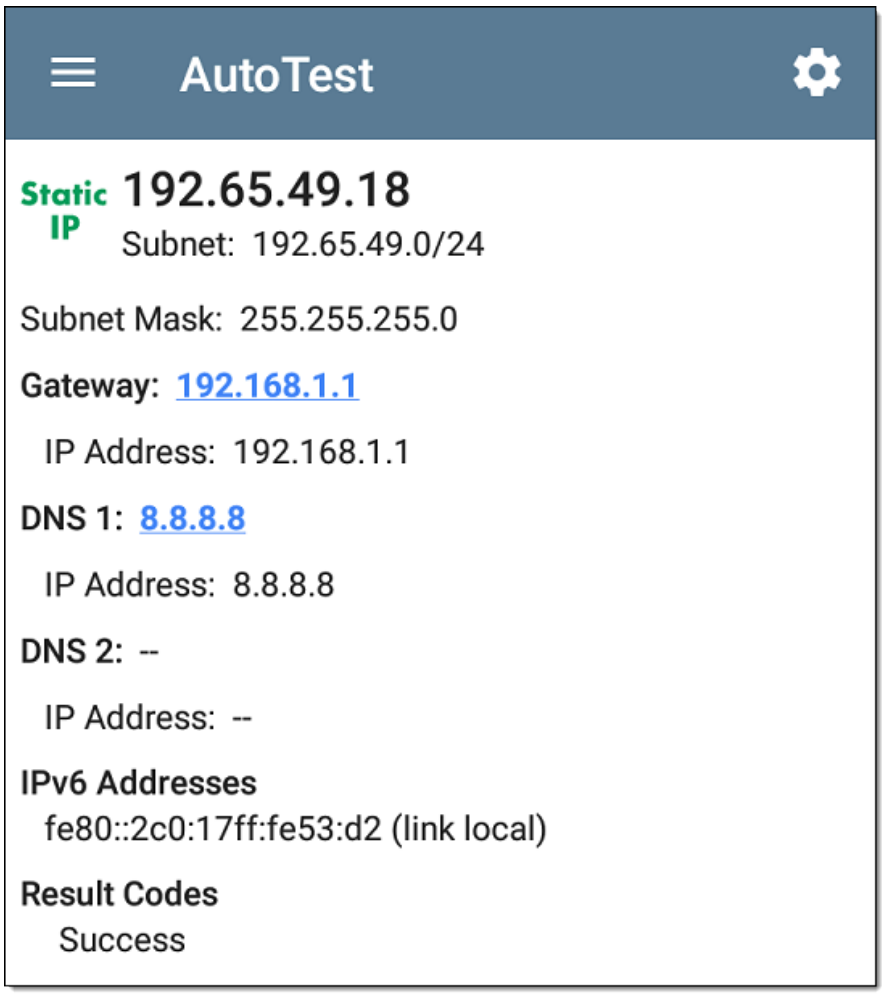
Static IP Test Results

If DHCP is disabled, the DHCP test becomes a "Static IP" test and the Subnet and addresses that were entered in the DHCP test settings are displayed.



The Static IP card displays the configured IP and Subnet addresses.

Tap the card to open the test results screen.



The Static IP test screen displays the configured addresses.

Subnet: Combination of the subnet mask and the offered IP address

Subnet Mask: Used to determine which addresses are local and which must be reached via a gateway

Gateway: Resolved hostname of the Gateway or its IP address if no name could be discovered

IP Address: IP address of the Gateway

DNS (1 and 2): Names and IP addresses of Primary and Secondary DNS servers

IPv6 Addresses: Addresses obtained via router advertisement

Results Codes: Final status of the test (Success or Failure)

Duplicate IP Address

The DHCP and Static IP tests also detect and report the presence of a device using the same IP address (duplicate IP). If the configured address is in use, the AutoTest fails.

IP Address In Use By: Shows the name of the device currently using the configured static IP address. Tap the blue underlined link to open a Discovery Details screen for the device.

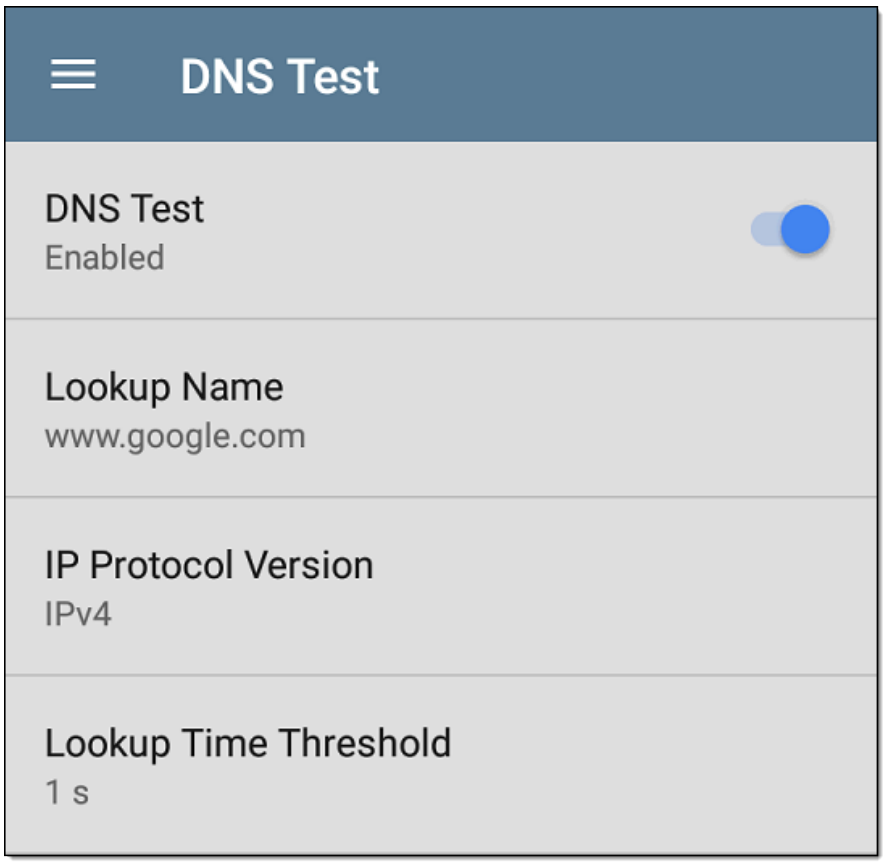
MAC Address: MAC of the device using the IP address

DNS Test

For overview information, see DHCP, DNS, and Gateway Tests.

The DNS (Domain Name System) server test checks the performance of DNS servers resolving the specified URL. The EtherScope obtains DNS addresses through DHCP or static address configuration.

DNS Test Settings



DNS Test

If desired, you can tap the top field on the DNS Settings screen and switch the toggle to disable the DNS test in your current AutoTest. When this setting is disabled, the DNS card does not appear on the main AutoTest results screen, and the following settings are hidden.

Lookup Name

This is the URL the DNS server(s) attempts to resolve. Tap the field to enter a URL other than the default: www.google.com.

IP Protocol Version

Tap the field to switch between IPv4 and IPv6.

Lookup Time Threshold

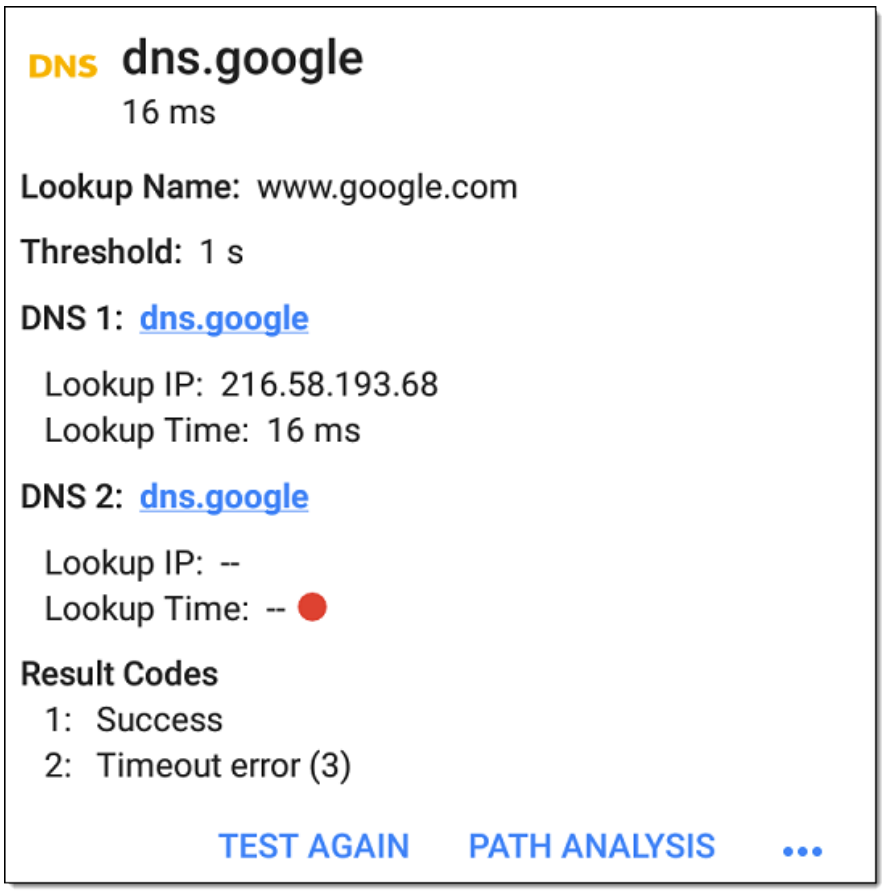
This threshold controls how long the EtherScope waits for a response from the DNS server(s) before the test is failed. The default is 1 second. Tap the field to select or enter a new threshold.

DNS Test Results

The server name and lookup time for DNS 1 are shown on the DNS test card.

Tap the card to open the DNS test results screen.

DNS Test Results Screen



Lookup Name: Name resolved by the DNS servers

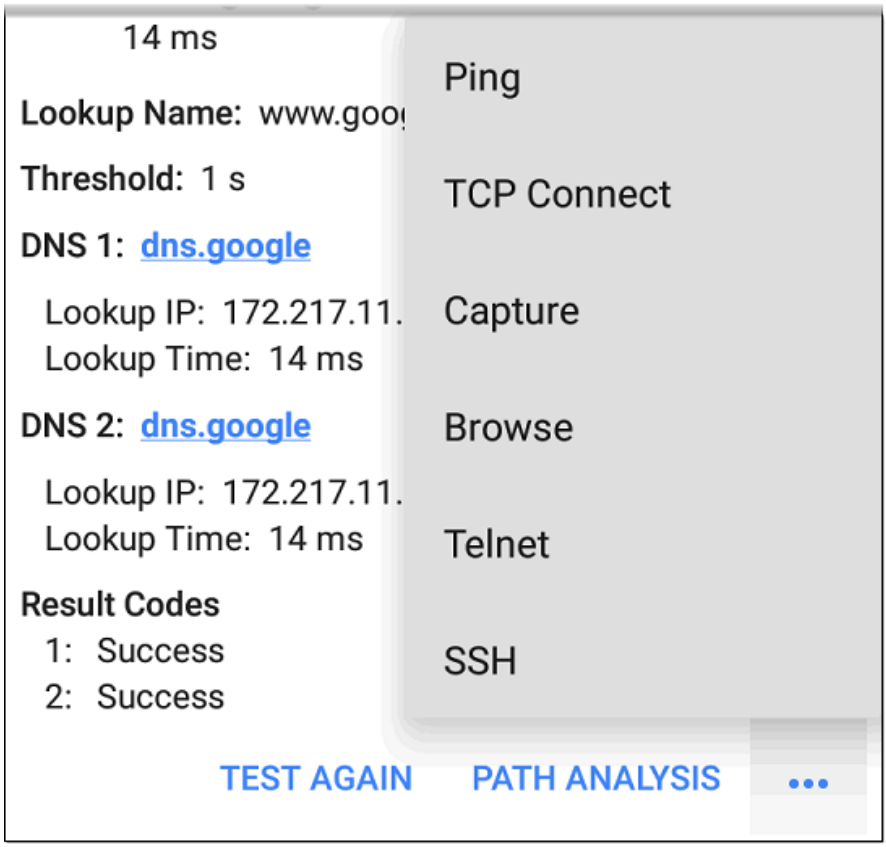
Threshold: Lookup Time Threshold from the DNS test settings

DNS #: Name of the listed DNS server

Lookup IP: Resolved IP address

Lookup Time: Time to receive the IP address after the lookup request sent

Results Codes: Final status of the test (Success or Failure) for each DNS server



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the DNS **Test Again**, open another app populated with the name and IP address of DNS 1, or **Browse** to the Primary DNS server in your web browser.

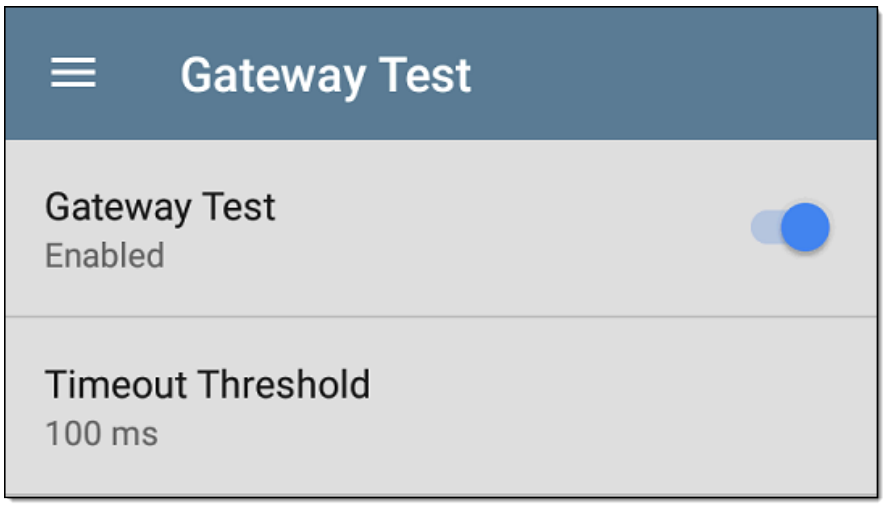
Back to Title and Contents

Gateway Test

For overview information, see DHCP, DNS, and Gateway Tests.

This test indicates whether the default Gateway could be successfully pinged and identifies the address of the current IPv4 and IPv6 routers.

Gateway Test Settings



Gateway Test

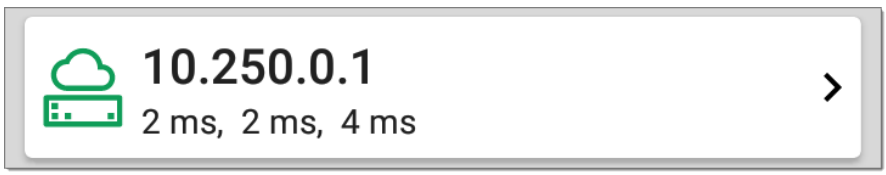
If desired, you can tap the top field on the Gateway Test screen and switch the toggle to disable the Gateway test in your current AutoTest. When this setting is disabled, the Gateway card does not appear on the main AutoTest results screen, and the following setting is hidden.

Timeout Threshold

The only other setting for the Gateway Test is the timeout threshold, which indicates how long the EtherScope waits for a response from the gateway before grading the test as a fail. Tap the field to select one of the value options, or enter a custom value.

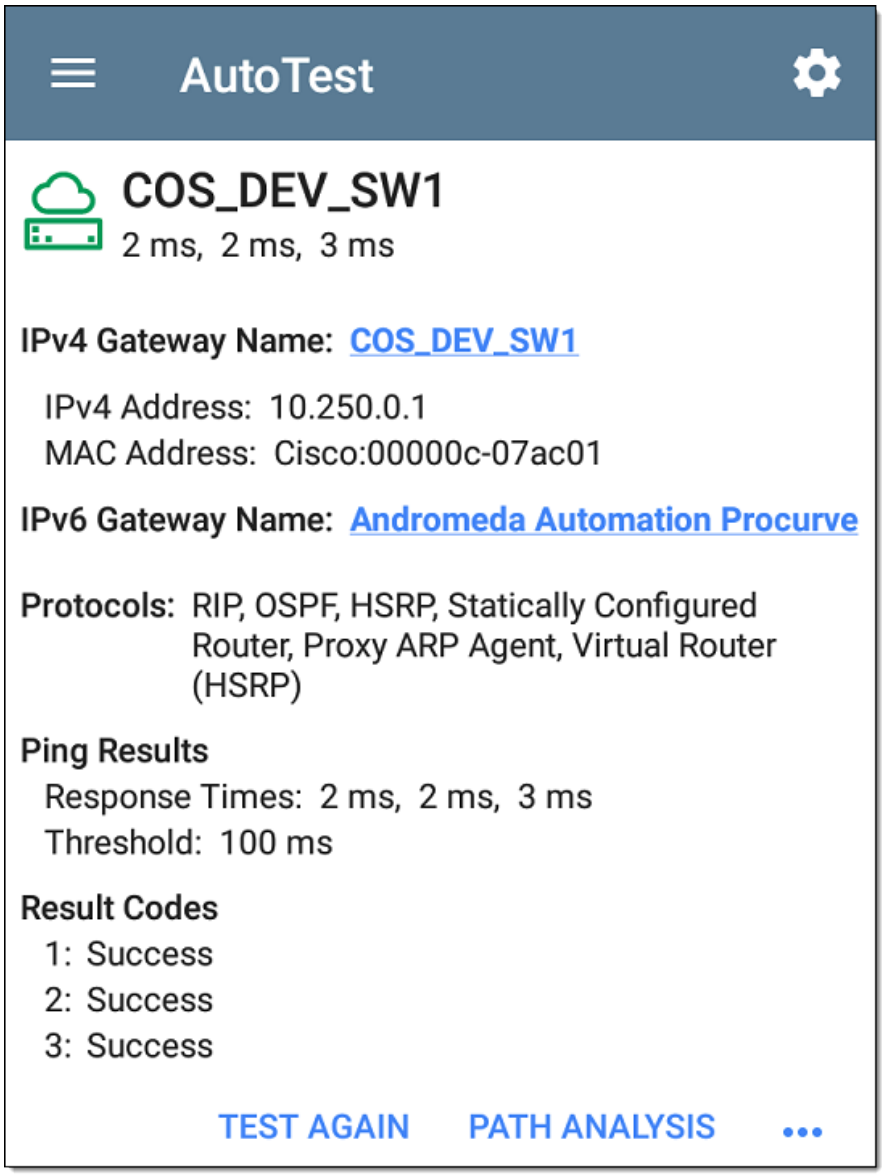
Gateway Test Results

EtherScope gets the Gateway's IP address from DHCP or the static IP configuration, and uses SNMP to acquire system group information and statistics for the port that services the EtherScope's subnet. See Discovery Settings for information about SNMP configuration.



The Gateway test card shows the gateway's IP address and the three Ping response times.

Gateway Test Results Screen



IPv4 Gateway Name: Resolved hostname of the Gateway or its IP address if no name could be discovered

IPv4 Address: Internal IPv4 address of the Gateway

MAC Address: Server's MAC address. Two dashes -- indicate that no MAC address was provided from the server.

IPv6 Address: Router's IPv6 address (if available)

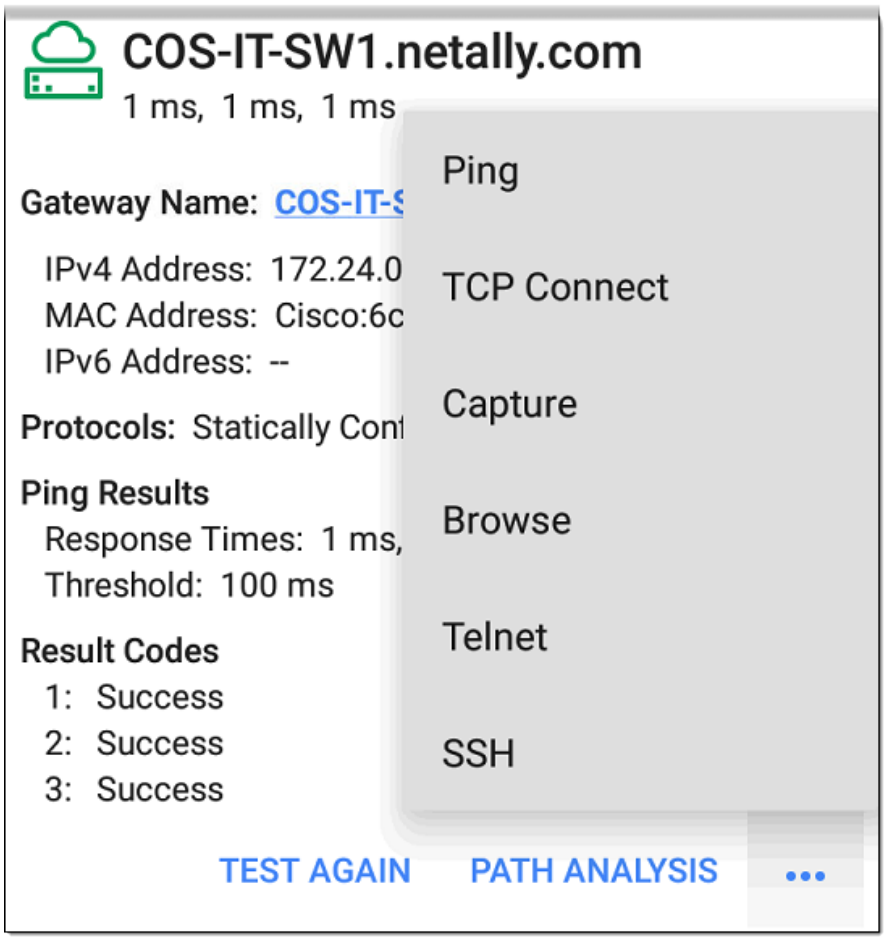
IPv6 Gateway Name: Name advertised by the IPv6 router (if available)

Protocols: Routing protocols the EtherScope used to obtain the Gateway data

Ping Results

- **Response Times** from the three Pings sent to the gateway
- **Threshold**: Gateway Timeout Threshold configured in the gateway settings

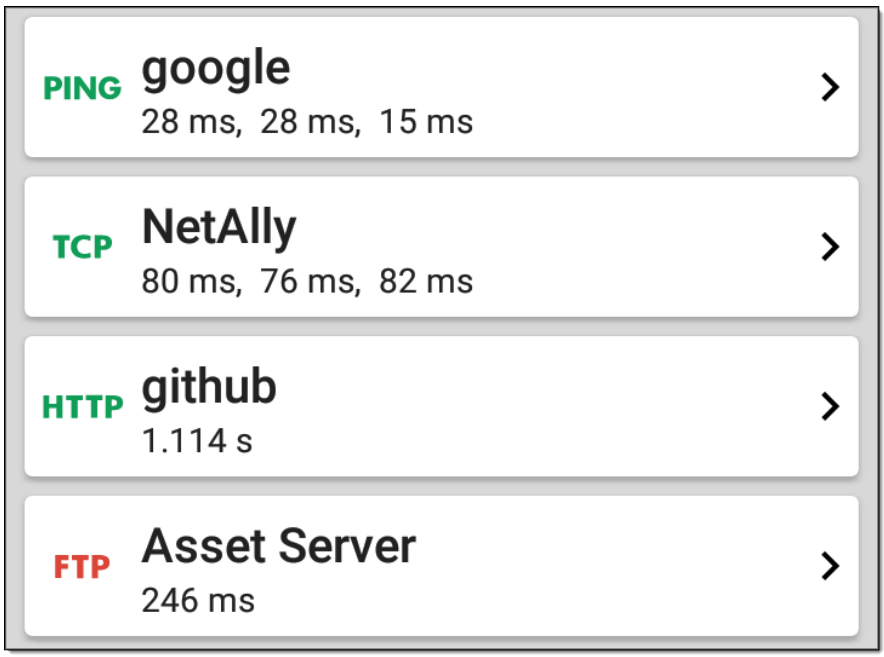
Results Codes: Final status of the test (Success or Failure) for each of the three Gateway Pings



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the Gateway **TEST AGAIN**, open another app, **Browse** to the Gateway's IPv4 Address, or start a Telnet or SSH session to the Gateway.

Back to Title and Contents

Test Targets for Wired and Wi-Fi AutoTests



AutoTest Target tests are user-assignable endpoints to which EtherScope nXG attempts to connect each time the AutoTest profile runs. These tests ensure availability of internal or external websites, servers, and devices to users of your network.

Tap a link below to go to the test's topic:

Ping

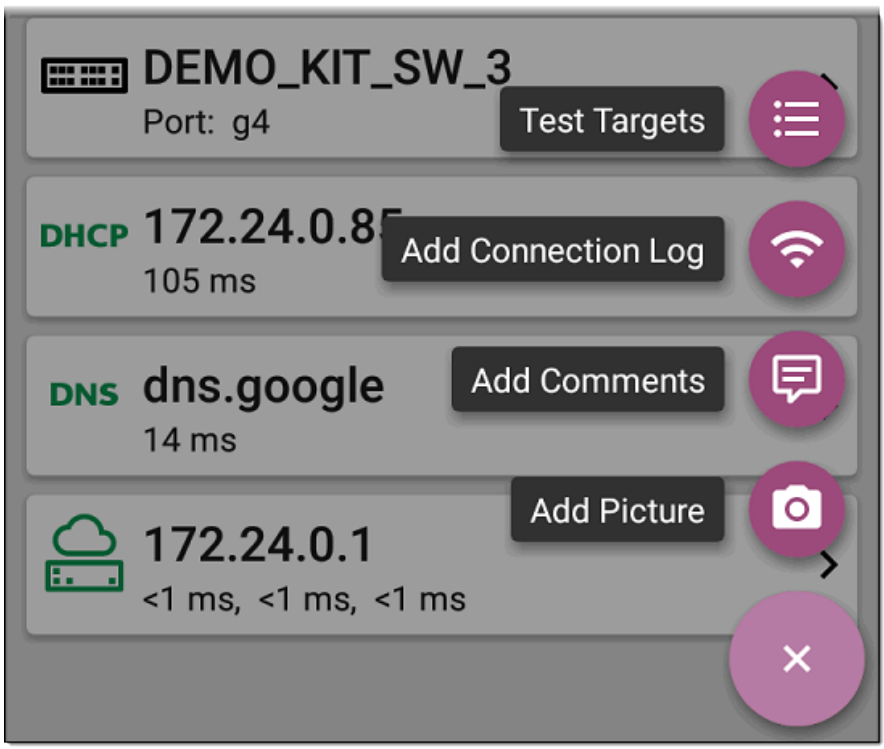
TCP Connect

HTTP

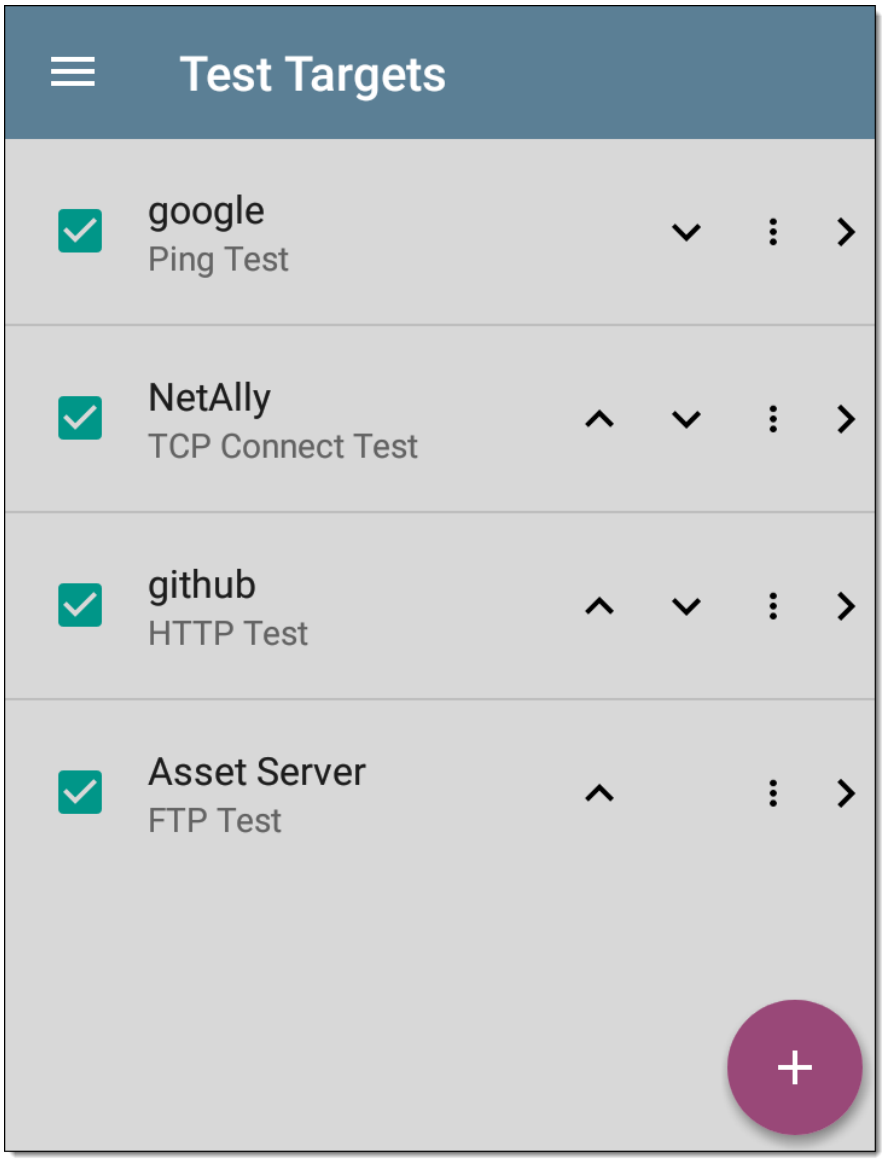
FTP

Adding and Managing Test Targets

To add test targets to AutoTest profiles and manage your saved targets, open the **Test Targets** screen from either the Wired or Wi-Fi Profile Settings or by tapping the FAB on the Wired or Wi-Fi Profile results screens.



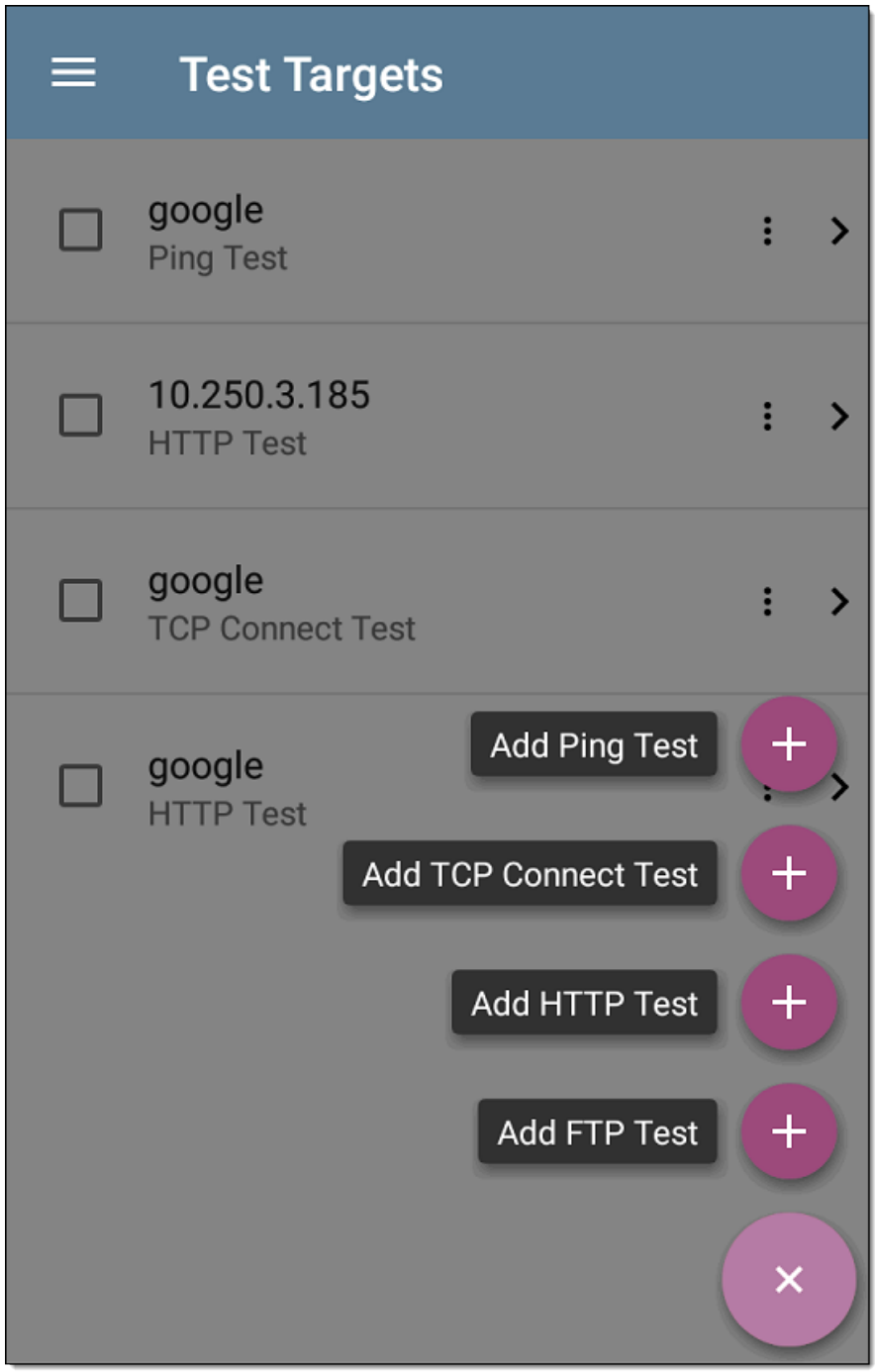
The Test Targets screen lists all of the defined and saved Test Targets. Checked boxes indicate the Test Targets that are enabled in the current Profile. Remember, Test Targets can be added to and used in any number of Wired or Wi-Fi Profiles.



On the Test Targets screen, you can perform these actions:

- Select the checkboxes for each Target you want to include in the current profile.
- Tap the up and down arrows to reorder the saved Test Targets on this screen and the main AutoTest Profile screen.

- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a target test.
  CAUTION: When you delete a Test Target, you delete it from all Profiles. To remove a Test Target from the current profile, simply uncheck it.
- Tap the FAB icon + to add a new target test: Ping, TCP Connect, HTTP, or FTP.



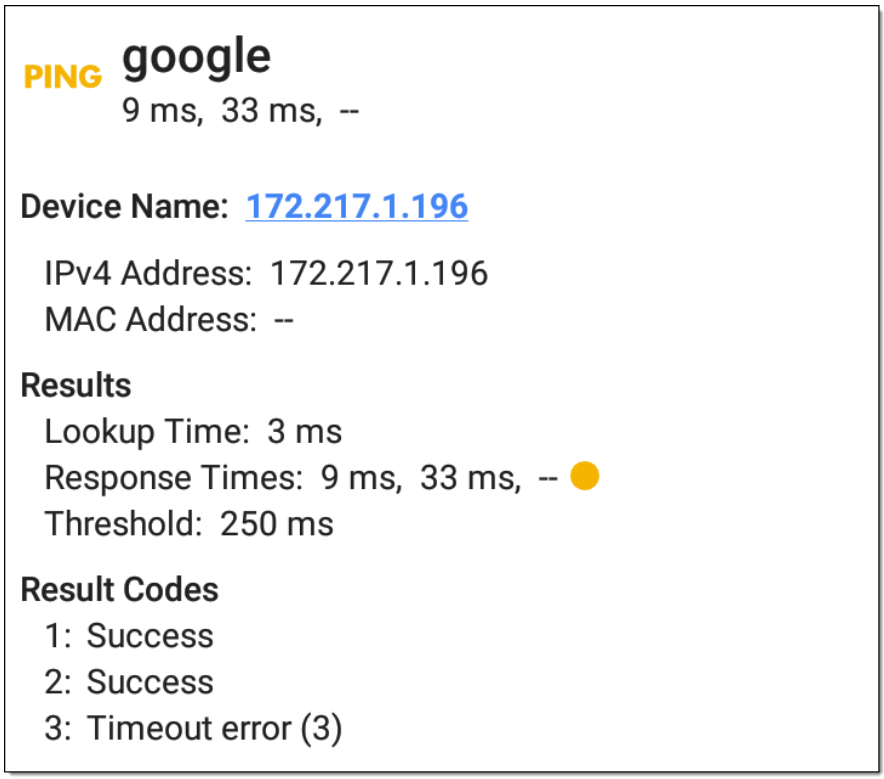
- Tap any target test name to open that test's settings. You can then enter a custom test name, target address, or thresholds. For more information on settings, see:

- Ping Test
- TCP Connect Test
- HTTP Test
- FTP Test

Target Test Results Screens

The Target Test type icons display green, yellow, or red to indicate the status (or grade) of the completed test portions: **Success**/**Warning**/**Fail**.

As an example, in the Ping test image below, the entire Ping test is graded with a Warning because the third Ping was not returned within the Timeout Threshold configured in the settings.



The third Response Time displays two dashes -- to indicate that no response was received, and under the Results heading, the yellow dot points out the third Response Time as the reason for the Warning. Additionally, the third Result Code lists "Timeout error" as the reason for the Warning.

Additional Target Test Actions

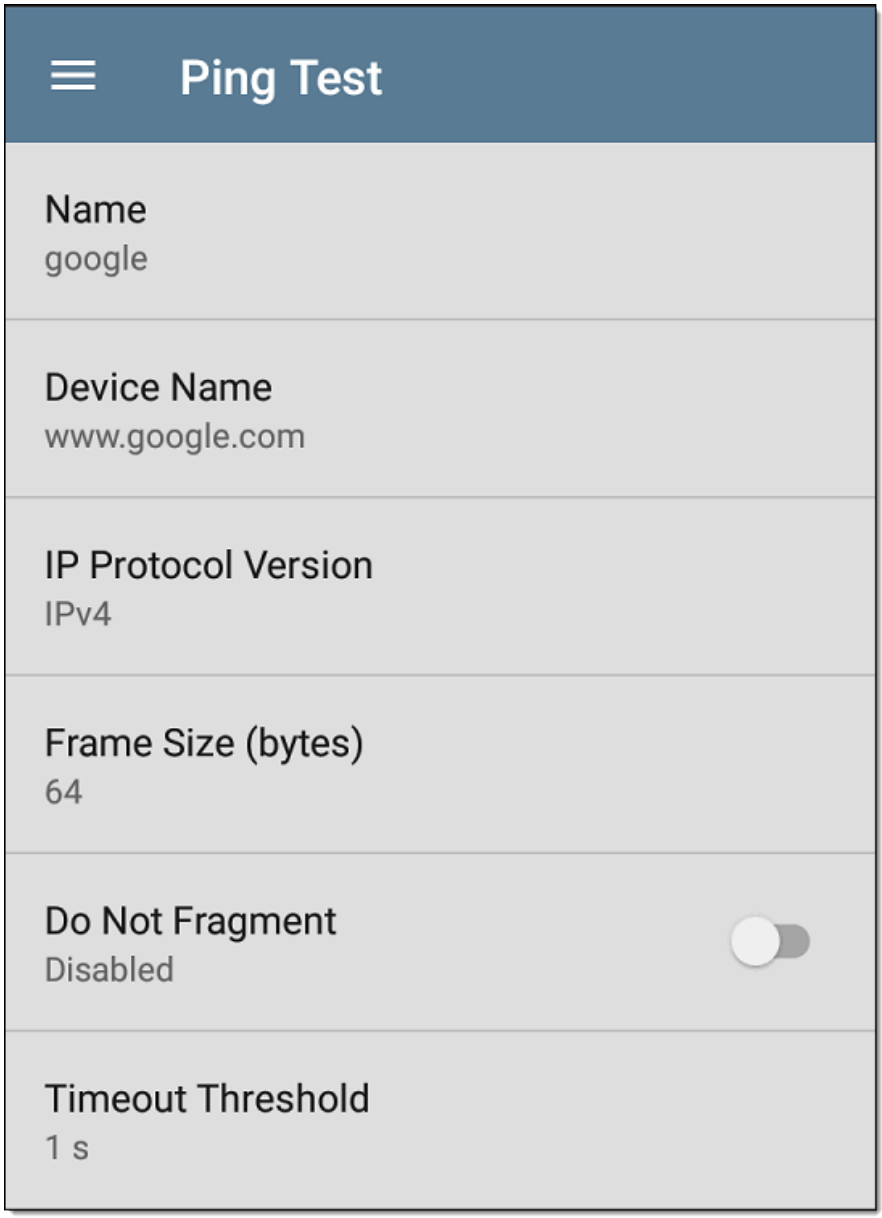
After the Target test has completed, tap any of the blue links to perform additional actions, including opening other testing apps.

- Tap the blue linked Device Name to open a Discovery Details app screen for the selected device. From there, you can open other apps and run additional tests.
- Tap TEST AGAIN to run just the target test again.
- Tap PATH ANALYSIS to open the Path Analysis app. The path Destination is configured with the current target.
- Tap the action overflow icon ••• to open the listed apps or tools with the target pre-populated, for example:
  - Open the Ping/TCP app with the current target address.
  - Run a packet Capture on traffic from the test target.
  - Browse to the target URL on the internet with your web browser app.

AutoTest Ping Test

A Ping test sends an ICMP echo request to the selected target to determine whether the server or client can be reached and how long it takes to respond. The AutoTest Target Ping Test sends three Pings to the target and reports the response times. The target can be an IPv4 address, IPv6 address, or named server (URL or DNS).

Ping Test Settings



Name: This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

Device Name: Enter the IP address or URL of the server you want to ping. If you enter an IP

address, the DNS lookup portion of the test is skipped.

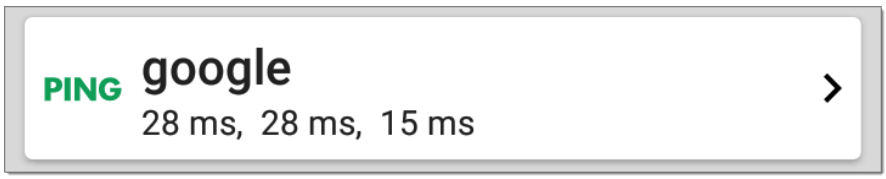
IP Protocol Version: IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Frame Size (bytes): This setting specifies the total size of the payload and the header sent. Valid sizes are 64 bytes to 1518 bytes. To test the Maximum Transmission Unit (MTU) along a route to a target, select the MTU frame size you want to test, and set **Do Not Fragment** to **Enabled**.

Do Not Fragment: Tap the toggle button to enable.

Timeout Threshold: This threshold controls how long the EtherScope waits for a response from the target before failing the test.

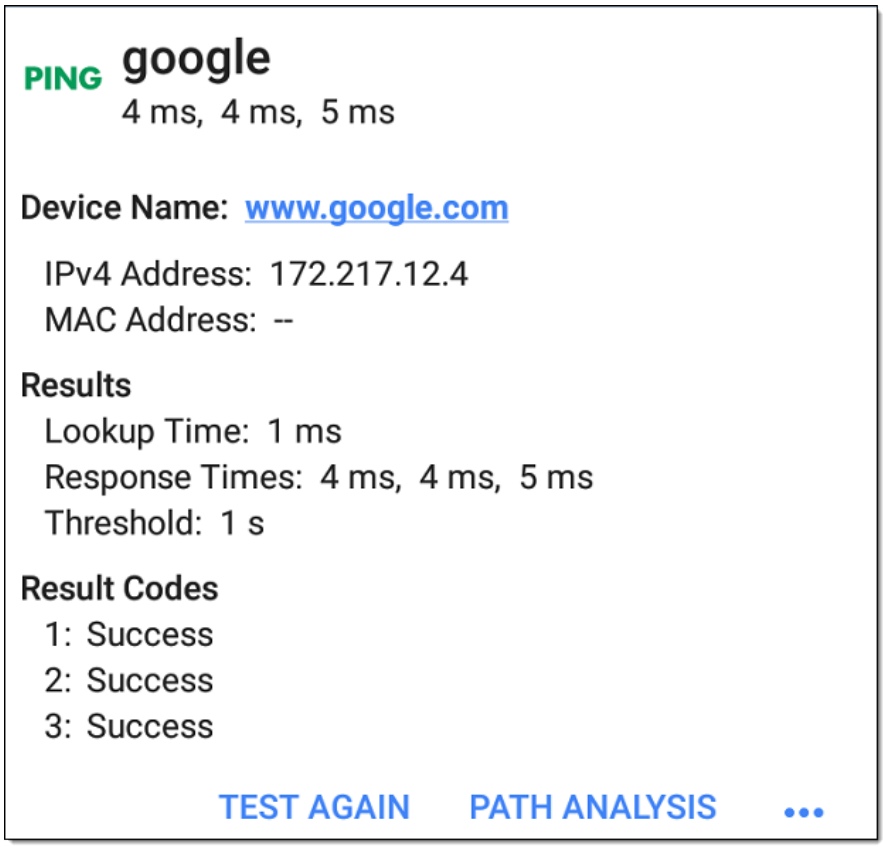
Ping Test Results



The Ping card shows the Ping test name entered in the Ping test settings and the three Ping response times from the target.

Tap the card to open the Ping results screen.

AutoTest Ping Results Screen



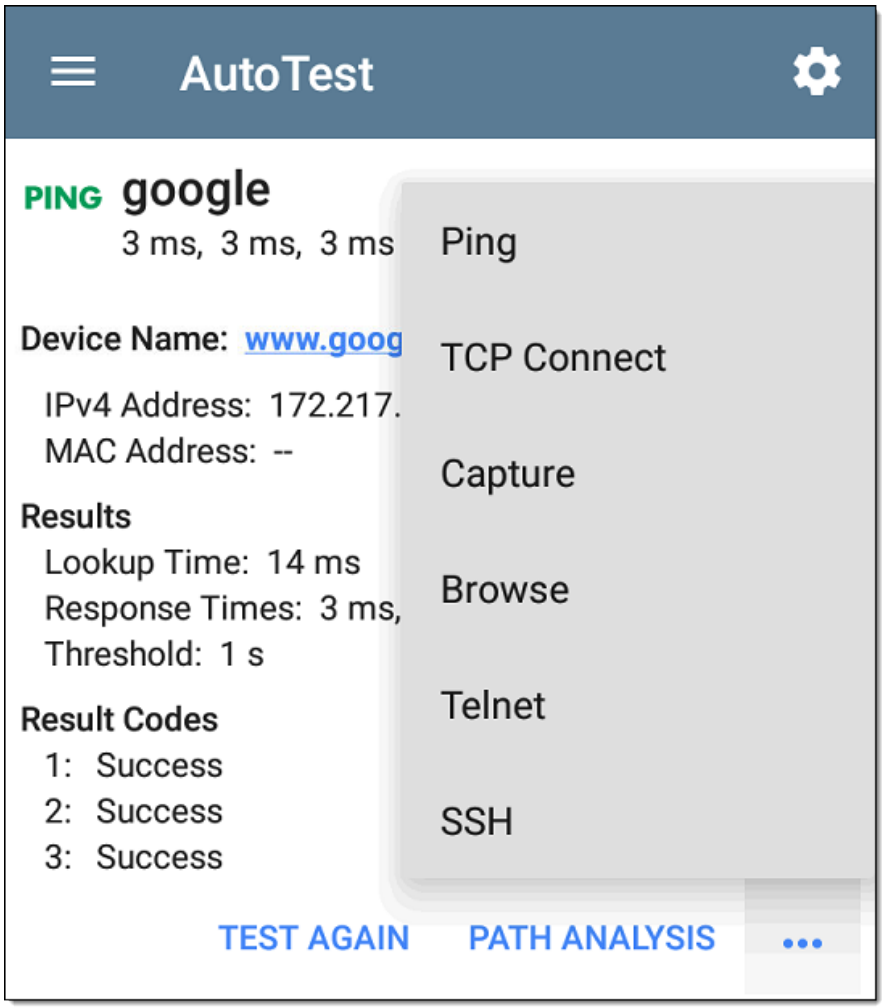
Device Name: Hostname or address of the target device

- **IPv4 or IPv6 Address**: IP address of the target device
- **MAC Address**: Target device's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

Results

- **Lookup Time**: How long it took to resolve the URL into an IP address
- **Response Times**: How long it took for the EtherScope to receive a response from the target after sending each of the three Pings
- **Threshold**: The Timeout Threshold indicated in the test's settings

Results Codes: Final status of the test (Success or Failure) for each of the three Pings

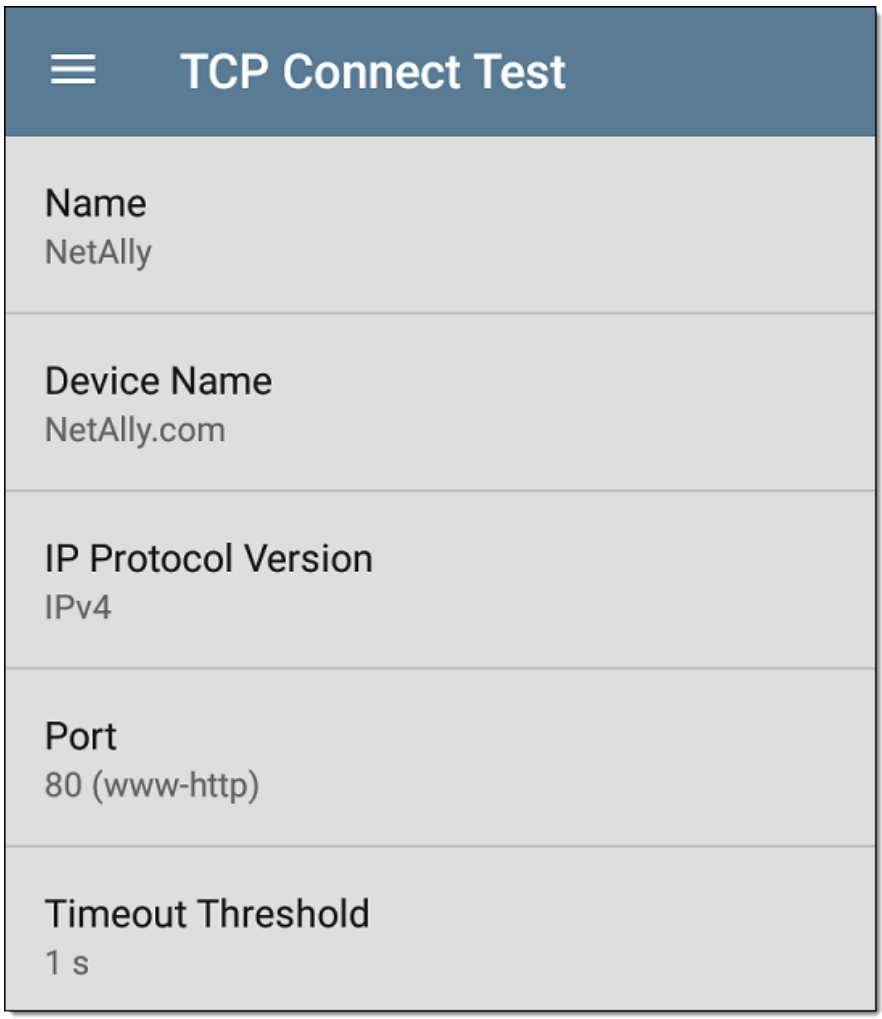


Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the Ping **TEST AGAIN**, open another testing app, **Browse** to the Ping target address in your web browser, or start a Telnet or SSH session.

AutoTest TCP Connect Test

A TCP Connect test opens a TCP connection with the selected target to test for port availability using a 3-way handshake (SYN, SYN/ACK, ACK). The AutoTest Target TCP Connect test runs three connection tests and reports the response times.

TCP Connect Test Settings



Name: This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

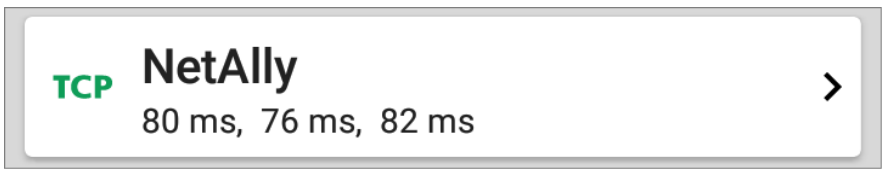
Device Name: Enter the IP address or URL of the target you want to test. If you enter an IP address, the DNS lookup portion of the test is skipped.

IP Protocol Version: IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Port: Specify the TCP port number for the EtherScope to use to connect to the target.

Timeout Threshold: This threshold controls how long the EtherScope waits for a response from the target before failing the test.

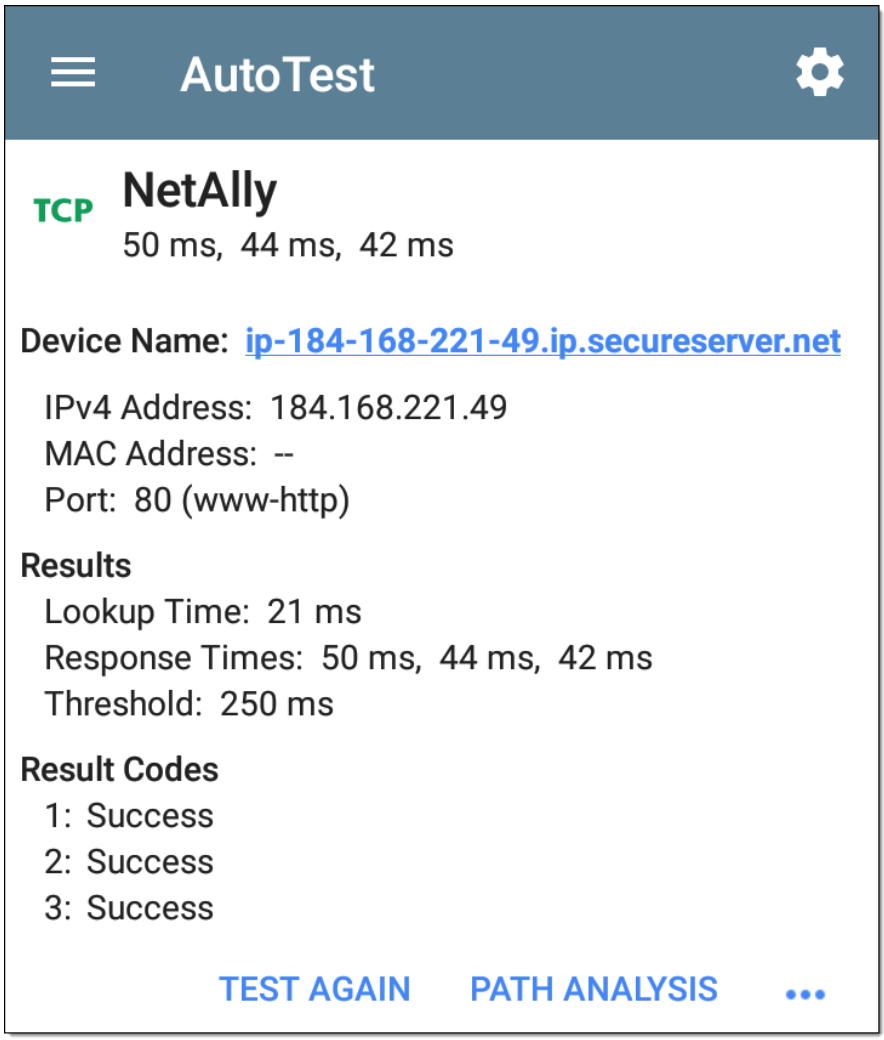
TCP Connect Test Results



The TCP card shows the test name entered in the settings and the three response times from the target.

Tap the card to open the TCP results screen.

AutoTest TCP Results Screen



Device Name: DNS name of the device tested

IPv4 or IPv6 Address: IP address of the target device

MAC Address: Device's MAC address. The two dashes -- indicate that no MAC address was provided.

Port: Port number tested

Results

Lookup Time: How long it took to resolve the URL into an IP address

Response Times: How long it took for the EtherScope to receive a response from the server for each of the three connect tests

Threshold: The Timeout Threshold indicated in the test's settings

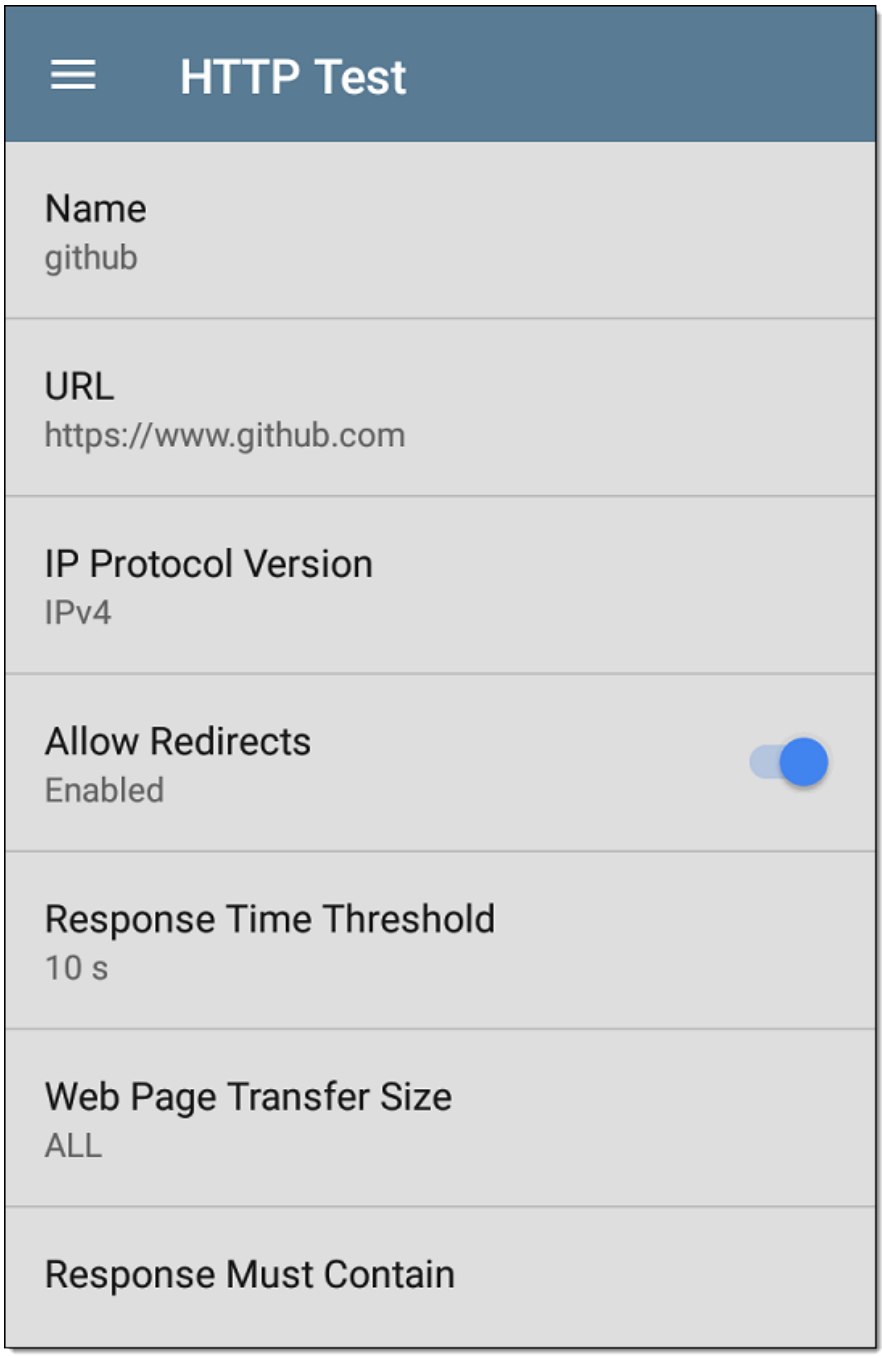
Results Codes: Final status of the test (Success or Failure) for each of the three Pings

HTTP Test

The HTTP test performs a comprehensive end user response time (EURT) measurement when downloading the specified web page. The target can be an IPv4 address, IPv6 address, or URL.

HTTP Test Settings

HTTP settings allow test grading criteria based on responses and return code in addition to the time threshold.



Name

This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

URL

Enter a target address. To reach web servers that operate on a non-default port, enter a colon (:) and specify the port number after the URL.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

Allow Redirects

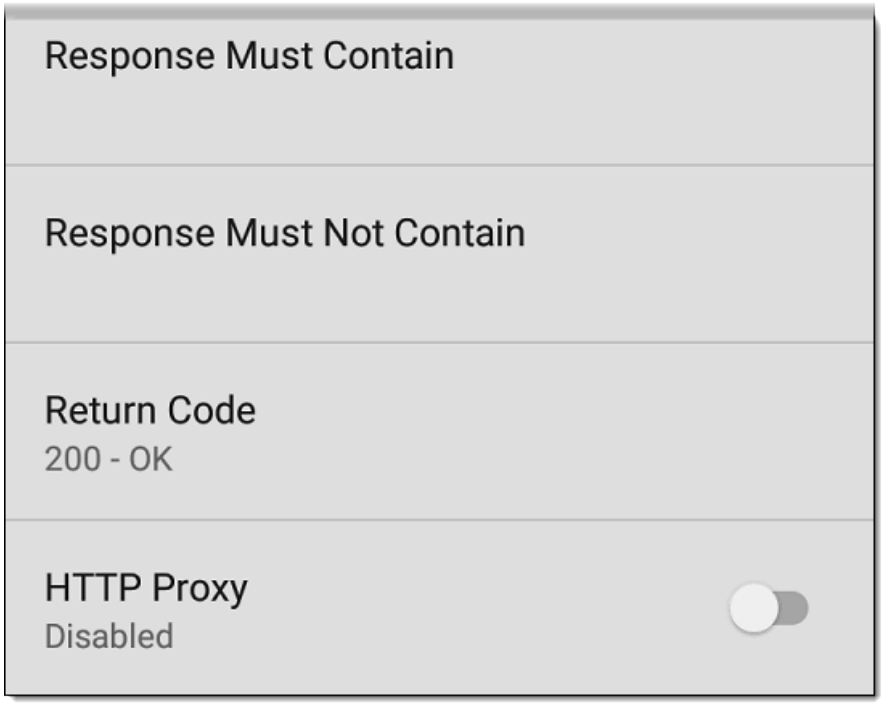
Tap the toggle button to permit web redirects when trying to connect to the target.

Response Time Threshold

This threshold controls how long the EtherScope waits for a response from the URL before failing the test. Tap the field to change the value.

Web Page Transfer Size

This setting allows you to limit the amount of data downloaded, ranging from the HTML **Header Only** to the entire page (**ALL**). Tap the field to select a different transfer size.



Response Must Contain

Text entered here functions as **pass**/**fail** test criteria based on the presence of the text string on a specified server or URL. To construct a text string, enter a word or several words with exact spacing. When specifying several words, they must appear consecutively at the source. The test passes if the text string is found. If the string is not found, the test fails with the Return Code: "Response does not contain required text."

Response Must Not Contain

Like the setting above, except text entered here functions as **pass**/**fail** test criteria based on the

absence of the text string on a specified server or URL. The test passes if the text string is not found. If the string is found, the test fails with the return code: "Response contains excluded text."

Return Code

The Return Code set here functions as **pass**/**fail** test criteria. The default is "OK (HTTP 200)." Tap the field to select a different Return Code from the list. If your selected Return Code value matches the actual return code value, the test passes, and if EtherScope receives a different return code, the test fails.

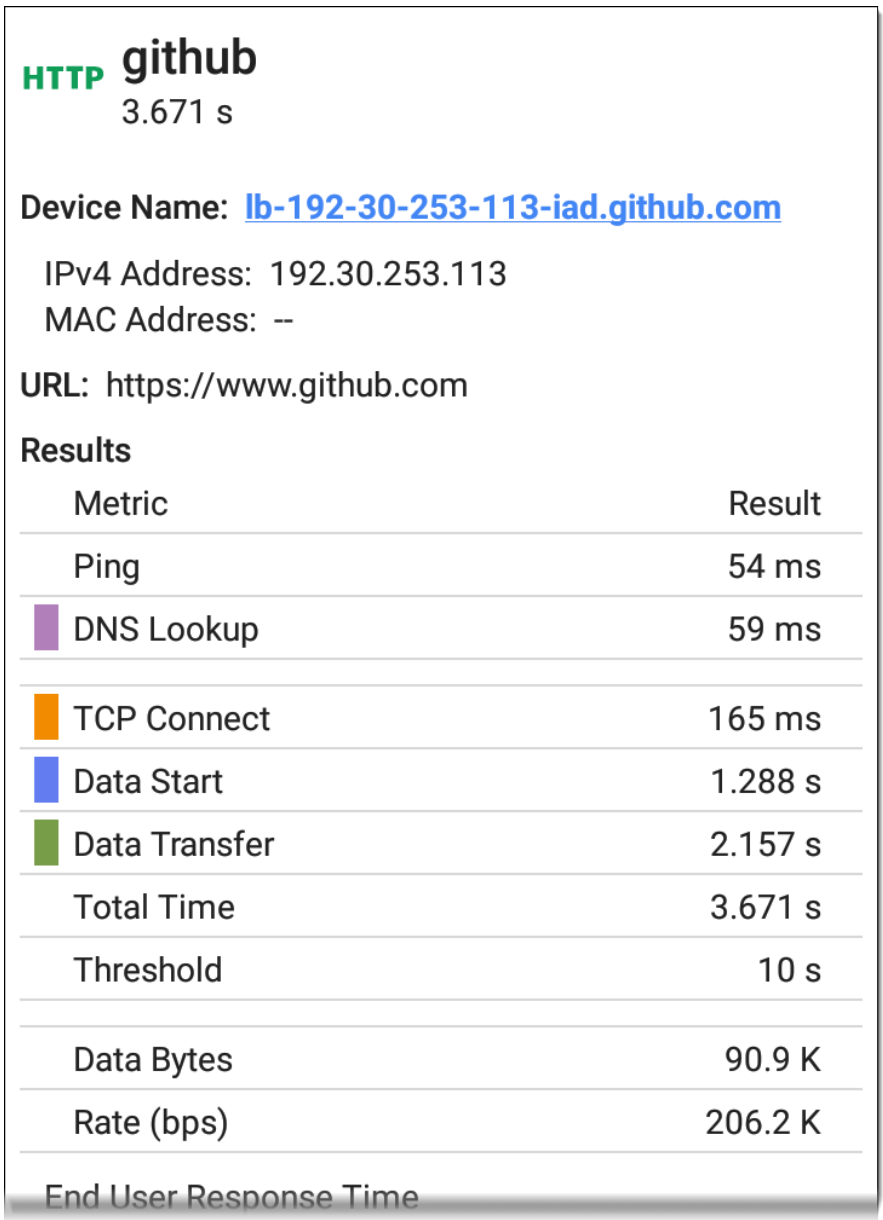
HTTP Proxy

The Proxy control in target test settings uses the server address and port specified in the main profile settings. Tap the toggle to use those Proxy settings. See Wired Profile Settings or Wi-Fi Profile Settings.

HTTP Test Results

The HTTP card shows the test name entered in the test settings and response time from the target.

HTTP Test Results Screen



Device Name: DNS name of the server tested

IPv4 or IPv6 Address: IP address of the server

MAC Address: Server's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

URL: The target URL

Results

Ping: A ping test runs simultaneously with the HTTP test, and this result field displays the Ping response time. If the HTTP test finishes before the ICMP echo reply packet arrives, dashes -- are displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

DNS Lookup: Amount of time it took to resolve the URL to an IP address. If you enter an IP address, DNS lookup is not required, so dashes are displayed to indicate that this part of the test was not executed.

TCP Connect: Amount of time it took to open the port on the server

Data Start: Time to receive the first frame of HTML from the web server

Data Transfer: Time to receive the data from the target server

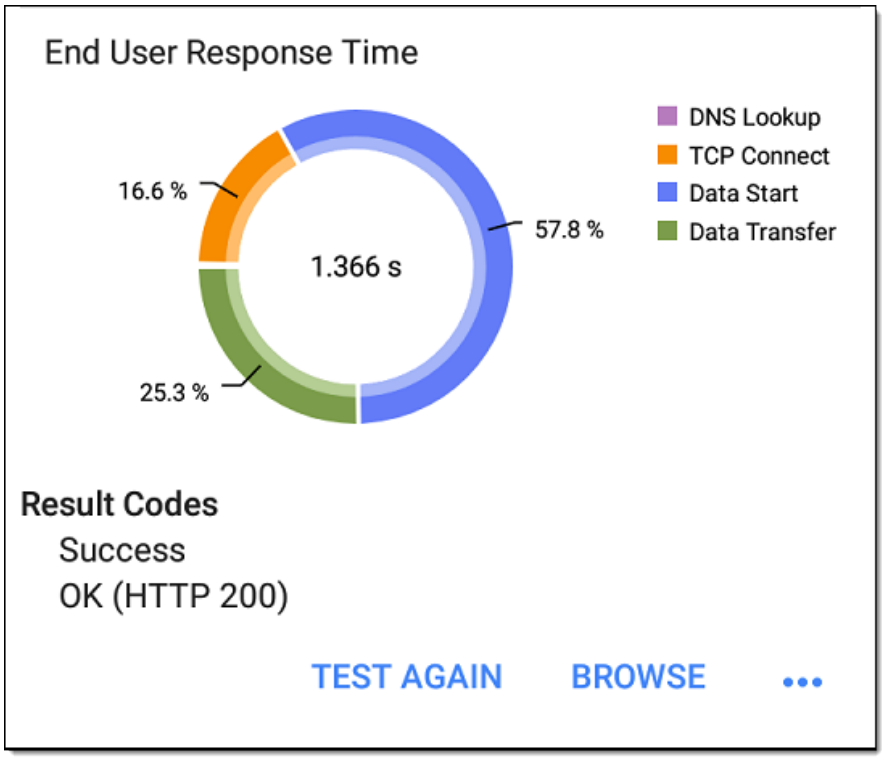
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

If the Response Time Threshold is exceeded during a step in the test, the current phase of the test (DNS, Lookup, TCP Connect, Data Start, or Data Transfer) is denoted with a red dot, and the rest of the test is aborted.

Threshold: The Response Time Threshold from the test settings

Data Bytes: Total number of data bytes transferred. This does not include header bytes

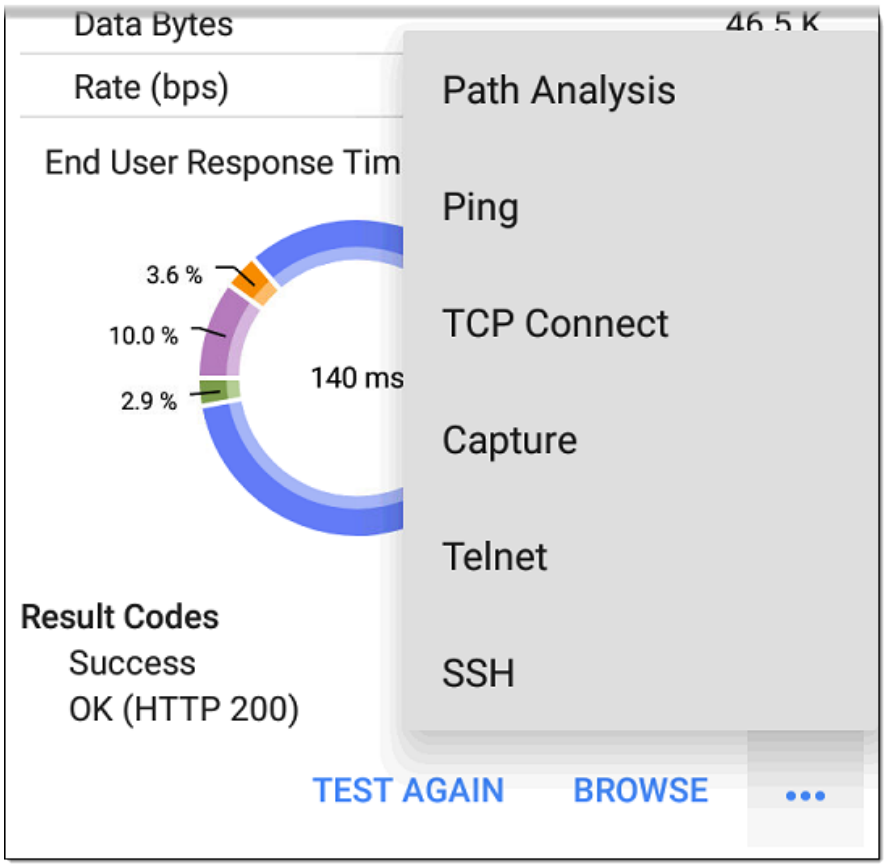
Rate (bps): The measured data transfer rate



End User Response Time : Pie chart of the times for each phase of the test (DNS, Lookup, TCP Connect, Data Start, and Data Transfer)

Results Codes: Final status of the test (Success or Failure)

The HTTP test also shows the **Return Code** from the website server.



Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the HTTP **TEST AGAIN**, open another testing app, or **Browse** to the target address in your web browser.

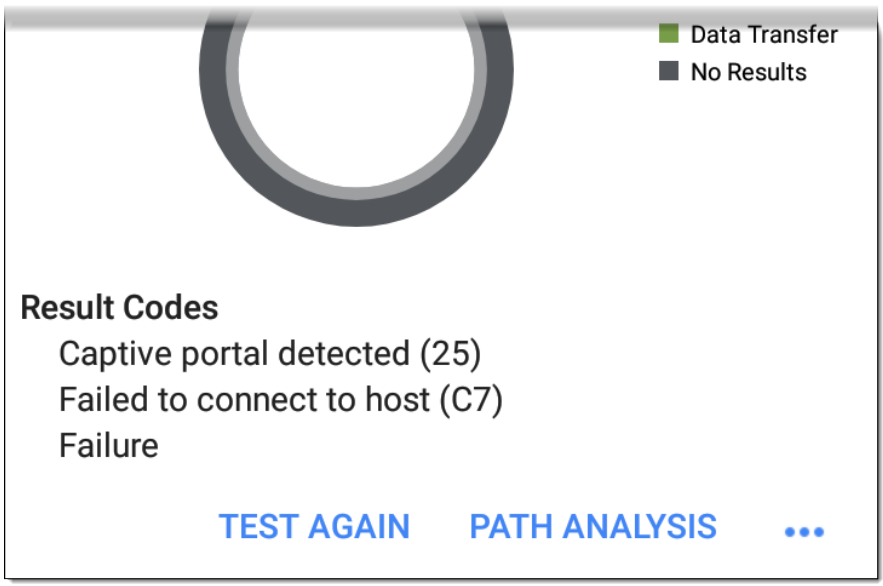
Captive Portal Connections

The HTTP test supports connections through a network with a captive portal requirement.

When running a Profile that connects to a network with a Captive Portal, a system

notification appears to prompt you to enter the captive portal credentials.

For the HTTP test to pass, you must select the notification and enter the required credentials on the portal website. Otherwise, the HTTP test fails, with a Result Code of "Captive portal detected (25)."



See the "Captive Portals" on page 59 for more instructions.

When finished in the captive portal browser window, hit the back button to return to the

HTTP test, and tap **TEST AGAIN** to receive valid results.

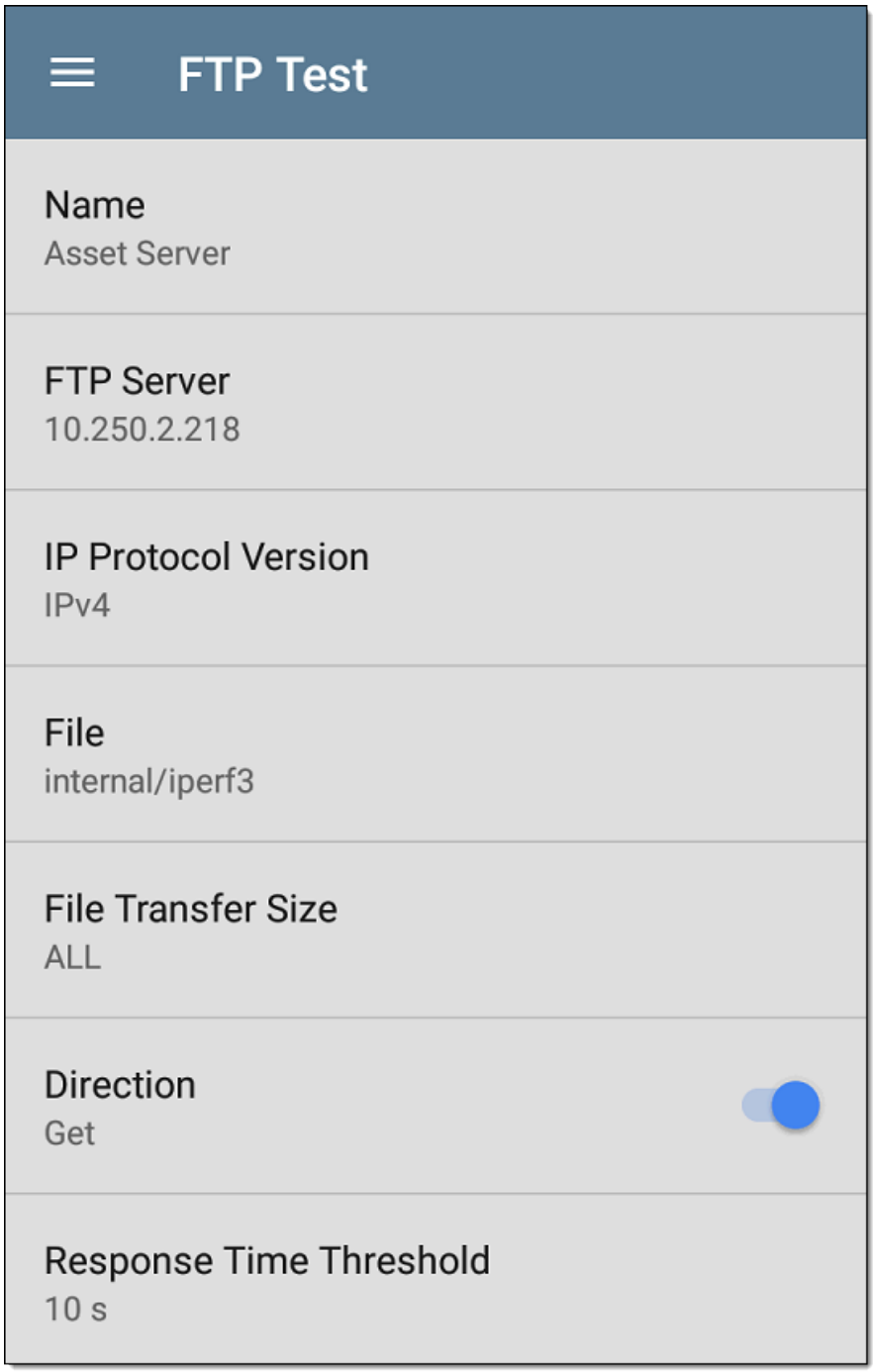
Back to Title and Contents

FTP Test

The FTP test performs a file upload to or download from an FTP server, allowing verification of server and network performance. The target can be an IPv4 address, IPv6 address, or URL. The results provide a complete breakdown of the overall file transfer time into its component parts.

FTP Test Settings

FTP settings allow you to specify a **Get** or **Put** test and the file path and name.



Name

This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

FTP Server

Enter the IPv4 address or URL of the FTP server you want to test. If you enter an IP address, the DNS Lookup portion of the test is skipped.

IP Protocol Version

IPv4 is used by default. Tap the field to switch between IPv4 and IPv6.

File

This setting specifies the path and name of the file that is downloaded from (**Get**) or uploaded to (**Put**) the server, based on the **Direction** setting below. Tap the field to enter the file path and name.

File Transfer Size

This setting lets you limit the amount of data to be downloaded or uploaded. The default transfer size is **ALL**.

- When the **Direction** setting is **Get**, a transfer size of ALL causes the download to continue until the entire file is downloaded or the Response Time Threshold is exceeded.

Specifying a transfer size that is greater than file being retrieved does not cause the test to fail. The test stops when the file has finished downloading.

- When the **Direction** setting is **Put**, the default transfer size of ALL causes the EtherScope to create and upload a file that is 10 MB.

Direction

Tap the toggle button to switch between a **Get** (download the **File** from the server) or **Put** (upload the **File** to the server) test.

- If Direction is set to Get, the file is retrieved, and the size and data rate are calculated. This data is discarded as soon as it is downloaded and is not retained on the EtherScope.
- If Direction is set to Put, the File named above is created on the FTP server. The size of this file is determined by the **File Transfer Size** setting. The file contains a text string indicating that it was sent from the EtherScope, and the test string is repeated to produce the set file size.

Response Time Threshold

This threshold controls how long the EtherScope waits for a response from the FTP server before failing the test. Tap the field to change the value.

Username and Password

Enter these credentials to access the target server you specified. Enter "anonymous" as the username to establish an anonymous connection. The test fails if the configured username or password are not valid on the target FTP server.

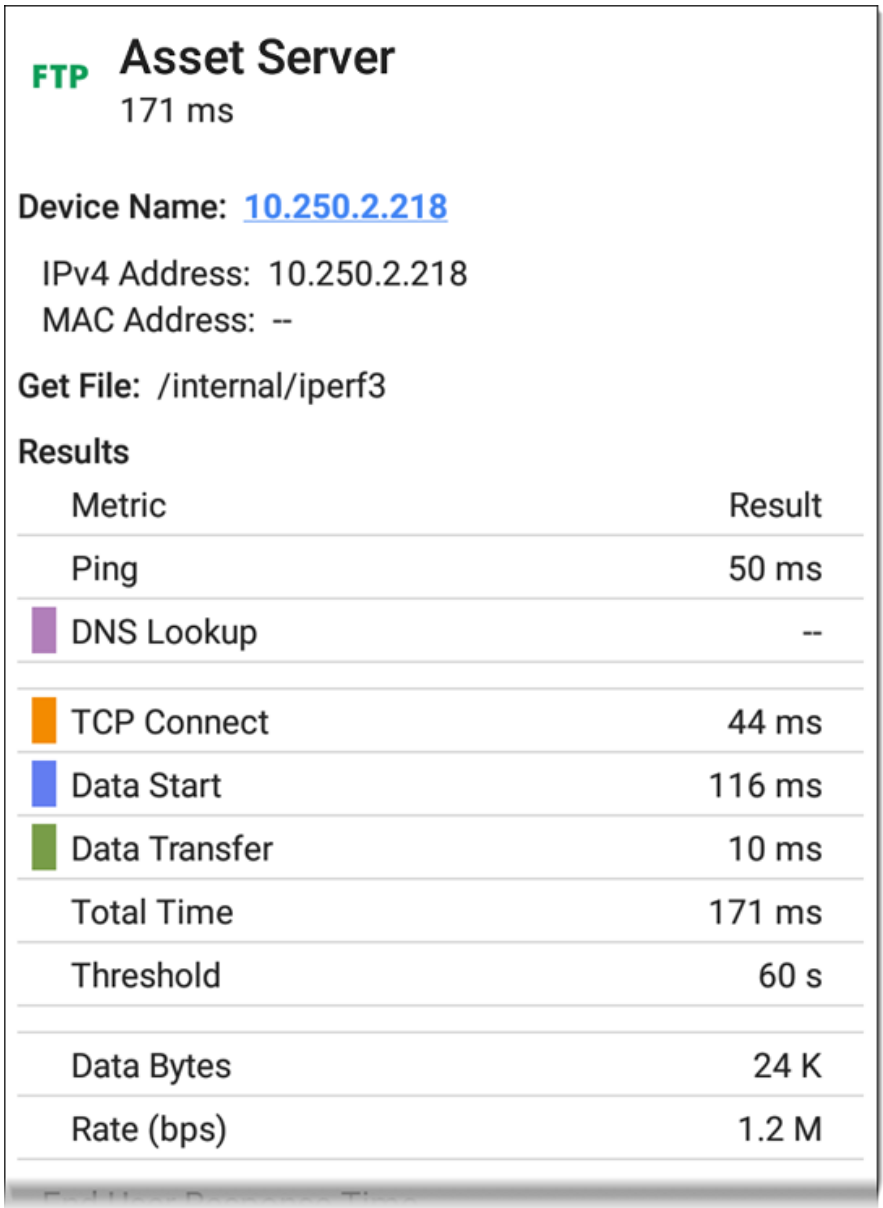
HTTP Proxy

The Proxy control in target test settings uses the server address and port specified in the main profile settings. See Wired Profile Settings or Wi-Fi Profile Settings.

FTP Test Results

The FTP card shows the test name entered in the test settings and response time from the target.

FTP Test Results Screen



Device Name: Hostname of the server tested

IPv4 or IPv6 Address: IP address of the server

MAC Address: Server's MAC address. The two dashes -- indicate that no MAC address was provided from the server.

Get File: File path and name entered in the settings that was transferred to or from the FTP server.

Results

Ping: A ping test runs simultaneously with the FTP test, and this result field displays the Ping response time. If the FTP test finishes before the ICMP echo reply packet arrives, dashes -- are displayed for the ping test results. Ping results do not affect the Pass/Fail status of the test.

DNS Lookup: Amount of time it took to resolve the URL to an IP address. If you enter an IP address, DNS lookup is not required, so dashes are displayed to indicate that this part of the test was not executed.

TCP Connect: Amount of time it took to open the port on the server

Data Start: Time to receive the first frame from the FTP server

Data Transfer: Time to receive the file from the target server

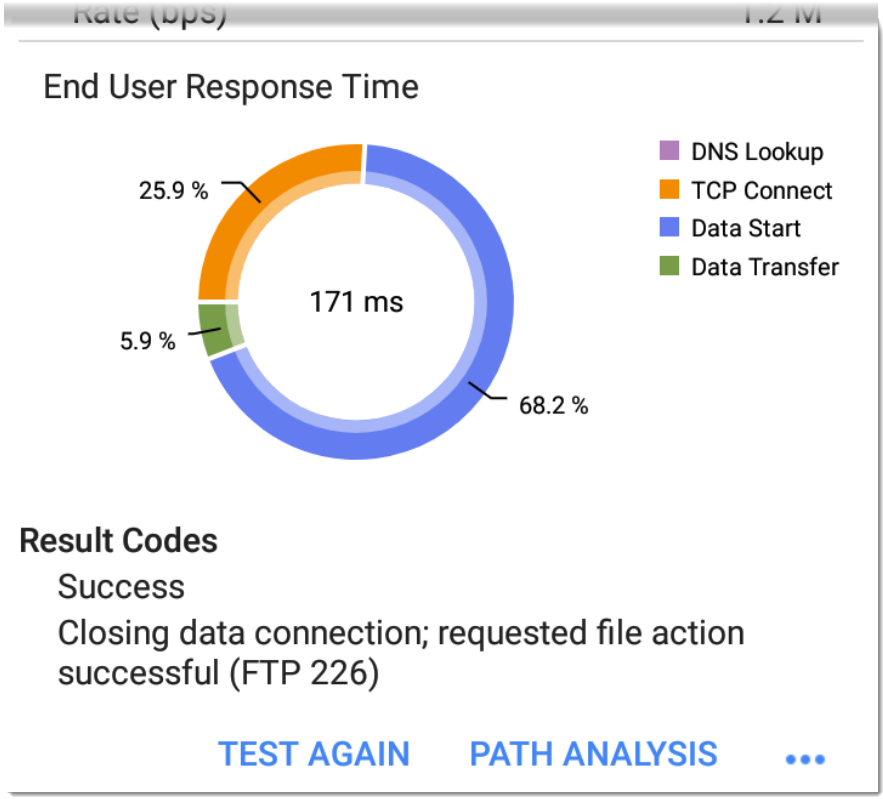
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

If the Response Time Threshold is exceeded during a step in the test, the current phase of the test (DNS, Lookup, TCP Connect, Data Start, or Data Transfer) is denoted with a red dot, and the rest of the test is aborted.

Threshold: The Response Time Threshold from the test settings

Data Bytes: Total number of data bytes transferred. This does not include header bytes.

Rate (bps): The measured data transfer rate



End User Response Time: Pie chart of the times for each phase of the test (DNS, Lookup, TCP Connect, Data Start, and Data Transfer)

Results Codes: Final status of the test (Success or Failure)

The FTP test also shows the **Return Code** from the server.

Tap blue links or the blue action overflow icon ••• at the bottom of the test results screens to run the FTP **Test Again**, open another testing app, or **Browse** to the FTP server in your web browser.

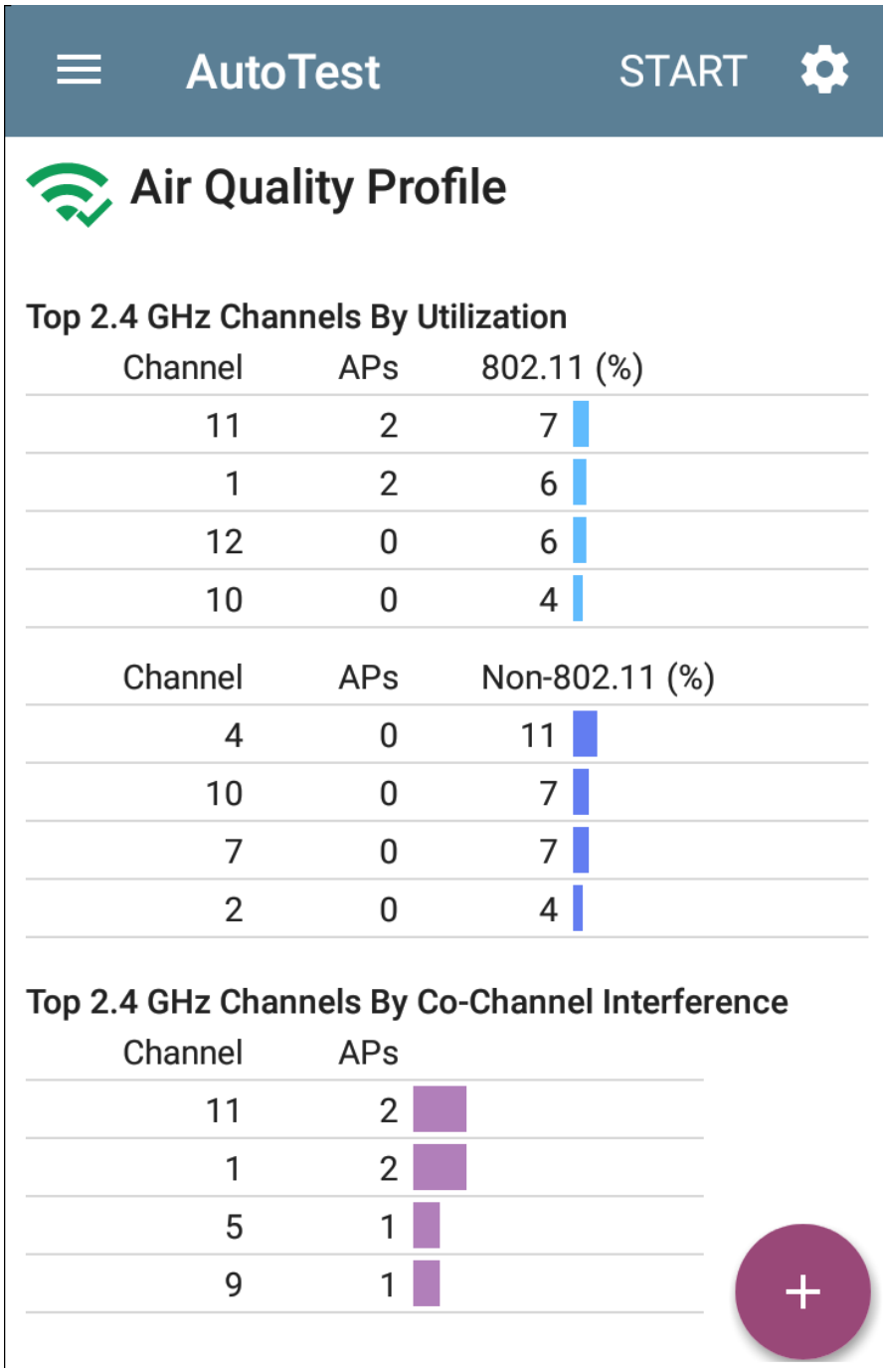
Back to Title and Contents

Air Quality AutoTest Profiles

Air Quality Profiles perform a scan of the channels in your wireless network to measure channel utilization and interference.

Each table on the Air Quality results screen shows the top four channels in each band with the highest utilization, co-channel interference or adjacent channel interference, along with the number of APs operating on the channel.

Air Quality Profile results are described next. Tap here to skip to Air Quality Settings.

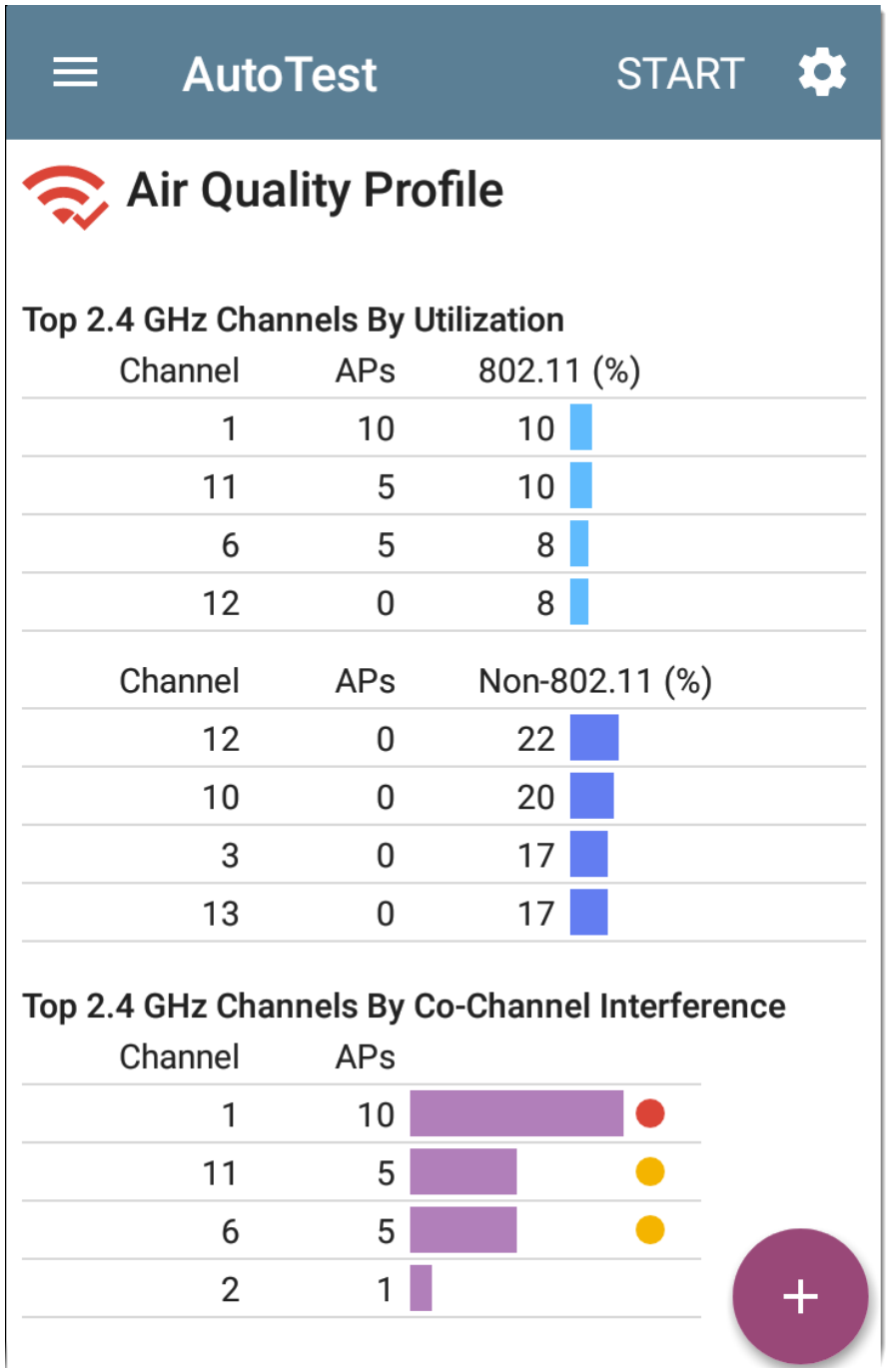


The EtherScope scans the 2.4-GHz band first and displays results and then does the same for the 5-GHz band and then the 6GHz band if applicable.

Channel usage depends on the number of clients connected to the network and the amount of interference from devices like microwaves or smartphones using Bluetooth. Very high utilization or interference can affect network performance.

Air Quality Profile Results

The image below shows a completed Air Quality Profile test with two **Warnings** and two **Failures** indicated by the yellow and red dots next to the corresponding measurements.


AutoTest
START
Air Quality Profile
Top 2.4 GHz Channels By Utilization
Channel APs 802.11 (%)
1 10 10
11 5 10
6 5 8
12 0 8
Channel APs Non-802.11 (%)
12 0 22
10 0 20
3 0 17
13 0 17
Top 2.4 GHz Channels By Co-Channel Interference
Channel APs
1 10
11 5
6 5
2 1

Top 2.4 GHz Channels By Adjacent Channel Interference

Channel	APs
2	15
1	1
6	1
--	--

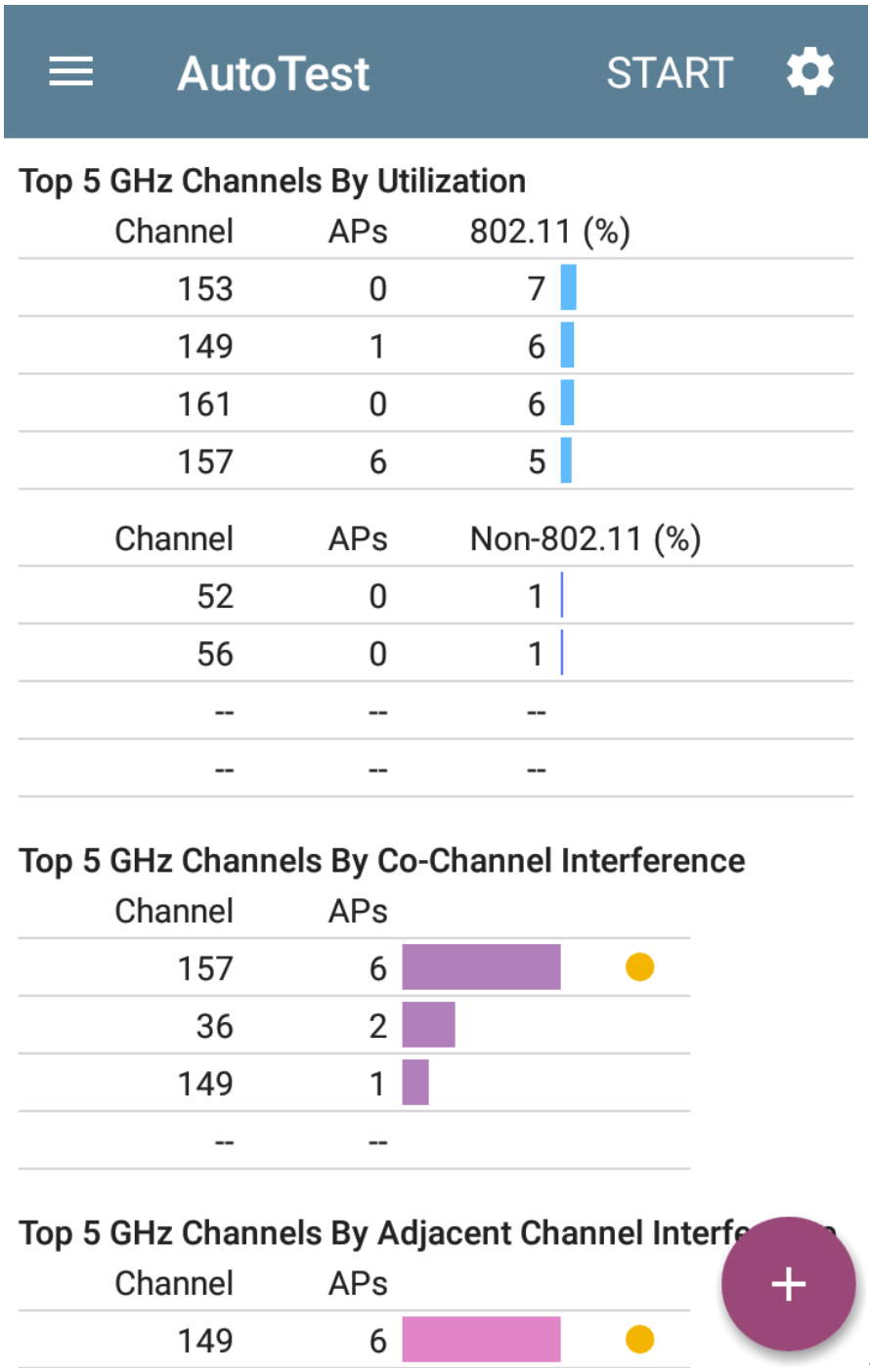
Air Quality test gradings are based on the Thresholds configured in the Profile's settings. In the case shown here, the Warnings and Failures occurred because of high Utilization and Co-channel Interference caused by the number of APs active on the top three 2.4 GHz channels: 1, 6, and 11.

802.11 Utilization %: Percentage of the displayed channel's capacity used by all 802.11 WLAN devices

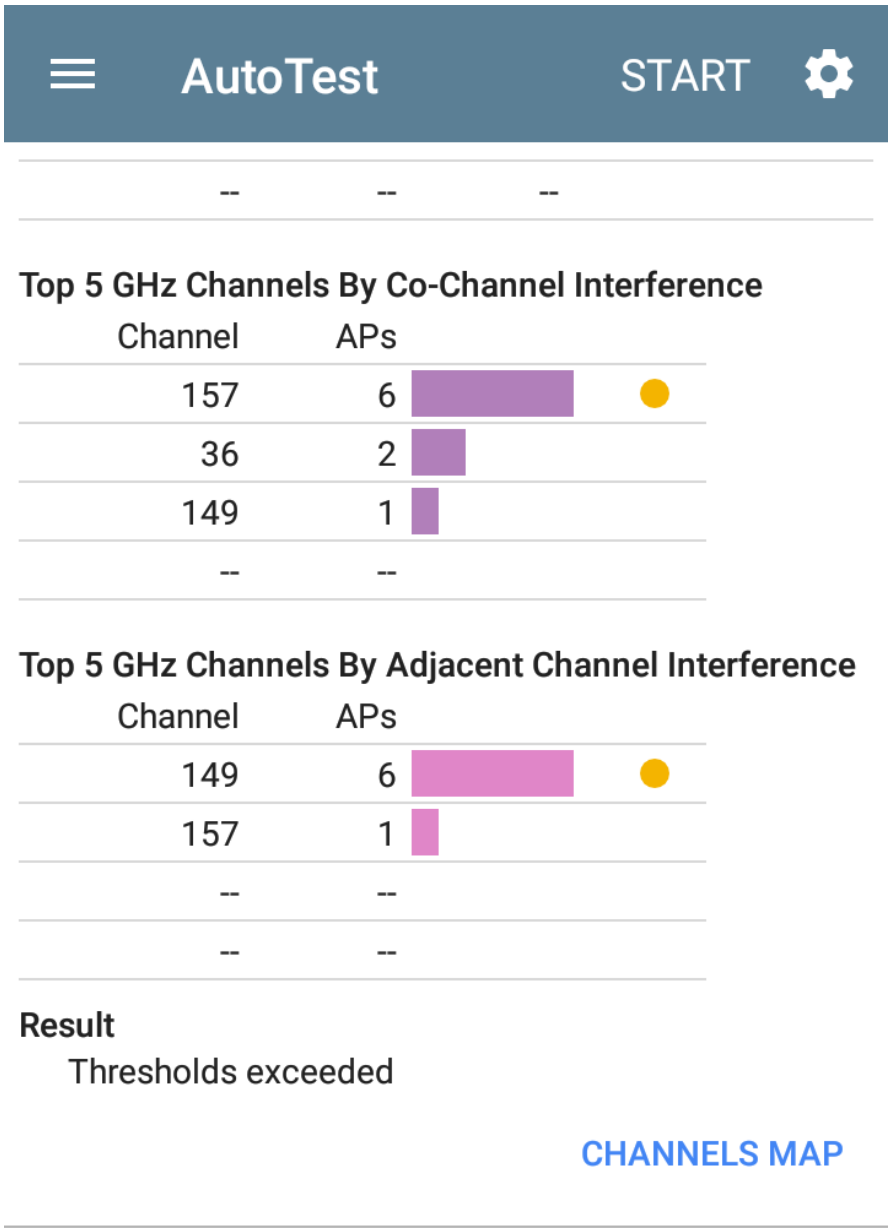
Non-802.11 Utilization %: Percentage of the displayed channel's capacity being used by non-802.11 interferers, which may be non-WLAN sources

(EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, there is only a

single combined 802.11 and non-802.11 Utilization Threshold.



s



Two dashes -- indicate that no Utilization was detected on the Channels shown.

Co-channel Interference: Interference caused by multiple APs operating on the same channel that exceed the minimum **Co-channel Interference AP Signal Level** threshold in the settings. This measurement accounts for 40-MHz and 80-MHz

channels in the 5-GHz band by counting an AP on its primary and each secondary channel.

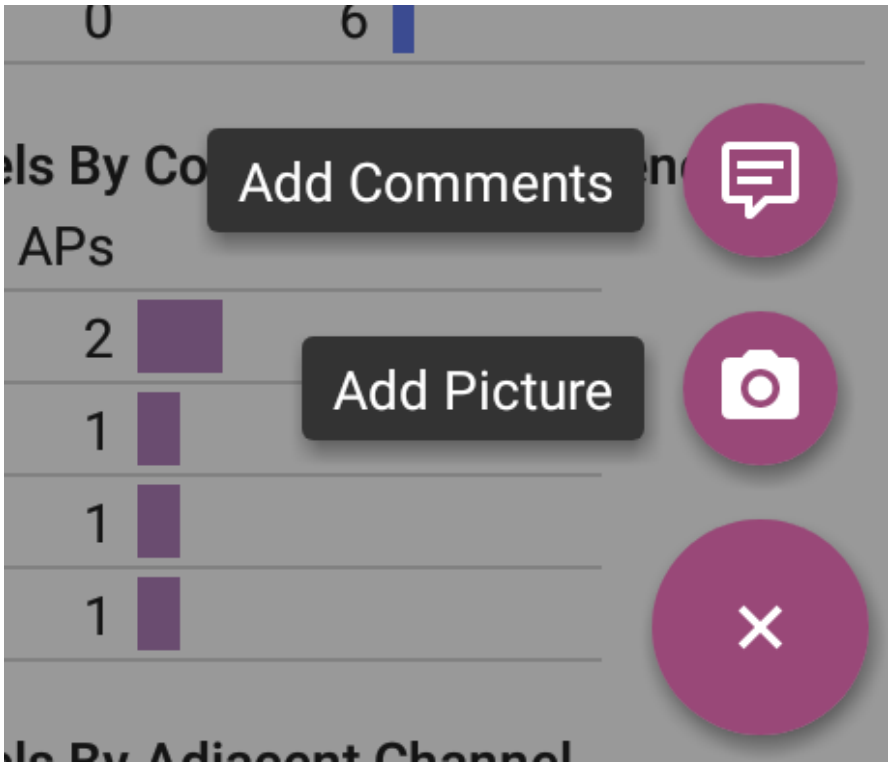
Adjacent Channel Interference: Interference caused by multiple APs operating on adjacent channels that exceed the minimum **Adjacent channel Interference AP Signal Level** threshold in the settings. This is most common in the 2.4 GHz band where channels are 5 MHz apart but span 20 MHz. There are only three channels that do not overlap in this band: 1, 6, 11. Larger channel widths (e.g., 40 MHz) also affects the adjacent channel interference counts.

Results Codes: Final status of the test (Success or Failure)

Tap the blue link at the bottom of the Air Quality Profile screen to open the Wi-Fi app's CHANNELS MAP, which provides real-time visual results of the utilization on each channel.

Air Quality Profile FAB

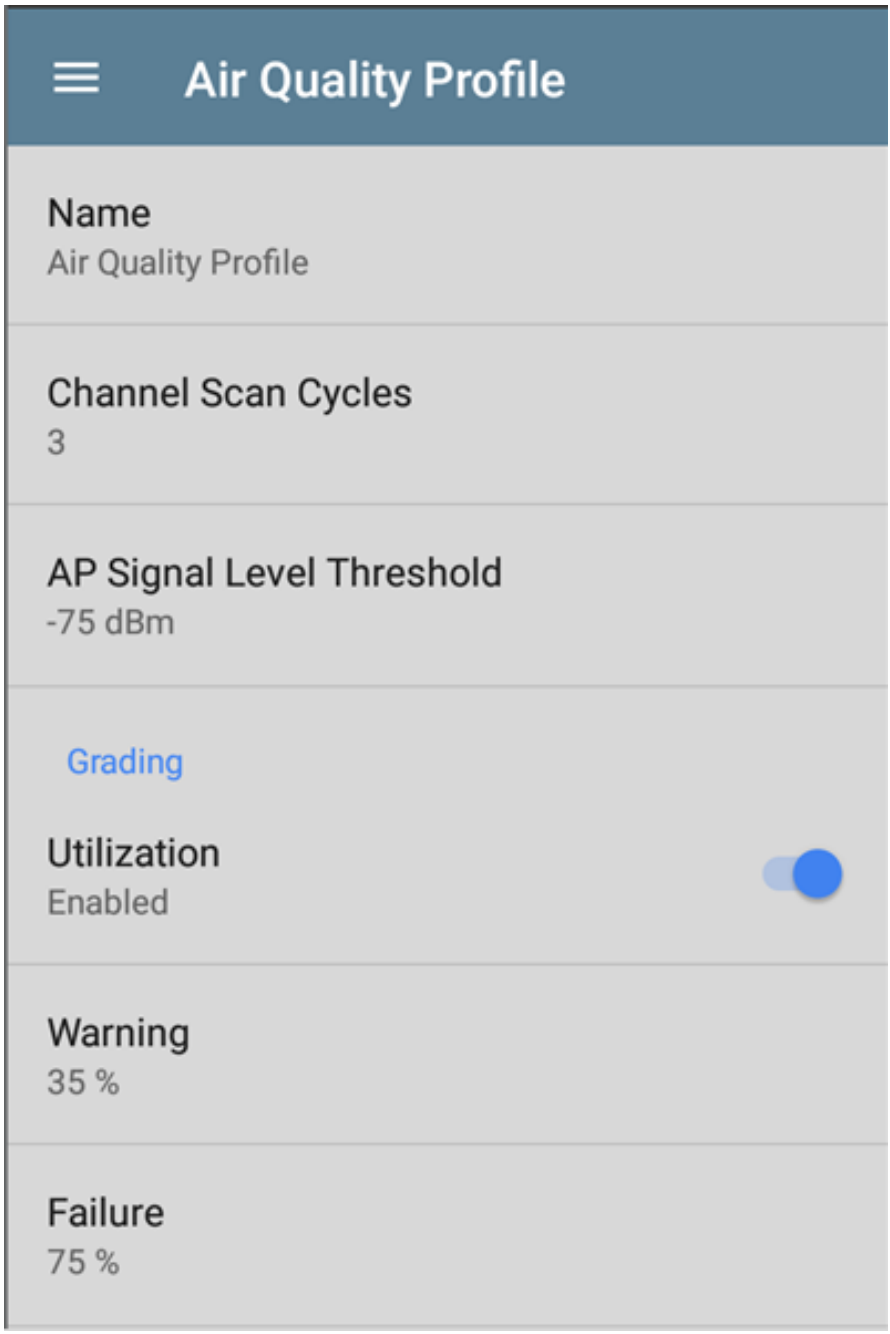
The floating action button (FAB) on the AutoTest Air Quality Profile screen allows you to attach comments and images to this AutoTest result on the Link-Live website.



- The **Add Comments** option opens a Link-Live sharing screen where you can enter comments.
- The **Add Picture** function lets you open the Gallery or Camera app to select or take a photo that is then uploaded and attached to your test result.

Air Quality Profile Settings

To configure the profile settings, tap the settings icon on the Air Quality Profile screen, or add a new Air Quality Profile to AutoTest.



The settings for Air Quality are thresholds for grading the channel utilization and interference.

On the **Air Quality Profile** settings screen, tap each field described below as needed to

configure the profile. Changed settings are automatically applied.

When you finish configuring, tap the back button  to return to the profile.

Name

Tap the **Name** field to enter a custom name for the profile. This name appears on the main AutoTest screen profile card and the Air Quality profile screen header.

Channel Scan Cycles

This setting designates the number of times all of the channels should be scanned before reporting the results. Tap the field to enter a new value between 1 and 10.

AP Signal Level Threshold

This setting designates the minimum signal level at which an AP must be measured to be counted in Co-Channel and Adjacent Channel Interference measurements. Tap the field to select a new value or enter a custom one.

Grading

Use the grading threshold controls to adjust the values that determine **Warning**/**Fail** results for the corresponding utilization and co-channel interference and adjacent channel measurements. Tap each Warning or Failure field to select a new value or enter a custom one. Each threshold also has a toggle button that allows you to disable grading based on that measurement entirely.

Thresholds

Use the threshold controls to adjust the values that determine **Warning**/**Fail** results for the corresponding utilization and co-channel interference and adjacent channel measurements. Tap each Warning or Failure field to select a new value or enter a custom one. Each threshold also has a toggle button that allows you to disable grading based on that measurement entirely.

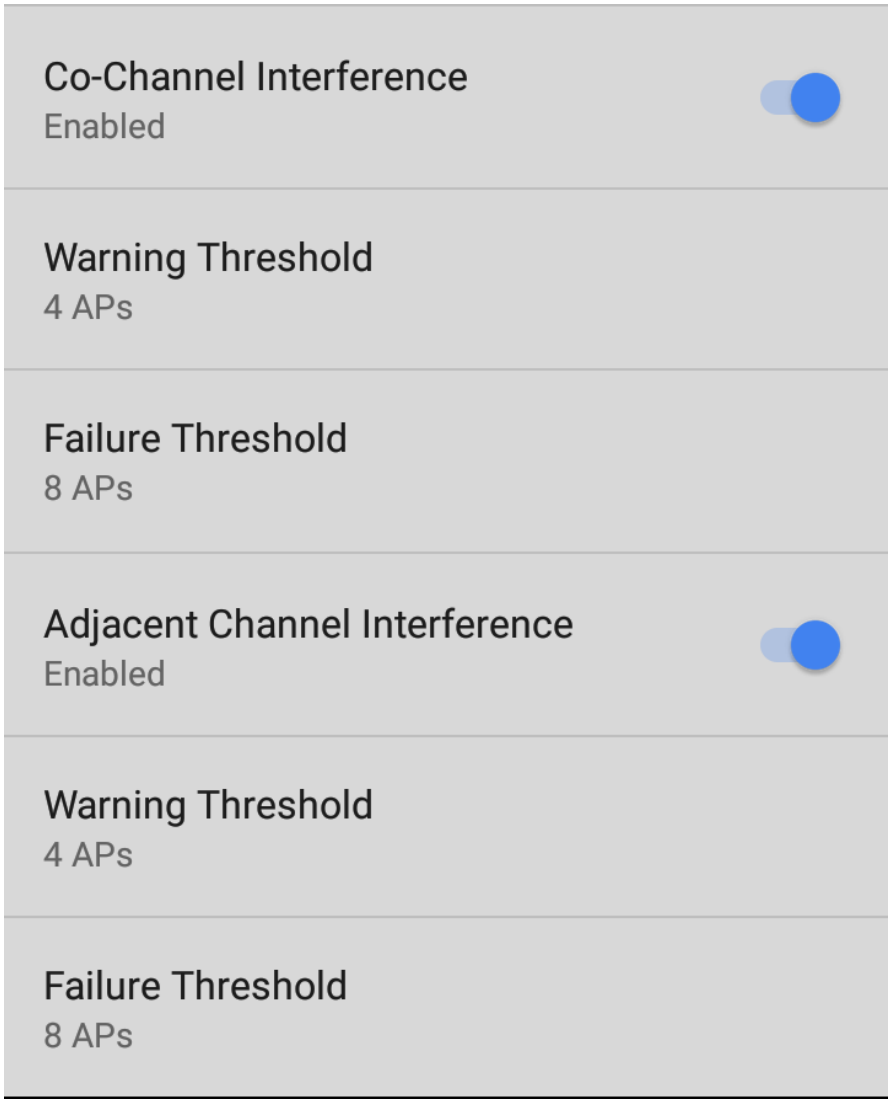
By default, you can set thresholds for both 802.11 and non-802.11 Utilization.

(EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, there is only a

single combined 802.11 and non-802.11 Utilization Threshold.

Utilization measurements and thresholds are percentages of a channel's capacity. Co-channel interference measurements and thresholds are the number of APs operating on the same channel.

Adjacent Channel Interference measurements and thresholds are the number of APs operating on nearby channels that cause interference.



Back to Title and Contents

Ping/TCP Test App

The Ping/TCP test app runs a Ping or TCP Connect test to your chosen target, allowing you to monitor connectivity changes.

A Ping test sends an ICMP echo request to the selected target to determine whether the server or client can be reached and how long it takes to respond. A TCP Connect test opens a TCP connection with the selected target to test for port availability using a 3-way handshake (SYN, SYN/ACK, ACK).

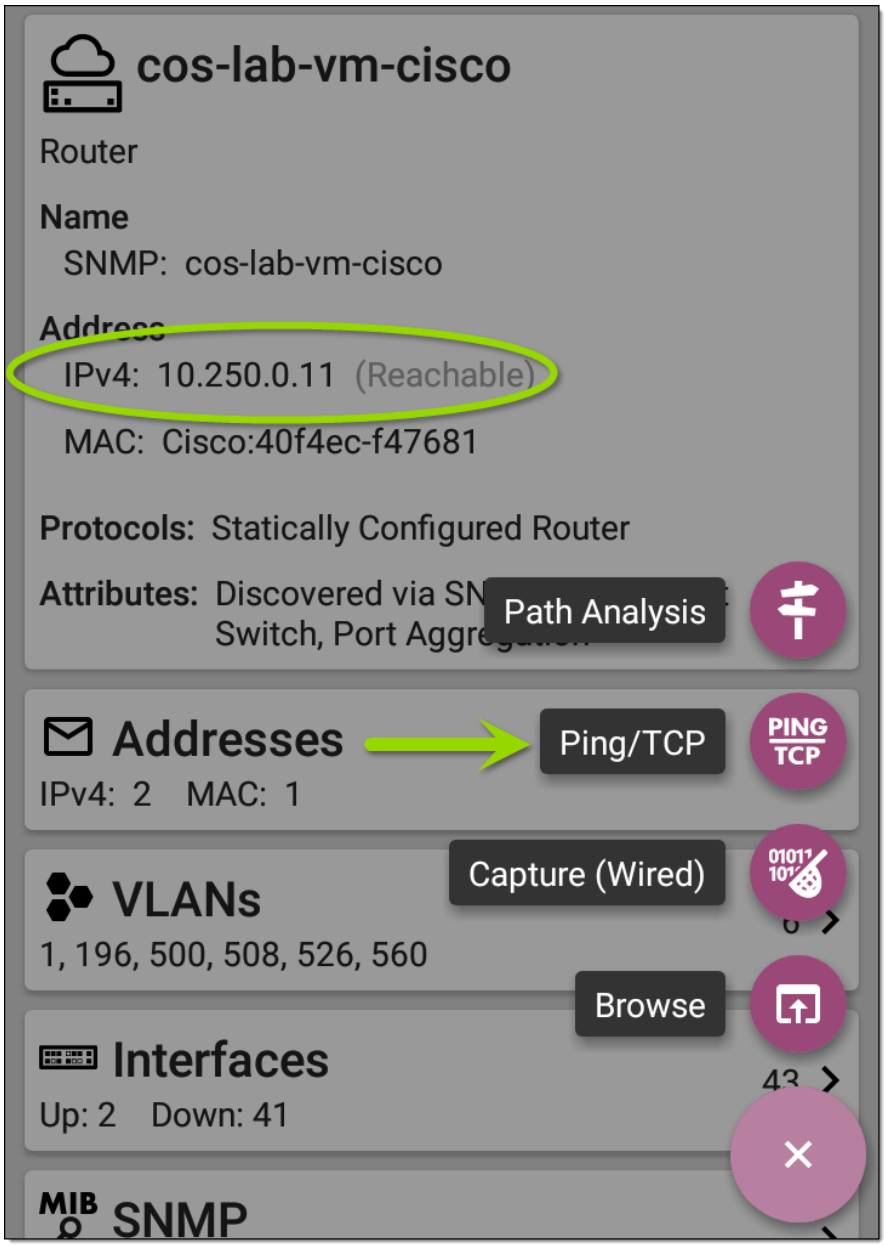
You can open the TCP/Ping app from the Home screen, or you can select **Ping** or **TCP Connect** from another app, such as AutoTest or Discovery, while viewing a device's details.

Ping/TCP Settings

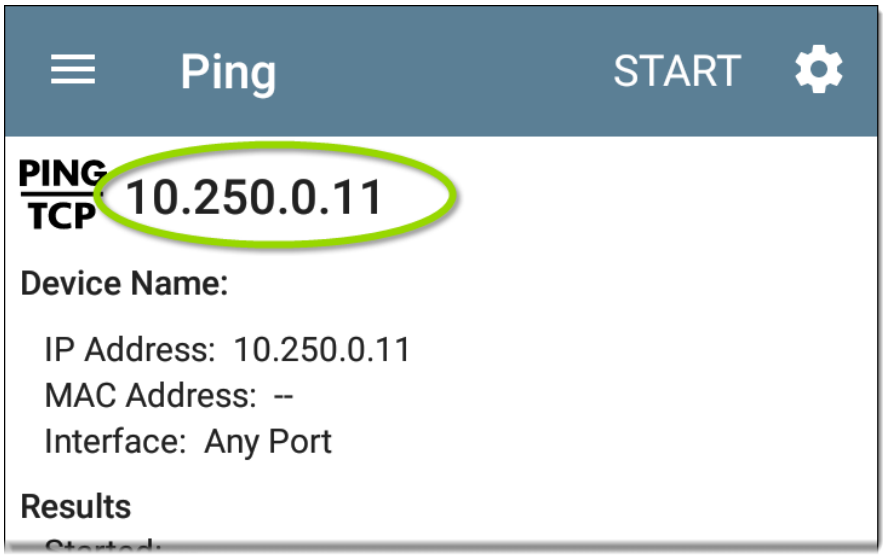
To configure a test, you can manually enter a hostname or IP address in the settings, or you can select Ping or TCP Connect from another testing app's device screen.

Populating Ping/TCP from Another App

When you open the Ping/TCP app from another app, the address is pre-populated as the Ping or TCP target device. For example, the floating action button (FAB) menu on the Discovery app screen shown below contains the option to open the Ping/TCP app.

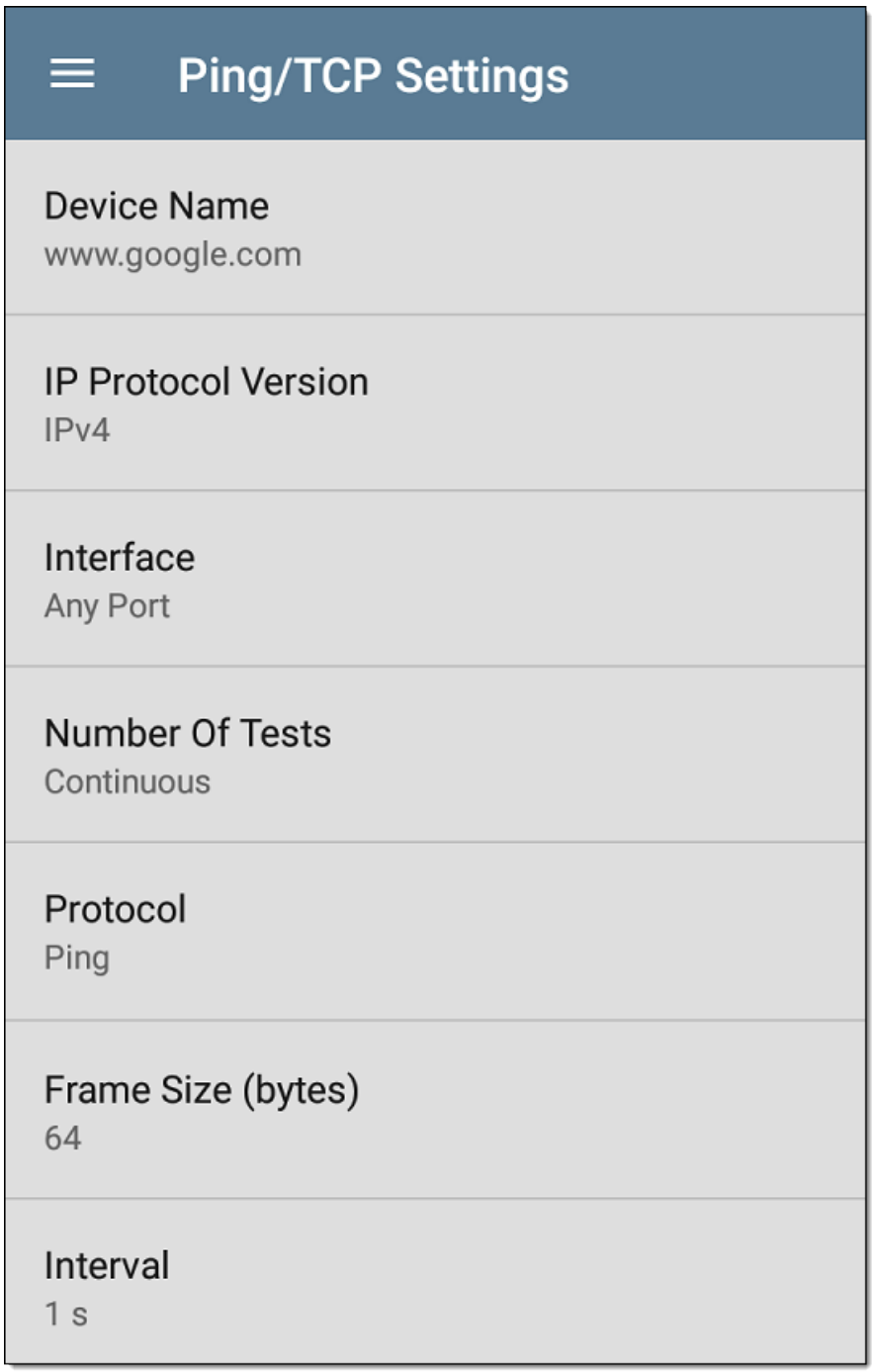


If the Ping/TCP app is opened from this screen, the IPv4 address from the Discovery app is already configured as the Ping/TCP target.


Ping
START
PING
TCP
10.250.0.11
Device Name:
IP Address: 10.250.0.11
MAC Address: --
Interface: Any Port
Results

Configuring Ping/TCP Settings Manually

To configure the target and settings manually, open the app's settings .



Device Name: Enter the IP address or DNS name of the target.

IP Protocol Version: IPv4 is used by default. Tap the field to enable IPv6 instead.

Interface: This setting determines the EtherScope port from which the port scan runs. Tap the field to select the port. (See Selecting Ports for explanations of the different ports.)

Number of Tests: Tap to select the number of Ping or TCP connect tests you want to run. The default setting of **Continuous** keeps running tests until you tap the **STOP** button.

Protocol: Tap to select the **Ping** or **TCP Connect** protocol for the test.

Some of the following settings depend on the selected protocol.

Frame Size (bytes): This setting only appears if the **Ping** Protocol is selected. It specifies the total size of the payload and header the EtherScope sends. Tap a radio button to select a new size, or enter a Custom Value from 64 to 1518 bytes.

To test the Maximum Transmission Unit (MTU) along a route to a target, select the MTU frame size you want to test, and set the **Do Not Fragment** setting (below) to **Enabled**.

Interval: This setting only appears if the **Ping** Protocol is selected. It controls how much time passes between each Ping sent from the EtherScope. By default, Pings are sent once every second (1 s). Tap a radio button to select a different interval, or enter a Custom Value between 100 and 10,000 milliseconds.

Port: This setting only appears if the **TCP Connect** Protocol is selected. It indicates the port number your EtherScope uses to connect to the target address for a TCP Port Open test. If needed, tap the **Port** field to open a pop-up number pad and enter a new port number. Tap **OK** to save it.

Timeout Threshold: This threshold controls how long the EtherScope waits for a response from the target before the test is failed.

Do Not Fragment: This setting only appears if the **Ping** Protocol is selected. Tap the toggle

button to enable. See the Frame Size setting description above.

Back to Title and Contents

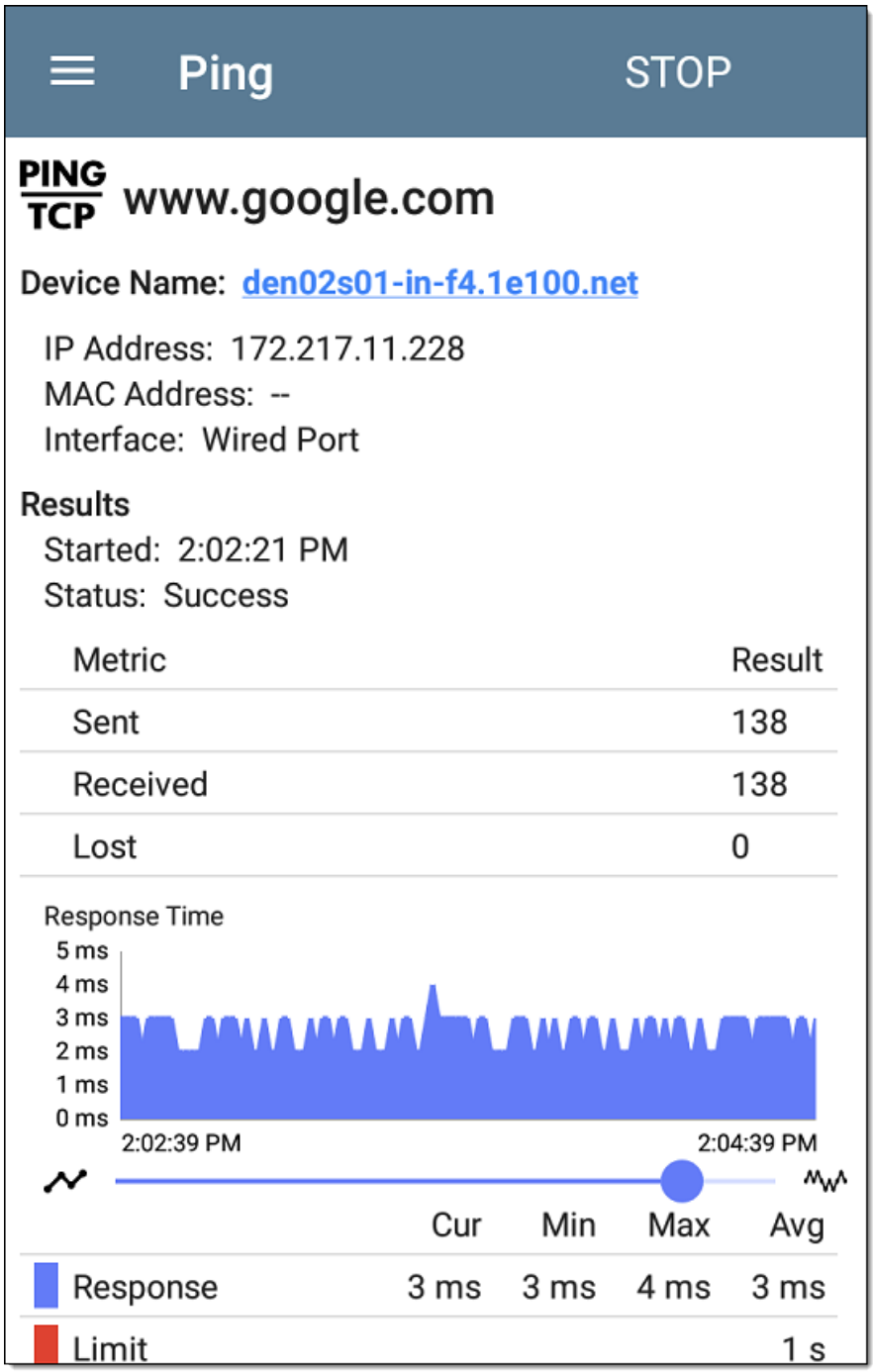
Running Ping/TCP Tests

Your unit must be connected to an active network (Test or Management Port) to run Ping and TCP Connect tests. Icons in the top Status Bar indicate whether and how your EtherScope is connected. See Connection Notifications for descriptions of the connection status icons, and select the appropriate **Interface** (or Any Port) from the Ping/TCP settings.

The default target is google.com. Open the app settings  to enter a new target.

To begin the test, tap **START**.

If the Number of Tests setting is set to **Continuous**, the Ping/TCP app runs tests to your selected target until you tap **STOP**.



Device Name: Hostname or address of the target device

IPv4 or IPv6 Address: IP address of the target device

MAC Address: Target device's MAC address. The two dashes -- indicate that no MAC address was provided from the device.

Port: The port number used for the TCP Connect test. This field does not appear in Ping test results.

Interface: The EtherScope Test or Management Port from which the test is running

Results

- **Started**: Time the test started
- **Status**: Most recent test status
- **Sent**: Number of Pings or TCP SYN packets sent to the target
- **Received**: Number of Ping or TCP SYN/ACK packets returned from the target
- **Lost**: Number of Pings or TCP packets that were not returned from the target

Response Time graph: Plots the target device's response times in milliseconds. The graph saves and displays data for up to 24 hours in the past if the unit stays linked.

To pan and zoom on the graph, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

Response: Table display of the Current, Minimum, Maximum, and Average response time measurements

Limit: The **Timeout Threshold** from the Ping/TCP app's settings

Back to Title and Contents

Capture App

Packet capture is the process of recording network traffic in the form of packets as data streams back and forth over Wi-Fi or wired connections. Packet captures can help you analyze network problems, debug client/server communications, track applications and content, ensure that users are adhering to administration policies, and verify network security.

The capture process uses the Wired or Wi-Fi Test port.

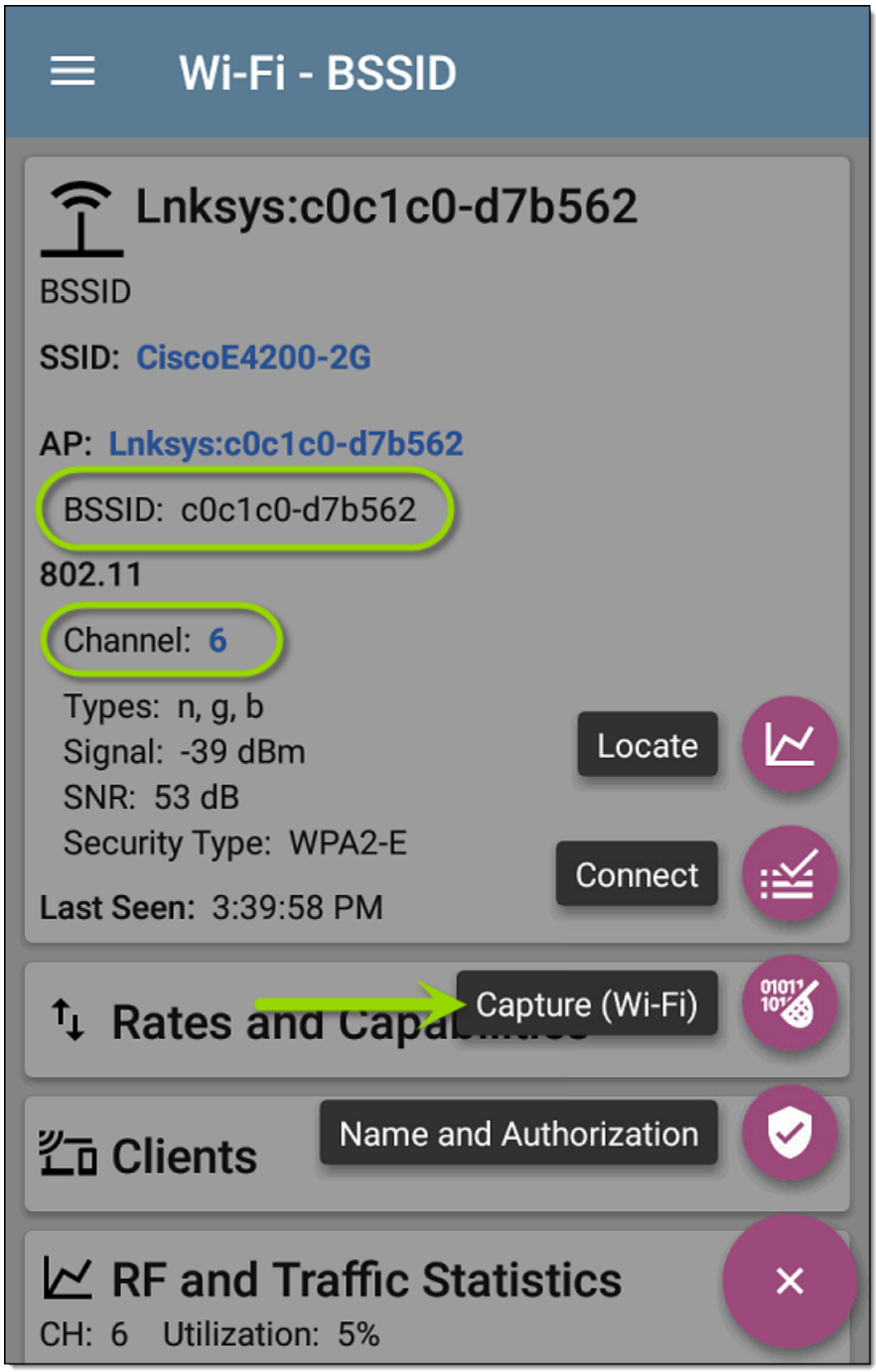
You can open the Capture app from the Home screen or using a link from another app, such as AutoTest, Discovery, or Wi-Fi.

Capture Settings

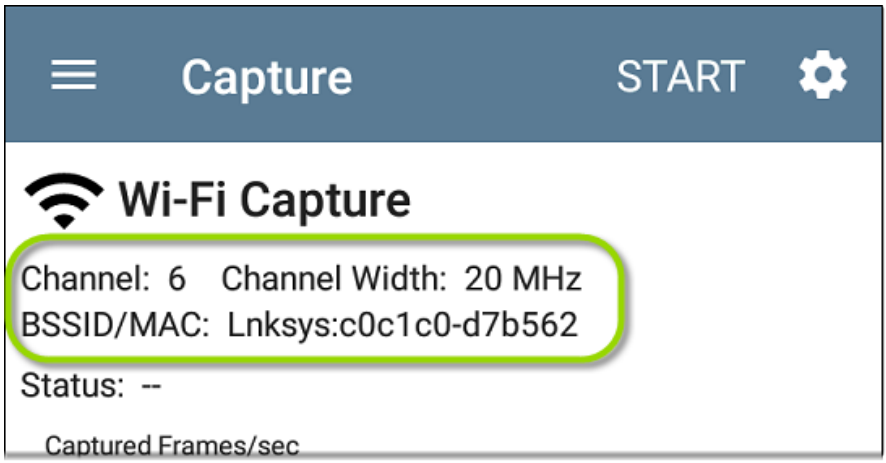
The Capture app settings allow you to switch between Wired and Wi-Fi, designate file and slice sizes, and apply filters to capture and analyze only certain packet types. For example, you can set a wired filter to capture only packets related to a specific application (based on IP address and port number), or create a Wi-Fi filter to capture only packets to and from a particular AP or client.

When you open Capture from Home and do not configure any filters, all packets from the switch or channel are captured. The default Wired capture saves all the packets sent from the local switch to the EtherScope. The default Wi-Fi capture saves the packets seen on channel 1.

If you open the Capture app from another NetAlly test app, Capture filters are automatically applied. Filters that can be applied from other apps include Wired IP and MAC or Wi-Fi Channel, Channel Width, and BSSID.
For example, the floating action menu on the Wi-Fi app's BSSID Details screen below contains the option to start a Wi-Fi Capture.

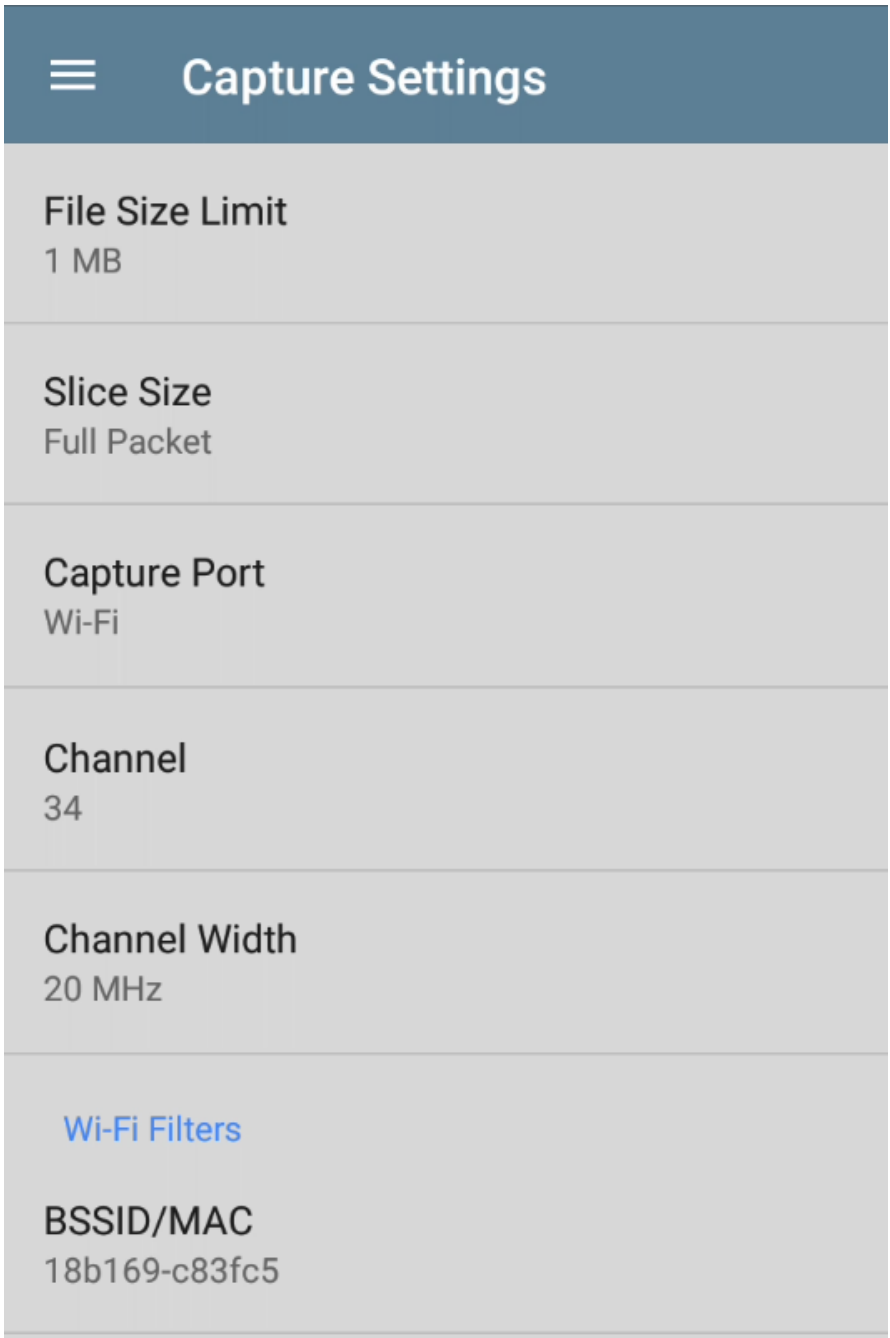


When the Capture app opens, filters are already set with the BSSID, Channel, and Channel Width from the Wi-Fi app.



The Capture settings are saved until you clear the filters or open the app with new filters applied.

Tap the settings icon in the Capture screen to configure capture settings.



File Size Limit: Tap this field to specify a size for the capture file. The default size is 1 MB, and largest size allowed is 1000 MB. The capture stops when the captured file reaches this size.

When capture is running, the capture screen displays the current file size as data is captured.

Slice Size: Tap this field to select a specific frame slice size or enter a custom value. The Slice Size setting limits how much of each packet is captured. A smaller slice size is useful when you are interested in the packet's header but do not need to see all the payload data. The default is Full Packet.
Capture Port: Tap to select either the **Wired** or **Wi-Fi** test port.

Wired Filters

All filters are disabled by default unless you open Capture from another app. Tap the fields below to enable the filter and enter filter values.

MAC: Enter the MAC address of a host to capture only packets that contain the host's MAC address as the source or destination.

IP: Enter the IPv4 or IPv6 address of a host to capture only traffic to and from the host.

VLAN: Enter a VLAN number to capture only traffic tagged for that VLAN.

Port: Specify a port number to capture only traffic from that UDP or TCP port. For example, select port 80 to capture HTTP traffic only.

NOT: Sets up a logical NOT to use with capture values you have set up with other filters. For example, if you set up a filter to capture traffic to and from IP 10.250.0.70 on Port 80, and then you enable NOT, the EtherScope nXG captures all traffic *except* traffic to and from 10.250.0.70 on port 80.

Wi-Fi Filters

Channel: Tap the channel button to set the channel on which packets are captured.

Channel Width: (Appears only if you select a Channel number in the 5-GHz or 6-GHz band, above channel 14). Tap to select a width of 20, 40, 80, or (for 6-GHz band only) 160 MHz.

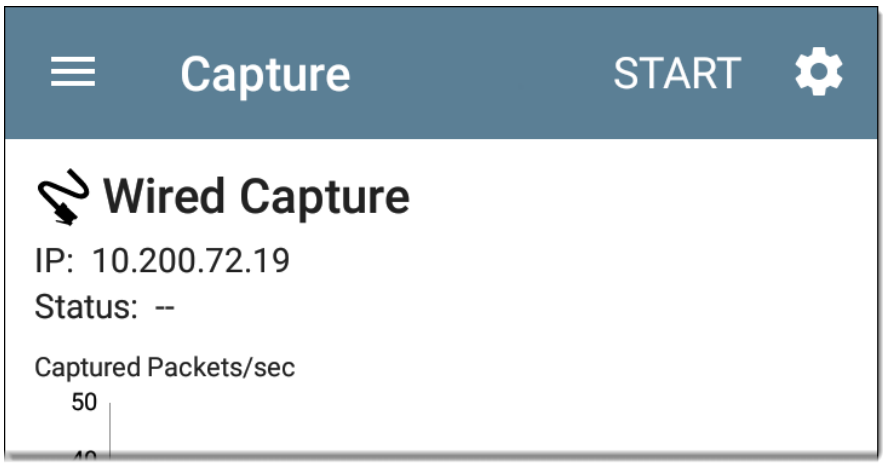
BSSID/MAC: Enter a BSSID to capture only packets going to or from the target device.

Control, Data, and Management Frames and Beacons: All frame types are captured by default. Tap the toggle button for each frame type to disable its capture.

Back to Title and Contents

Running and Viewing Captures

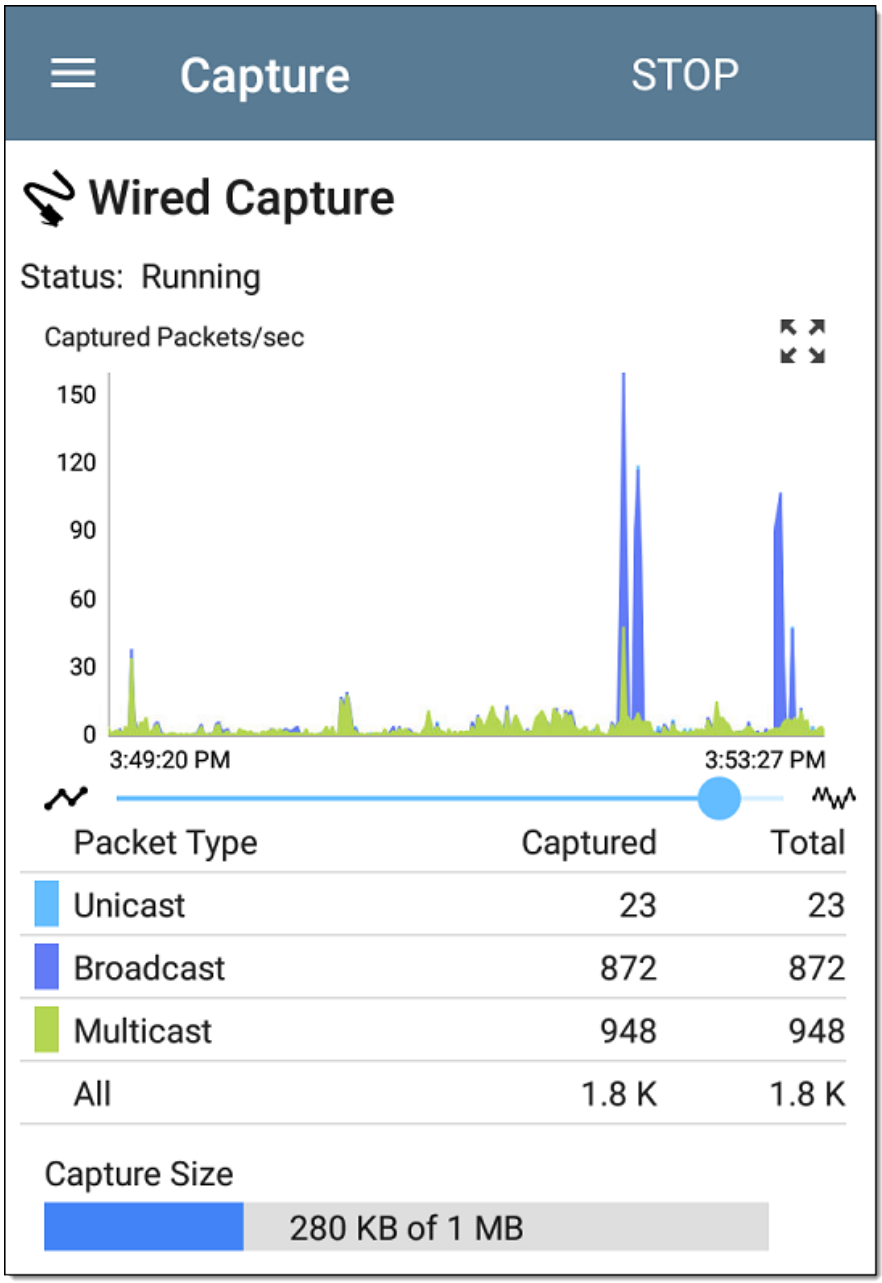
To start Capturing, tap **START** at the top of the app screen.



The current Status of the capture and any applied filters are shown under the capture type (Wired or Wi-Fi). The image above indicates that the app captures traffic for IP 10.200.72.19 only.

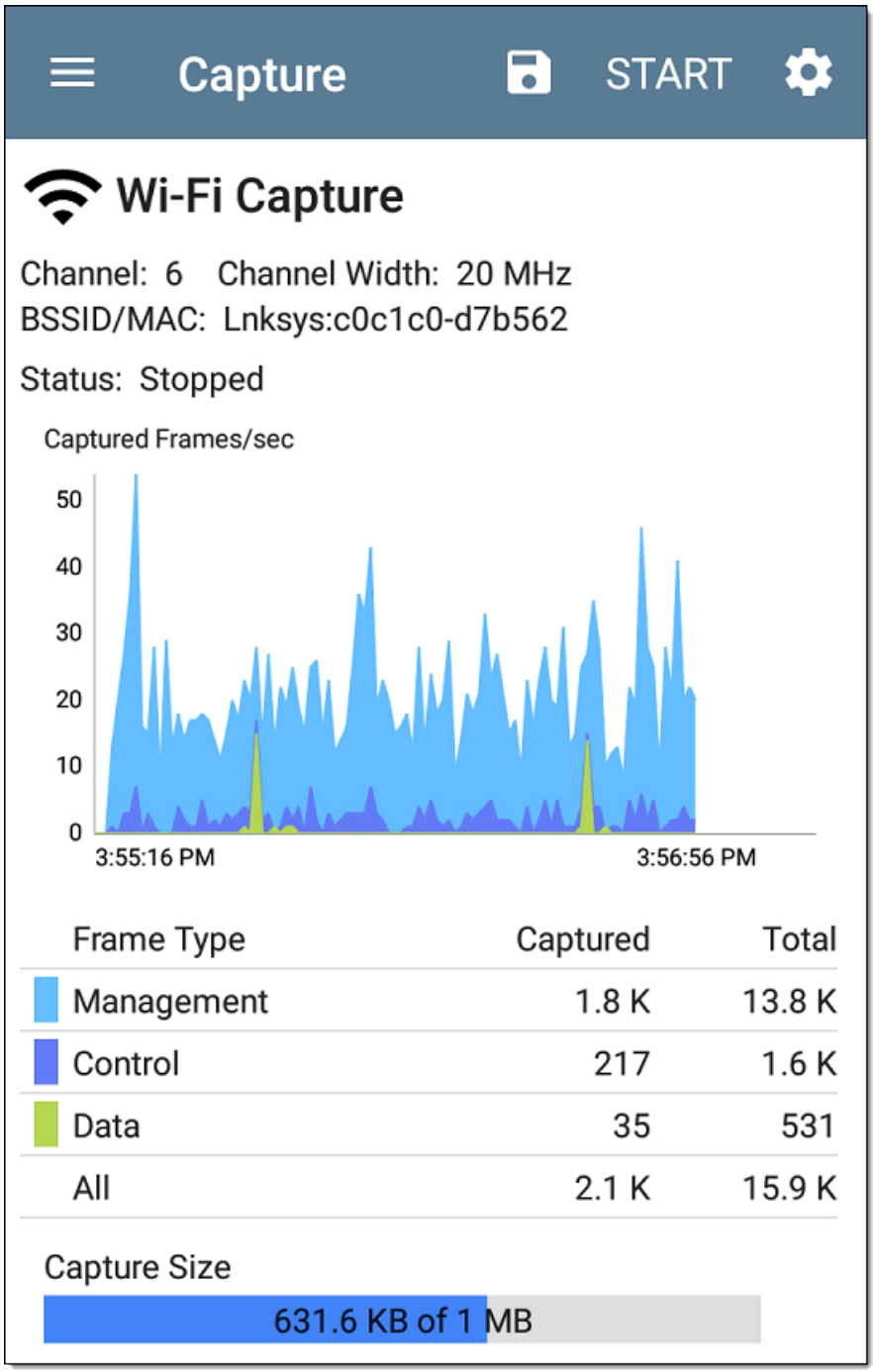
View the real-time status of the capture as it is running. If you navigate away from the Capture app, the capture process continues to run in the background until the File Size Limit (in Capture Settings) is reached. Captures also stop if you open the Wi-Fi app (which initiates scanning) or if you connect to a Wi-Fi network using AutoTest.

Tap **STOP** to stop the running capture before it reaches the File Size Limit.



The Wired graph plots the type and number of packets being captured while the capture is running and includes Unicast, Broadcast, and Multicast packet types.

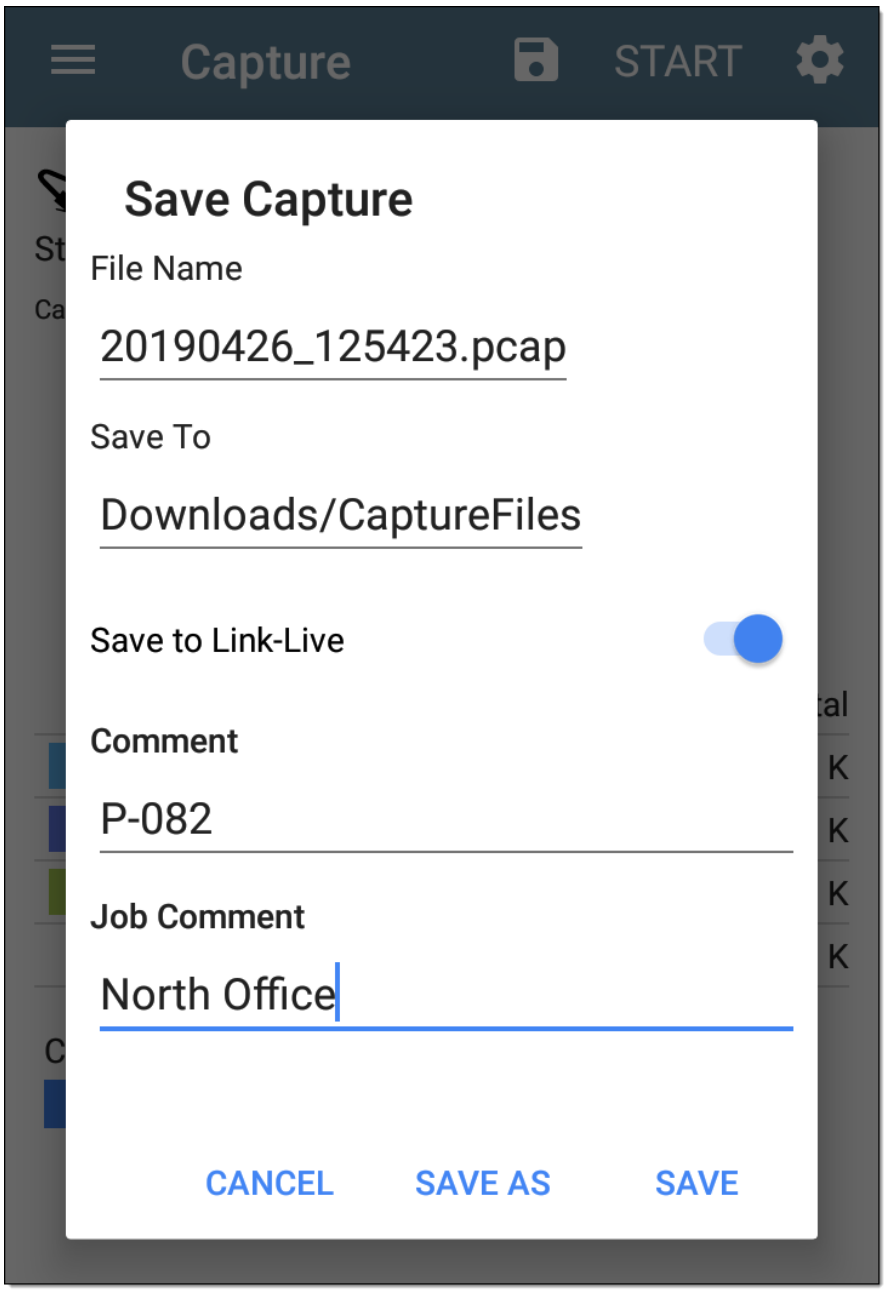
To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.
Wi-Fi captures graph the Management, Control, and Data Frame Types.



In the test shown above, the app has captured all three Wi-Fi Frame Types on channel 6 with the BSSID shown. The Total measurements in the table below the graph represent all frames seen, while the Captured frames are those that fall within the filter parameters.

Once a capture is completed, the **Save Capture** dialog appears automatically.

Tap the Save icon to reopen this dialog.



Captures are saved as .pcap files. Tap any of the fields in the dialog to enter changes.

File Name: Capture files are automatically named using the date and time. Tap this field to enter a custom name.

Save to: By default, capture files are saved in the **Downloads** folder in the EtherScope file system, but you can also save them to a Micro SD card or USB storage device or choose a different folder by tapping the **Save to** field. See also Managing Files.

Save to Link-Live: You can also upload capture files to Link-Live and then download them for analysis on a PC. Capture (.pcap) files appear on the Uploaded Files page in Link-Live.

Comment: This comment is attached to your capture file when it is uploaded to Link-Live.

Job Comment: This is the persistent Job Comment that uploads to Link-Live with all test results and files, until you change it. Changing the Job Comment here changes it throughout your unit.

Back to Title and Contents

Discovery App

The EtherScope nXG Discovery application creates an inventory of the devices on your networks along with their attributes: device types, names, addresses, interfaces, VLANs, resources, and other connected or associated devices. The app allows you to identify and analyze network devices and acts as a jumping-off point for further analysis using other apps, such as Wi-Fi, Path Analysis and connection tests.

Devices are discovered in the local broadcast domains where the EtherScope is physically connected, as well as other configured subnets. By default, discovery processes run out of all available **test and management ports, wired and wireless**.

Discovery Chapter Contents

This chapter describes how the Discovery process and app screens work, shows examples of Discovery data, and details the Discovery settings.

Introduction to Discovery

Discovery finds, classifies, and displays — through Ethernet, fiber, and Wi-Fi— the details of network components. Information provided by Discovery can include the following:

- IP, BSSID, and MAC addresses
- Device Names
- Device Connectivity
- SNMP Data
- Network Problems
- Interface Details and Statistics

Devices are discovered via ARP and Ping sweeps; SNMP, DNS, mDNS, and netBIOS queries; and passive traffic monitoring. Discovery classifies each device as it is found. Up to 2,000 devices can be reported.

The Discovery app also detects Problems with discovered devices, including **Warning** and **Failure** conditions.

The EtherScope's discovery process begins when the unit is powered on. A channel scanning

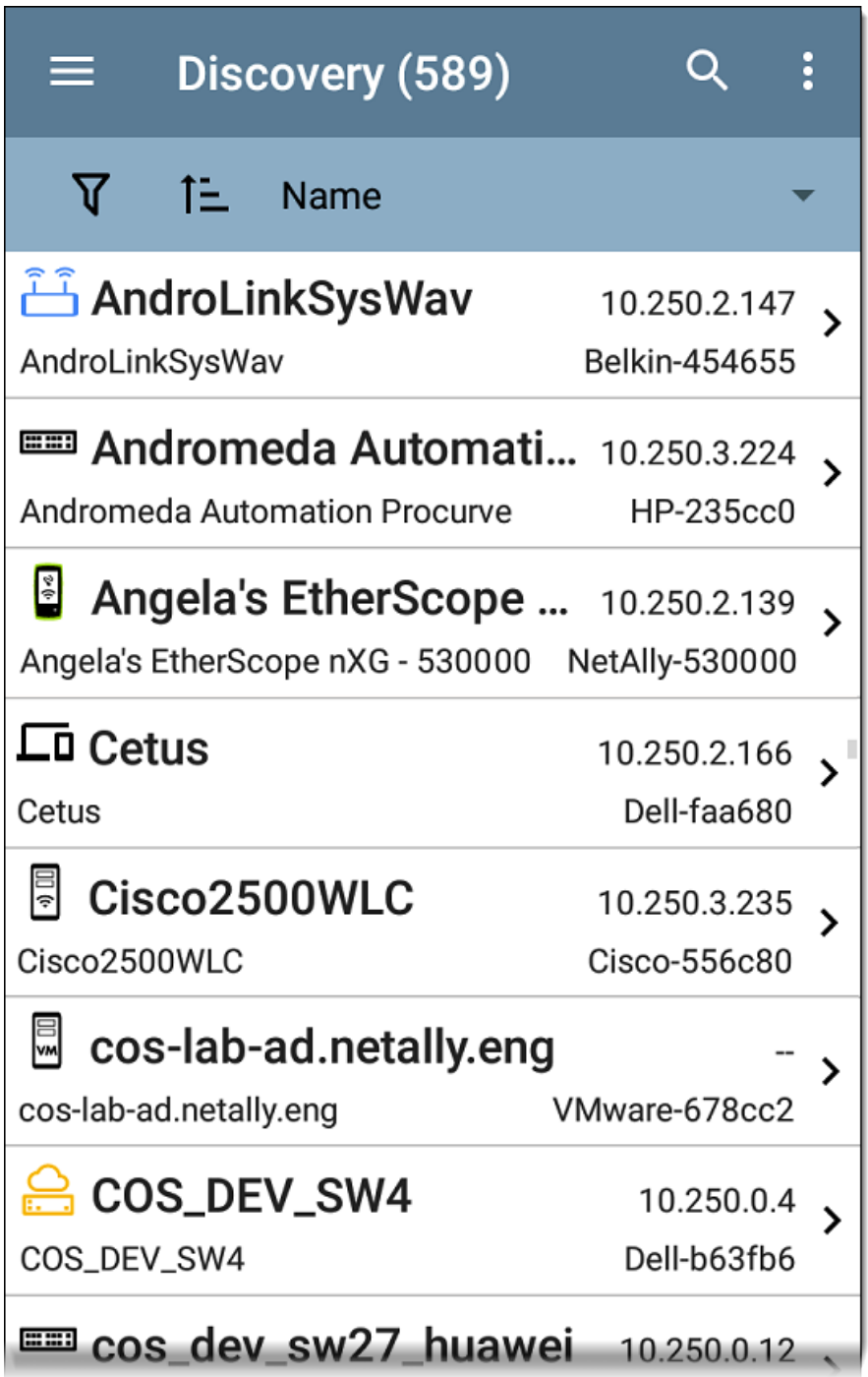
notification  in the top Status Bar indicates that the EtherScope is scanning Wi-Fi channels to passively discover devices on the wireless network. Once a network connection (wired or Wi-Fi, test or management) is established, the active discovery process begins.

Discovery notification icons  indicate the progress of active discovery. This icon  indicates that no links are currently available for active discovery, either because none of the ports enabled for discovery are connected or because AutoTest is running.

The Discovery app consistently monitors network traffic, but the active discovery process reruns every 90 minutes by default. You can select a different Refresh Interval in the Discovery Settings.

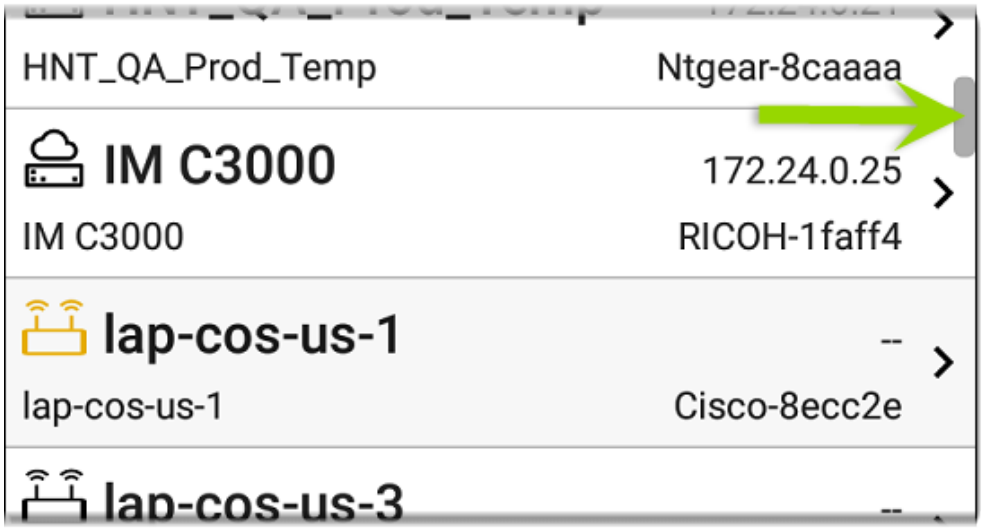
Main Discovery List Screen

The main Discovery screen lists all the devices the EtherScope has discovered.



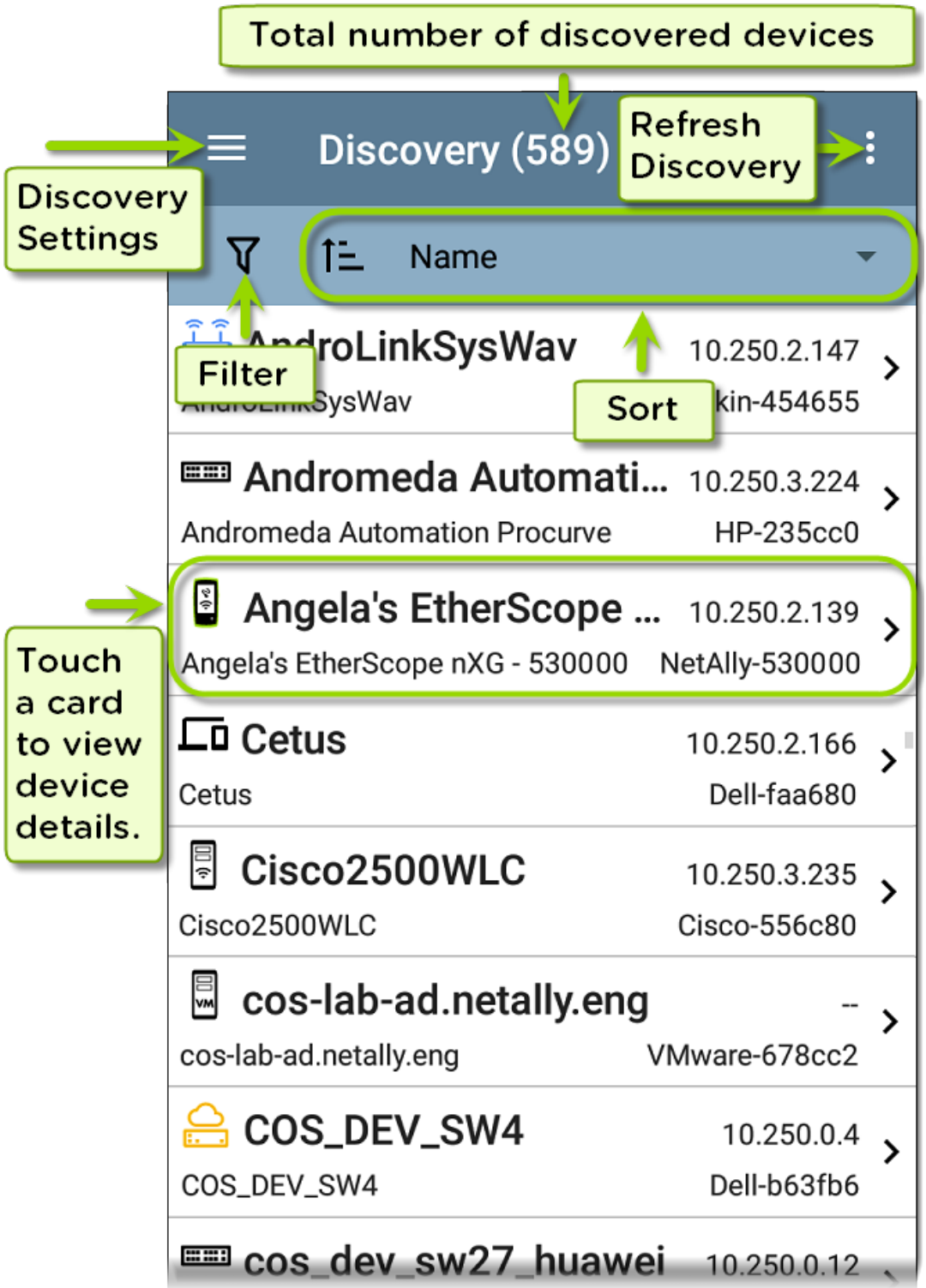
Like in AutoTest and other EtherScope screens, the icons in Discovery change color to indicate a **Warning** or **Failure** condition. Discovery also displays device icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous Problem has been resolved. (See the Problem Settings to adjust enabled Problems and thresholds.)

The Discovery screen, and other app screens with long lists, support fast scrolling. Touch and drag the scrollbar handle to the right of the list to scroll quickly up and down.



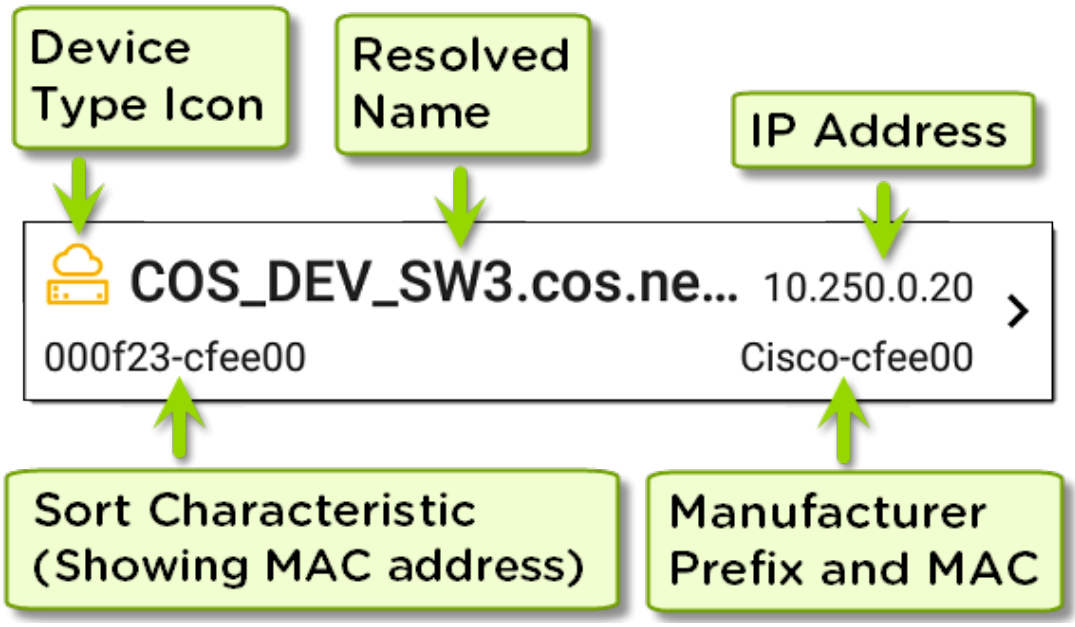
From the main Discovery screen, you can filter and sort the listed devices, open the left side

navigation drawer to configure settings, and tap a device's card to view its details.



Discovery List Cards

The information displayed on each device card varies depending on the selected Sort element and the data the EtherScope was able to discover.

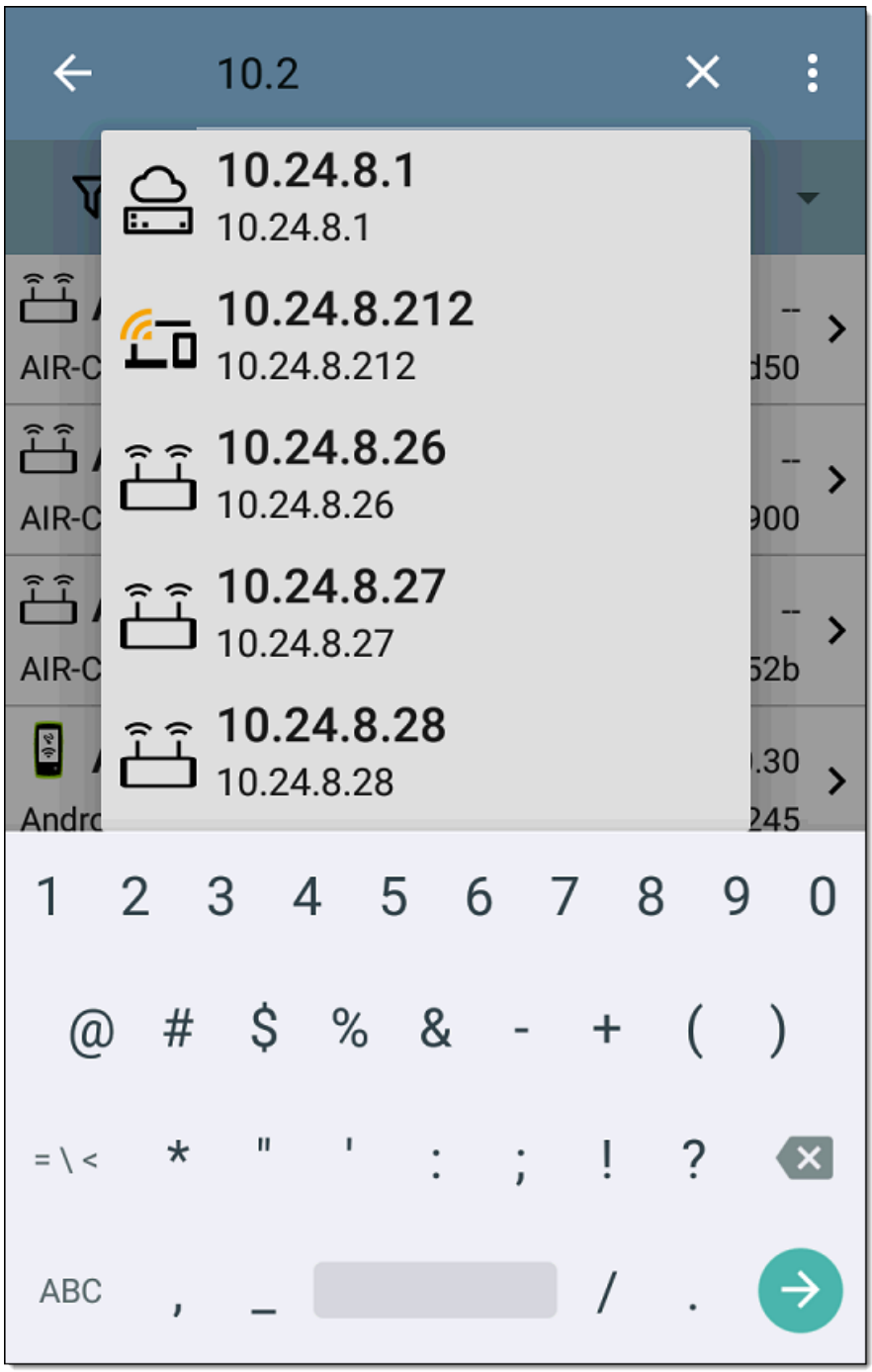


The lower left field displays the characteristic by which the Discovery list is currently sorted. In the image above, the list is sorted by MAC address. See Discovery Sorts in this topic for more about sorting.

Searching the Discovery List

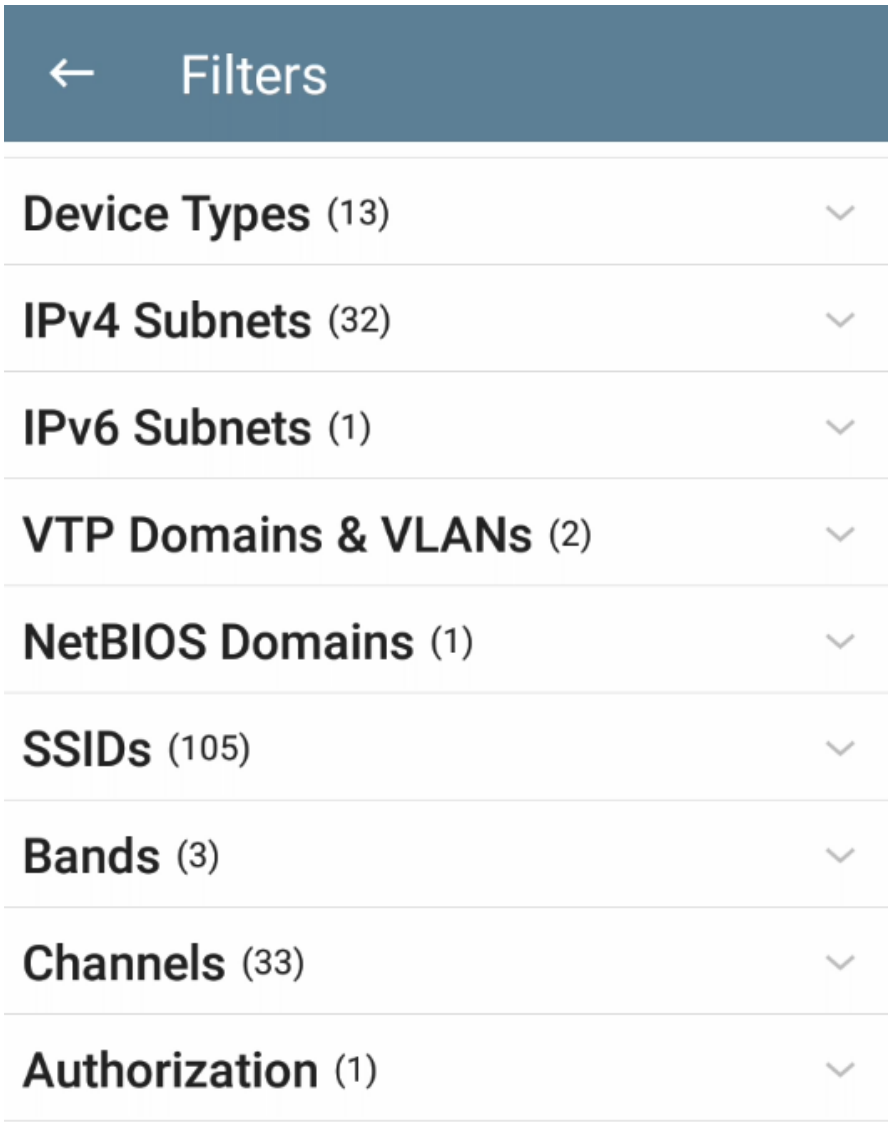
The main Discovery screen offers a search feature. Tap the search icon at the top of the

screen to search discovered devices.



Filtering the Discovery List

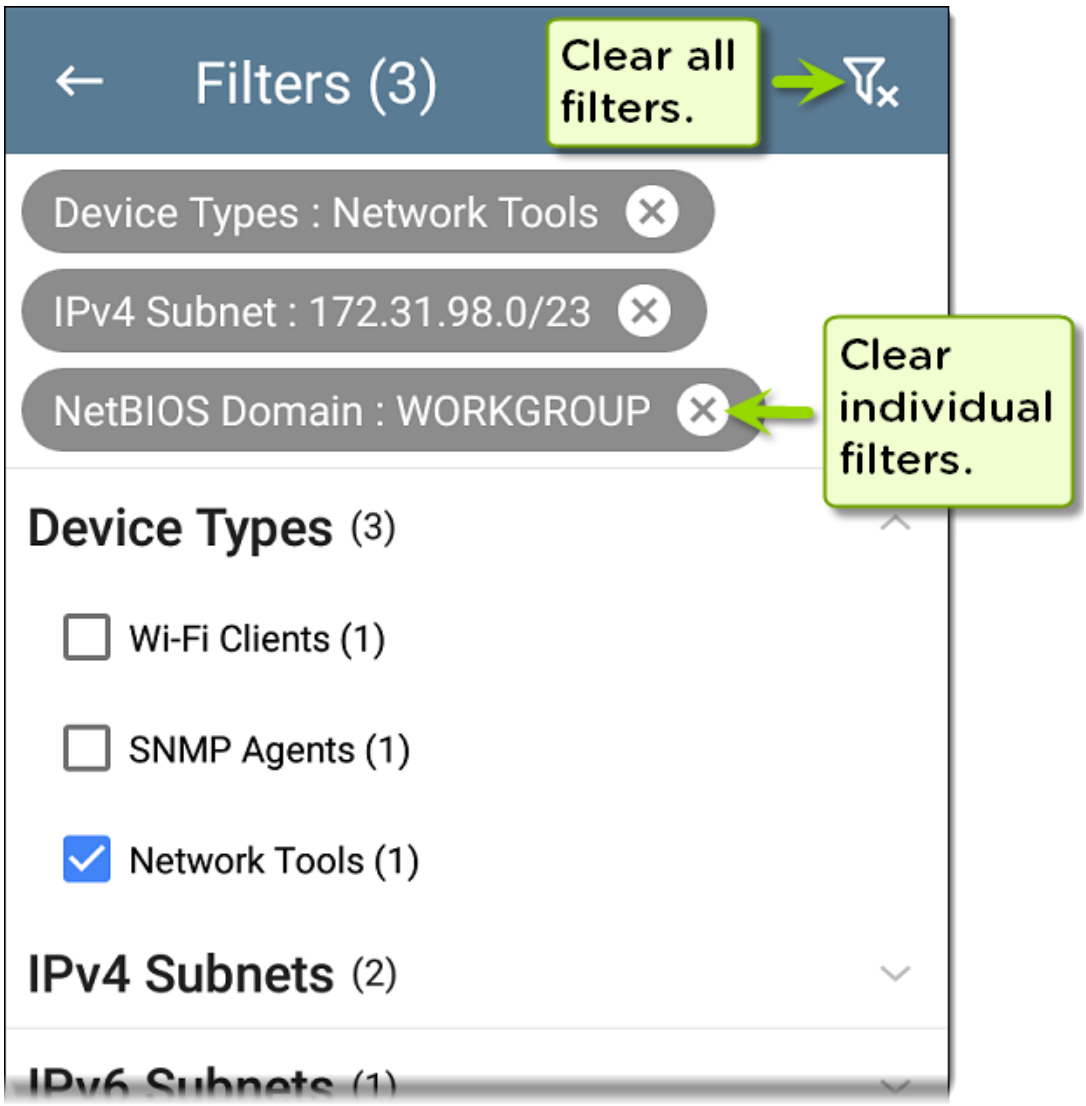
Tap the filter button near the top left of the main Discovery screen to set filters that control which devices are displayed in the list.



The Filters screen displays the number of devices or domains discovered for each category. Tap a category name to select filters

by checking the boxes. The main Discovery screen shows only those devices or IDs that fall under your chosen filter parameters.

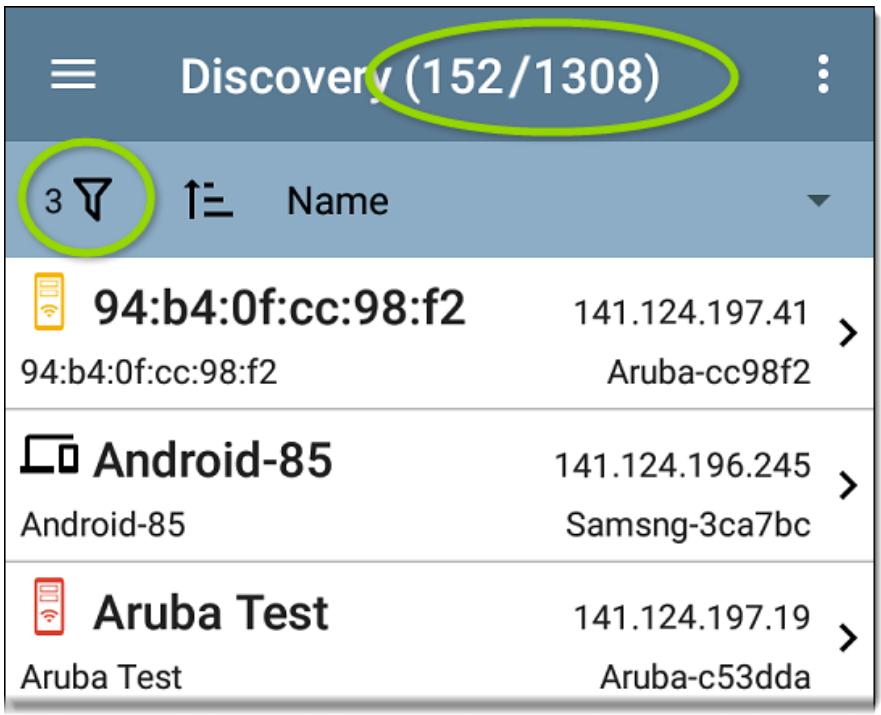
When filters are selected, those active filters are displayed at the top of the Filters screen.



- Tap the ✕ button to the right of each filter to clear it.

- Tap the clear filter icon at the top right to clear all filters.

After you select a filter, the Filters screen displays results filtered for that characteristic. For example, in the image above, the user has selected the **Network Tools** device type. As a result, only those subnets, addresses, Wi-Fi bands, etc., with a discovered Network Tool remain selectable in the filters list.

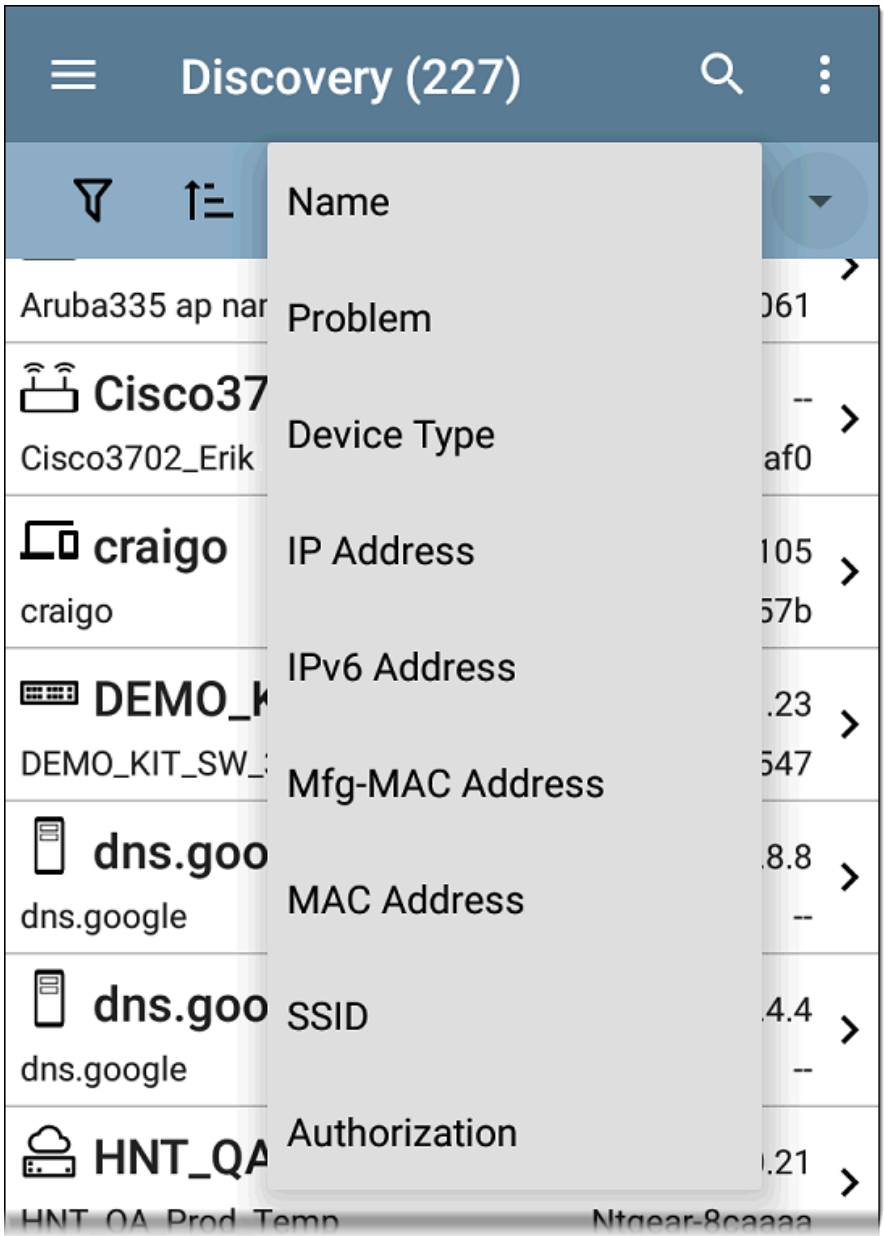


Back on the main Discovery screen, the screen title shows the number of filtered devices out of the total discovered devices (in the image above, 152 filtered devices out of 1308 total).

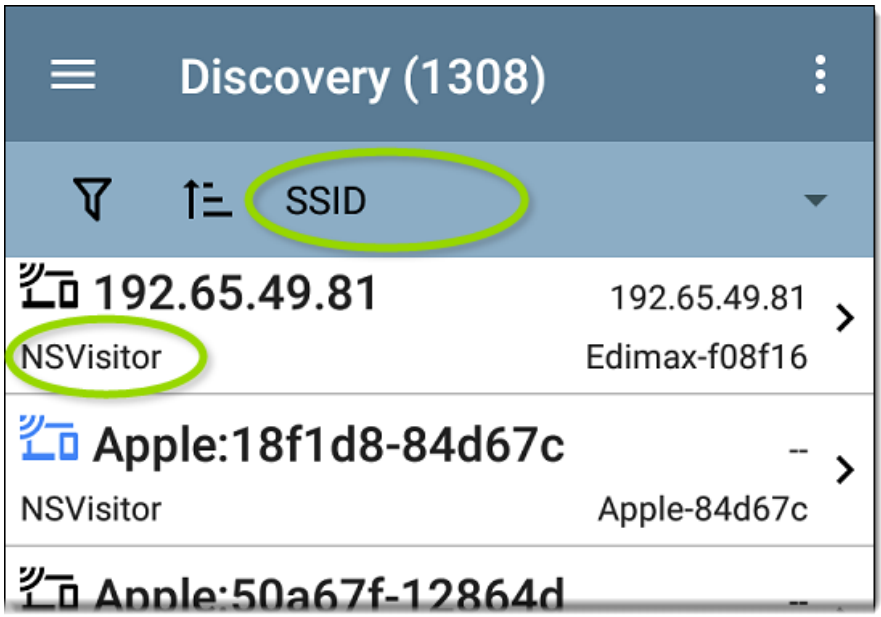
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

Sorting the Discovery List

Tap the Sort bar or down arrow to open the Sort drop-down menu.



Select a Sort option to order the devices based on your selected characteristic.



The selected Sort option displays in the Sort bar above the device list, and the sort characteristic for each device is shown under the device type icon. In the image above, all the devices associated with the "NSVisitor" SSID are sorted together. Individual devices on the same SSID are sorted numerically and alphabetically.

Tap the sort order icon to switch the sort order between normal and reverse order.

Devices are sorted in groups. Those with resolved names appear at the top (in normal order), and then devices with only IPv4, IPv6, and MAC addresses appear below, respectively.

Reversing the normal sort order reverses the devices within the groups but does not change the order of the groups.

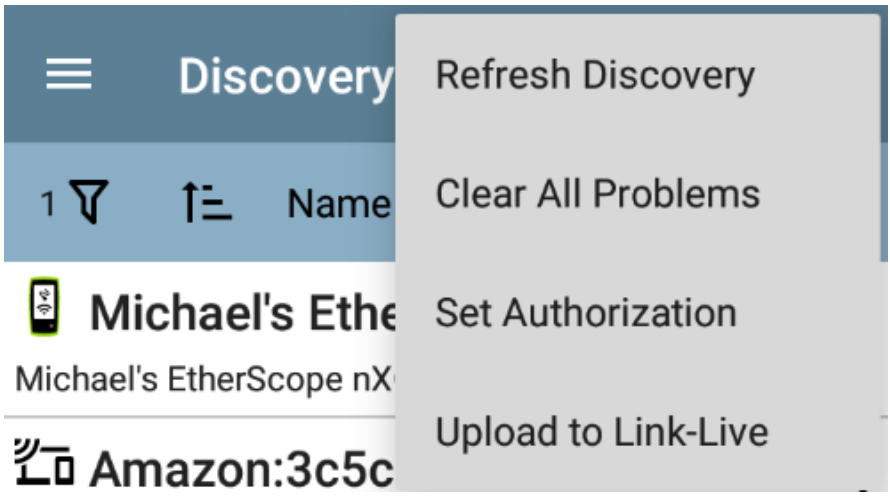
Security Auditing – Batch Authorization

Batch Authorization lets you extend filtering to organize devices into the following security categories:

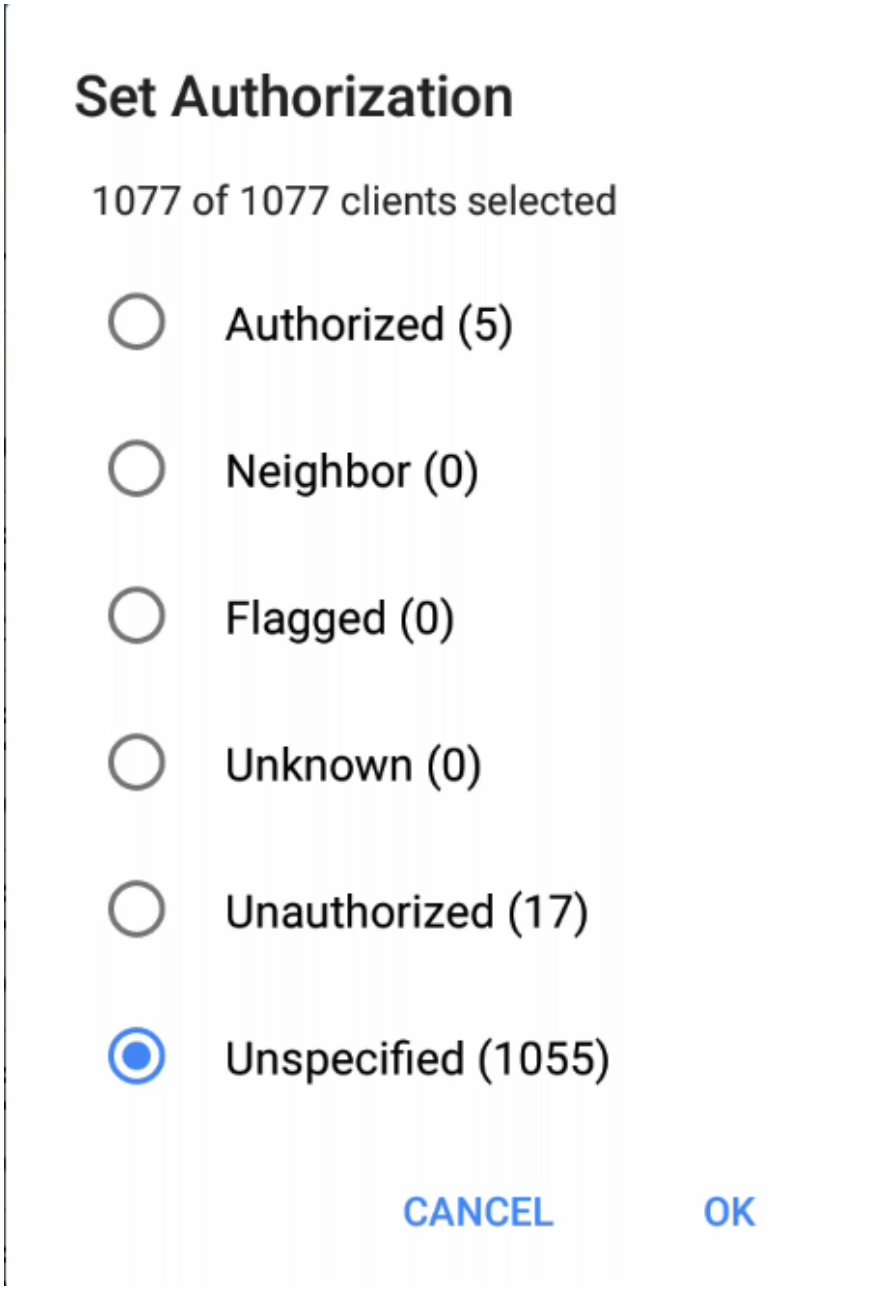
- **Authorized**: For devices approved for use on your network
- **Neighbor**: For devices owned and controlled by neighboring organizations
- **Flagged**: To give visibility to a specific device
- **Unknown**: For devices that have not been identified or classified
- **Unauthorized**: For devices that should not be on the network and may present a security risk
- **Unspecified**: Default unassigned Authorization status

Once categorized, it is simple to immediately identify any new devices on the network by filtering according to Authorization type. New devices are identified as Unspecified.

To use the Batch Authorization feature, create a filter that identifies the devices you want to categorize. For example, you could filter on SSIDs used by other offices in your building. After you filter the list of discovered devices, select the overflow menu.

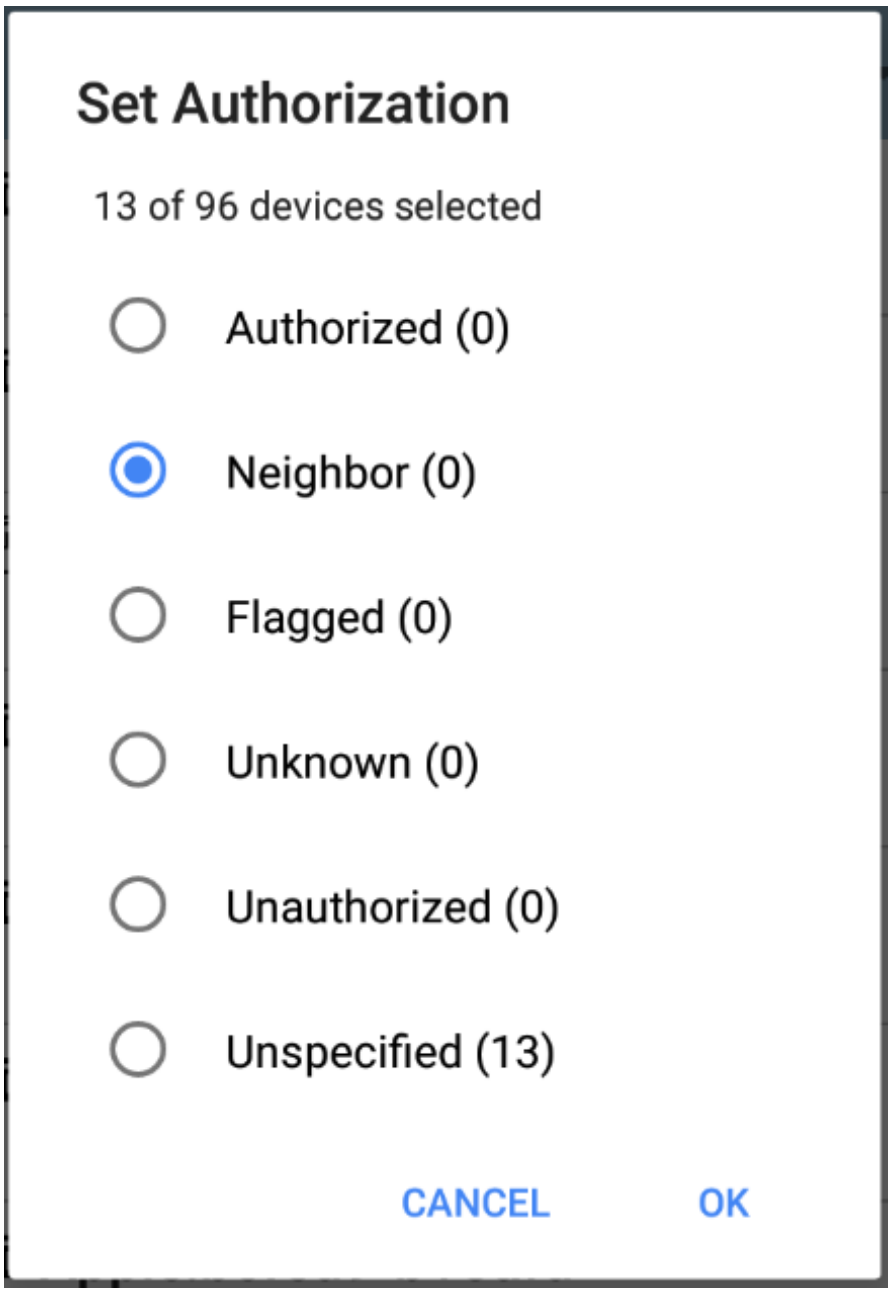


Select **Set Authorization** to see how these devices are currently categorized and the number of devices in each category.



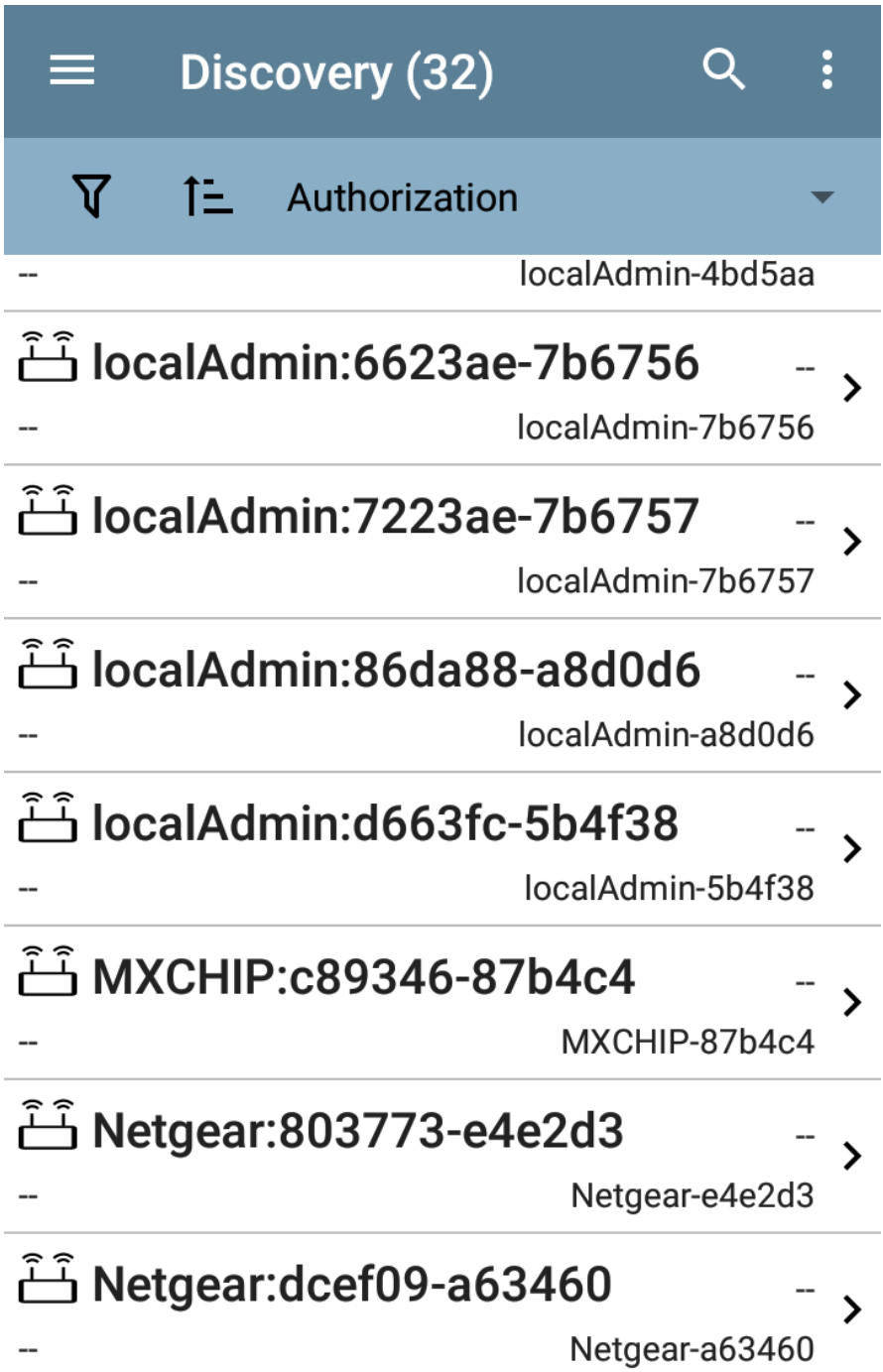
NOTE: The initial selection on this screen defaults to the category with the highest count. If other categories have non-zero counts, selecting **OK** changes the authorization setting for all devices to the selected category.

Select the appropriate security category. As in the example, if these devices belong to other offices, select **Neighbor**, and then tap the **OK** button.



You can now sort the list of discovered devices and clearly identify the security category of the

devices. Devices from other offices are identified as: Neighbor



See Assigning a Name and Authorization to a Device for more information on the Authorization feature.

> NOTE: Batch Authorization operates on the default MAC address of a device. If a device has multiple MACs, authorization is set only on the default MAC address. Devices that do not have a discovered MAC address, such as unknown switches and off-net devices, cannot have an authorization setting.

Refreshing Discovery

Tap the action overflow icon ⋮ at the top right of the main Discovery screen, and select **Refresh Discovery** to refresh the active Discovery process.

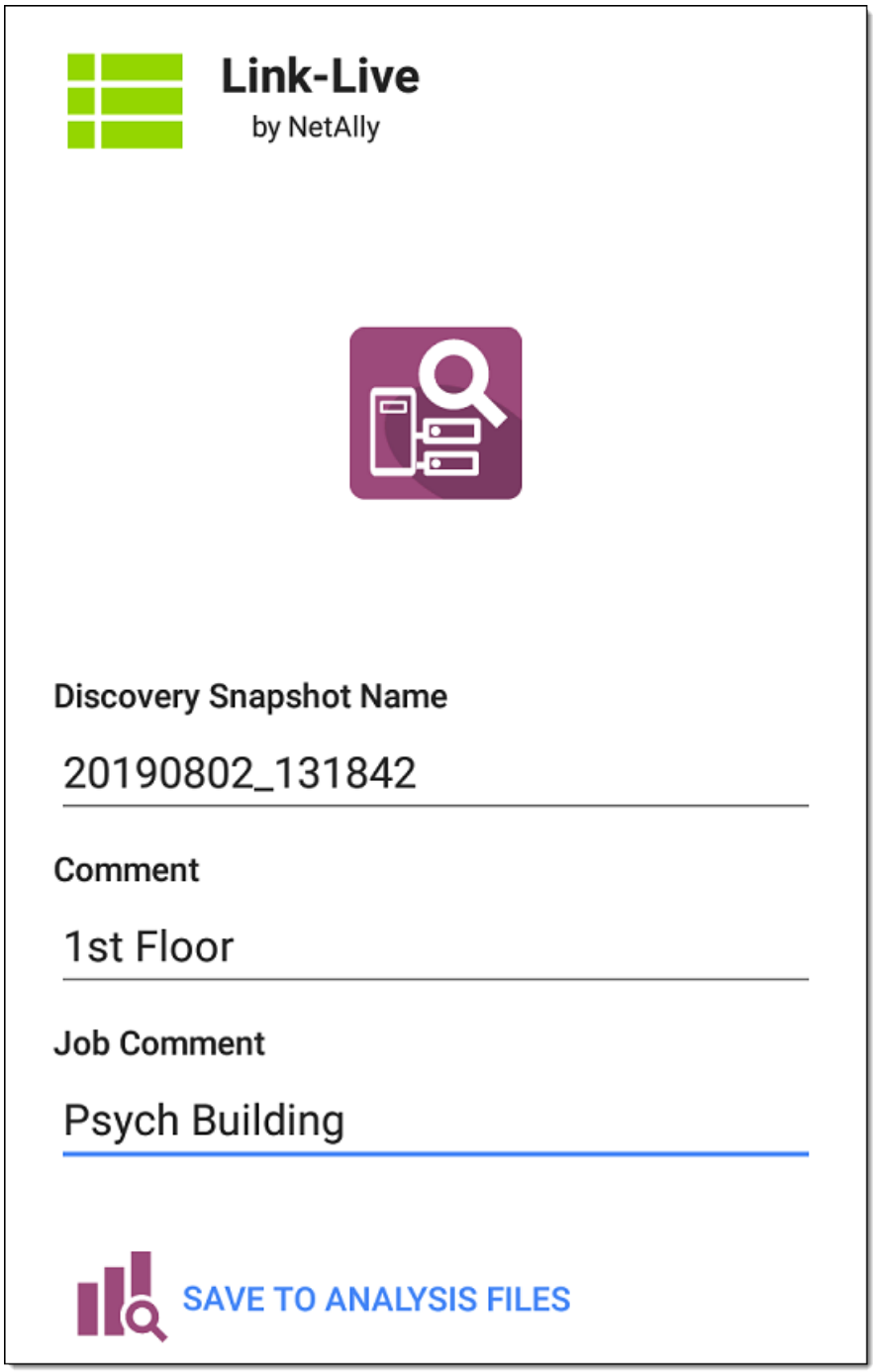
REFRESH DISCOVERY restarts the active discovery process without clearing the already discovered devices.

CLEAR AND RERUN DISCOVERY clears the accumulated results and restarts the discovery process.

Uploading Results to Link-Live

Tap the action overflow icon  at the top right of the main Discovery screen, and select **Upload to Link-Live** to send the current Discovery results to the Analysis page  on Link-Live.com.

> NOTE: Wi-Fi app results automatically upload with the Discovery results.



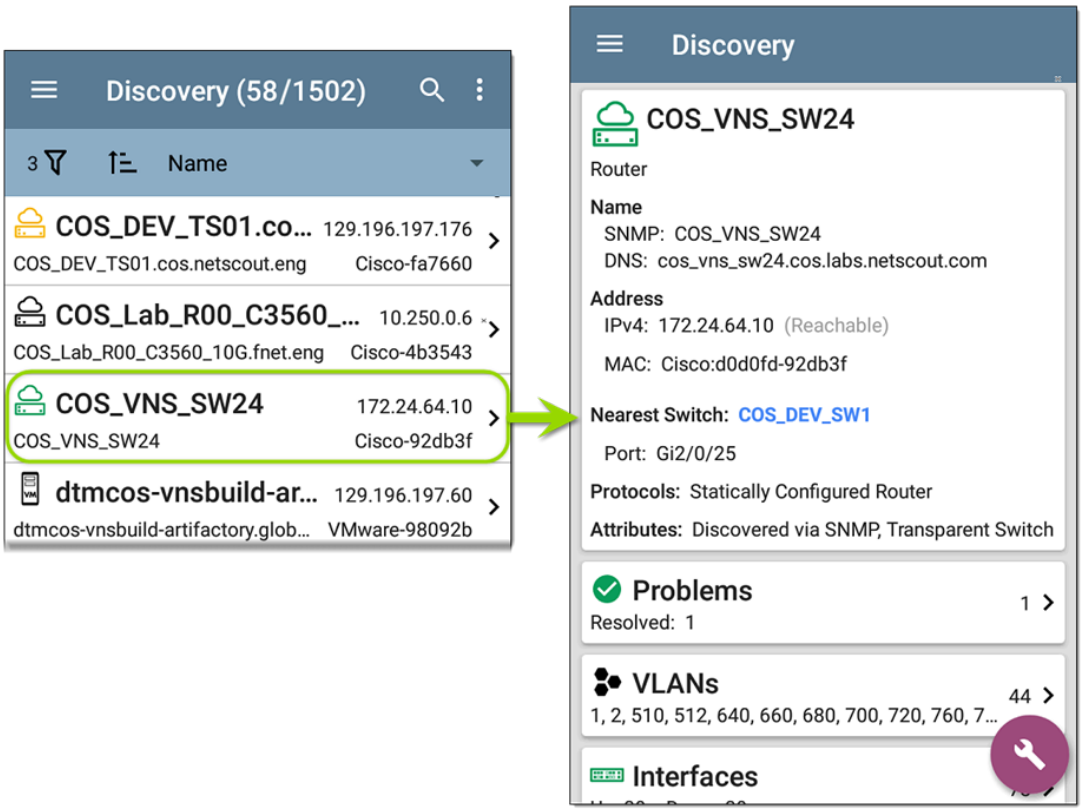
See the Link-Live chapter for more information.

Back to Title and Contents

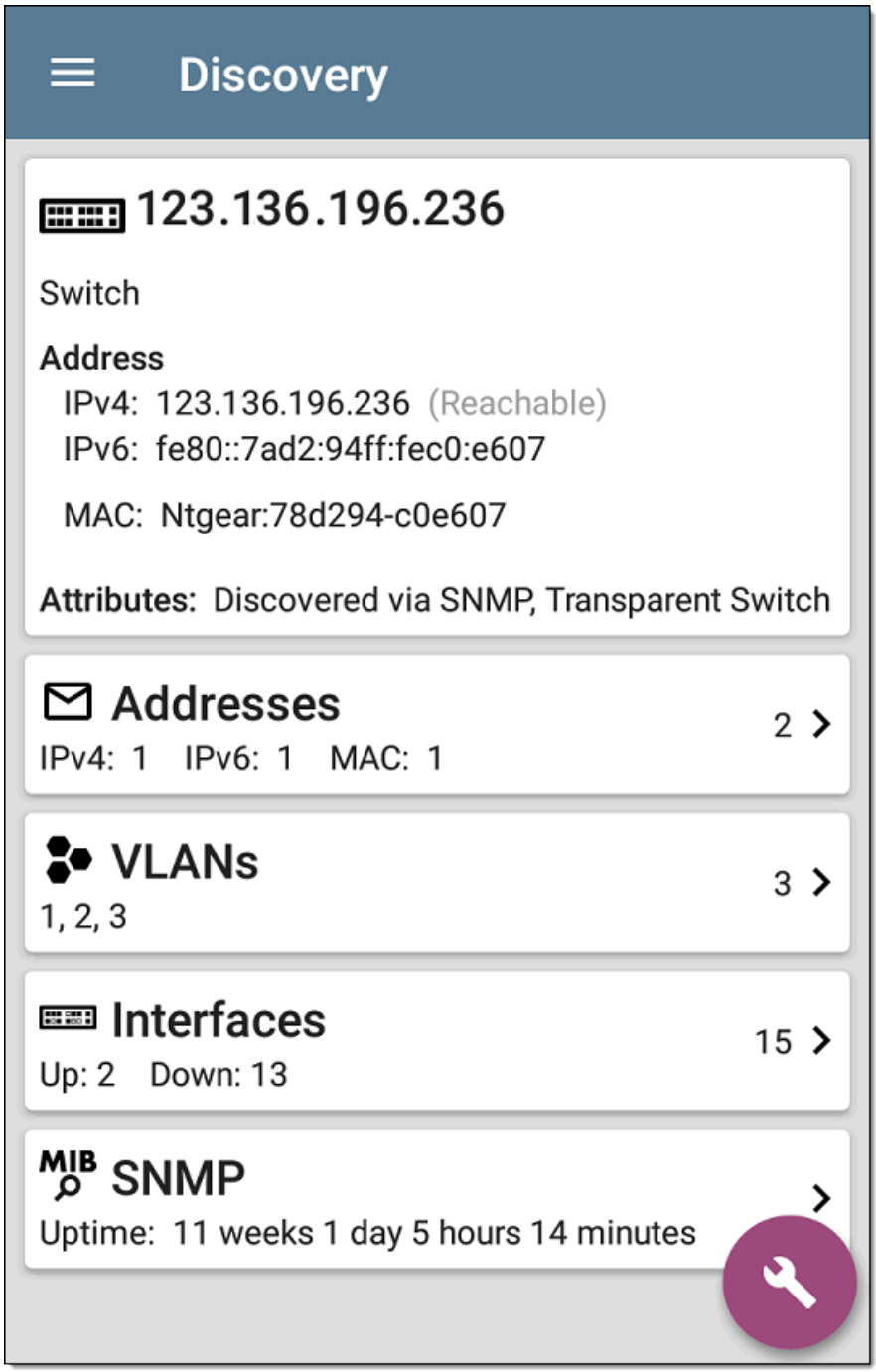
Discovery Details Screens

Tap any of the device cards on the main Discovery list screen to view Device Details.

The example below calls out a Router card and its Details screen.



The available data and actions on the Details screens vary significantly depending on the device type, connections, and data the EtherScope was able to discover. In other words, only the discoverable information for each device is shown on the Details screen.



For the Switch screen shown above, Discovery was able to find an IP address but not a name for the switch.

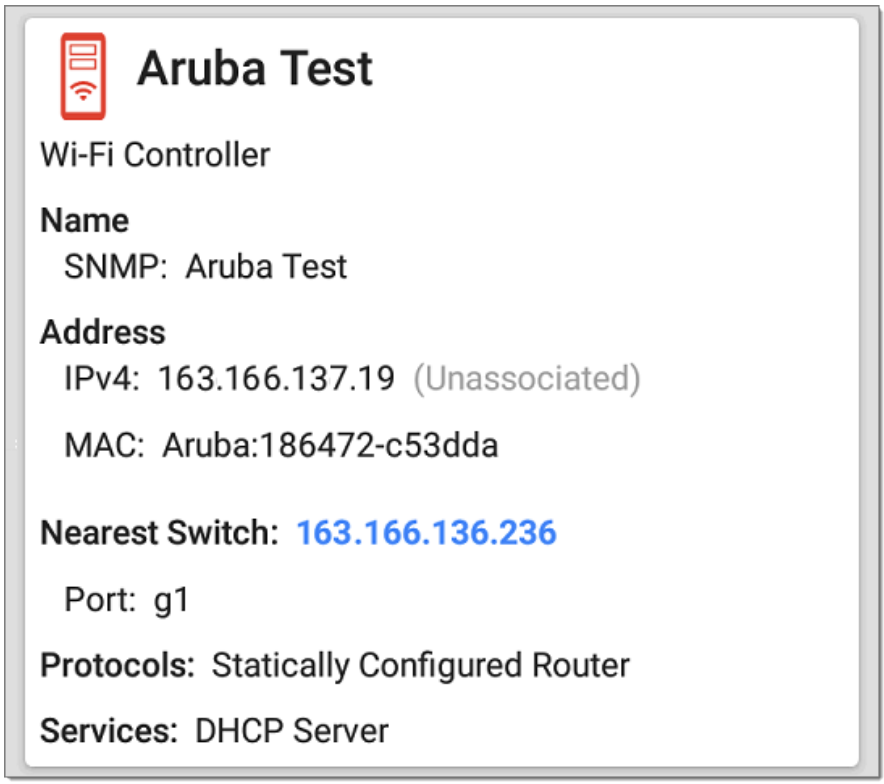
Each Details screen shows additional information about the selected device, any Problems detected by the EtherScope, and counts for other connected or corresponding network elements.

Each Details screen also has a FAB button that lets you take additional actions or run other applications on the device. The available actions and applications depend on the device type and connection available. See Discovery App Floating Action Menu for more information.

See Device Types for specifics about the different devices the EtherScope can discover.

Top Details Card

The top card on the Details screen summarizes the discovered data for the selected device.



The top of the card shows the device type(s) and icon (a Wi-Fi Controller with a **Failure or Error** status in the example image above).

The rest of the fields that appear on the top Details screen card depend on the device type and what the EtherScope can discover about the device.

On the Discovery Details screens, you can tap any **blue linked name or address** to open a Discovery or Wi-Fi Analysis screen for the linked device.

NOTE: Non-underlined links open in the same app (in this case Discovery), and **underlined links** open in a different app (in this case Wi-Fi) .

The linked and underlined Cisco MAC address in the screen image above opens the Wi-Fi app's AP Details screen, where you can view the other

wireless attributes associated with the Lightweight AP. The Nearest Switch and Wi-Fi Controller links open a Discovery app Details screen for those devices.

Data Fields on the Top Details Card

The following fields may appear on the top card on a Device Details screen, depending on the device type and the information EtherScope was able to discover:

Name: Discovered hostname(s) of the device. This section can display user-defined, DNS, mDNS, SNMP, NetBIOS, AP, and Virtual Machine names as discovered.

Address: Discovered IPv4, IPv6, BSSID, and/or MAC addresses of the device. This section displays the default (first discovered) addresses of each type. For more addresses, select the Addresses card when available.

Authorization: This field shows the user-assigned Authorization status of the device. See Assigning a Name and Authorization to a Device.

802.11: Wireless data

Channels: Wi-Fi channels on which the device is operating

Type(s): 802.11 media type(s) supported by the device

Nearest Switch: Name or address of the switch identified as closest to the device

- **Port**: Physical port where the device is connected
- **VLAN ID**: ID of the VLAN the device is on

Protocols: Routing protocols, discovered via packet analysis, operating on the device or network

Services: Network services provided by this device, such as DHCP or DNS

Attributes: Other discovered attributes about the device

Wi-Fi Controller: Name and address of the Wi-Fi Controller for a Lightweight AP

AP: Access Point to which the device is connected

- **SSID**: Name of the network on which the device is operating
- **Security**: AP's security type

Hypervisor: Name of the hypervisor on which a virtual machine is operating

Virtual Machine: Name of the virtual machine

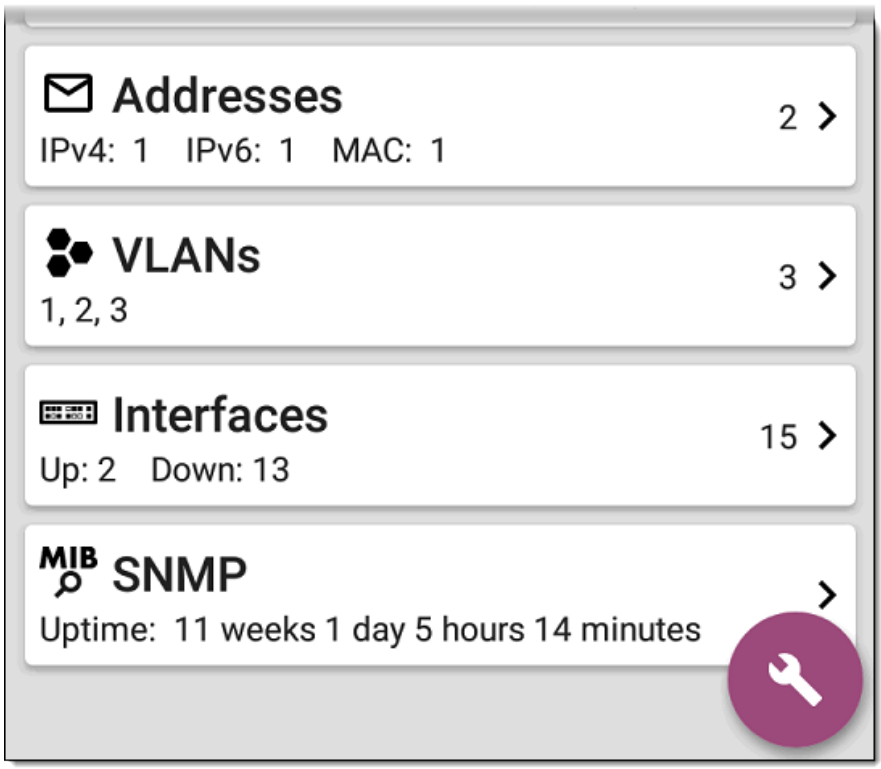
- **Guest OS**: Operating system running on the virtual machine
- **Memory Reservation**: Amount of memory reserved for the virtual machine

Last Seen: Time at which EtherScope most recently detected the device

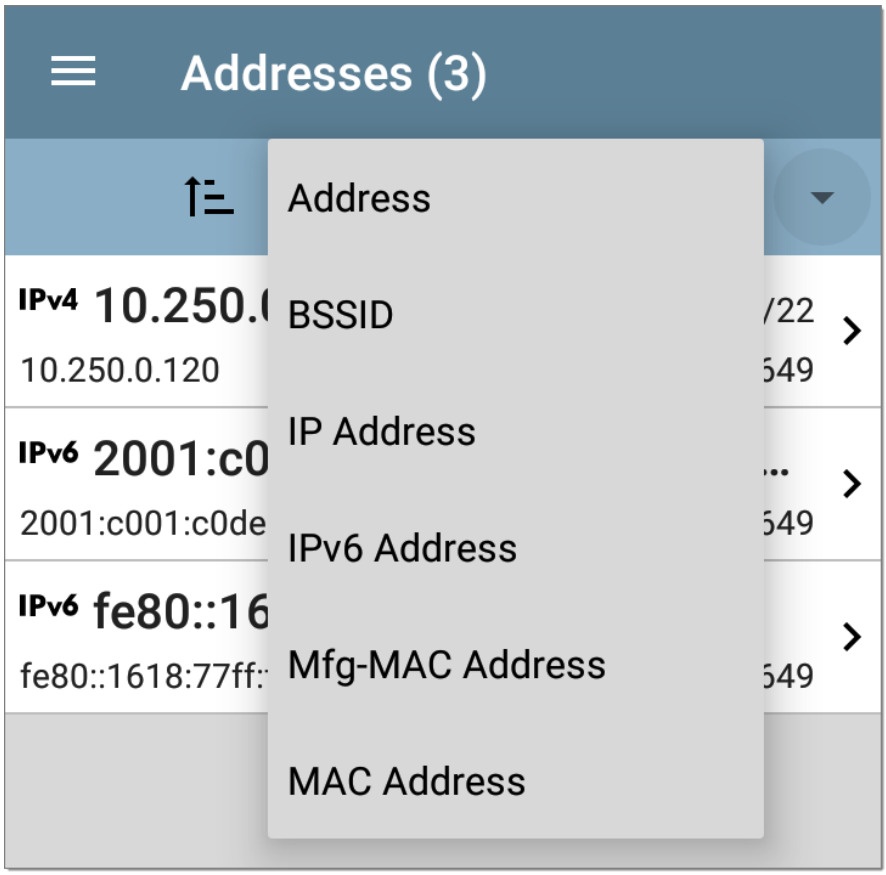
Back to Title and Contents

Lower Cards in Device Details

Tap any of the lower cards on a Device Details screen to view more discovered characteristics and "drill down" to specific Problems, Addresses, Interfaces, etc. for the selected device.



Screens with a list, such as Addresses shown below, also offer Sort options.



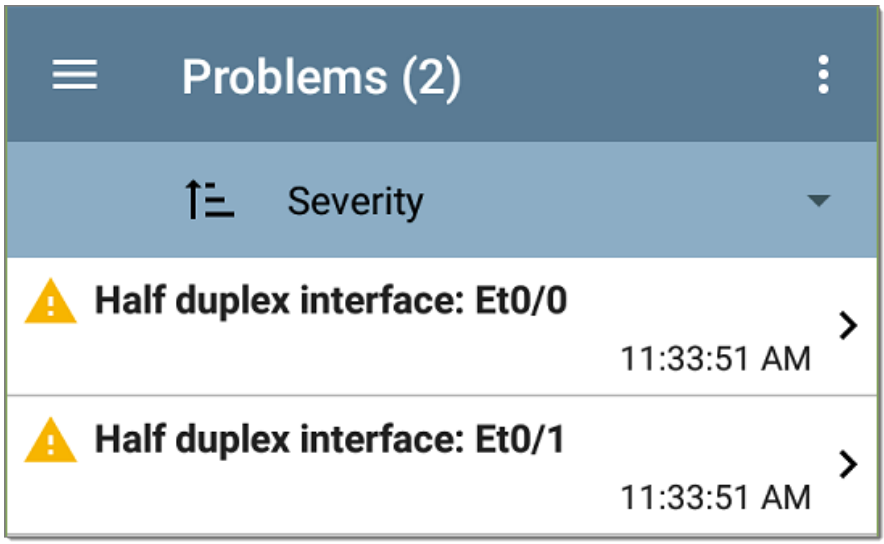
The rest of this topic provides examples of each type of Details screen and options for additional analysis.

Remember, you can tap any card with a right pointing arrow › to open a new screen with more information about the device or characteristic.

Problems

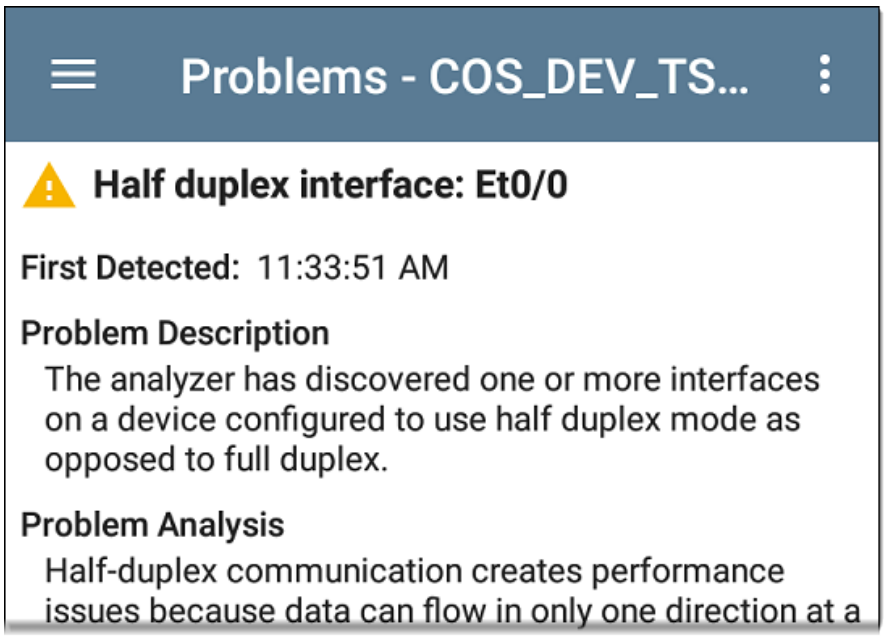
The Problems card shows the icon color of the highest severity problem, and the number of detected **Warning**, **Failure or Error**, **Information**, and **Resolved** conditions for the device or network component.

Tap the Problems card to view the Problems list screen (unless only 1 Problem is detected, in which case, the detailed Problem description opens, skipping the list screen).



Tap the sort field to sort the list by **Severity** or by the time when the problem was **First Detected**.

On the Problems list screen, tap a Problem's row to read a detailed description.

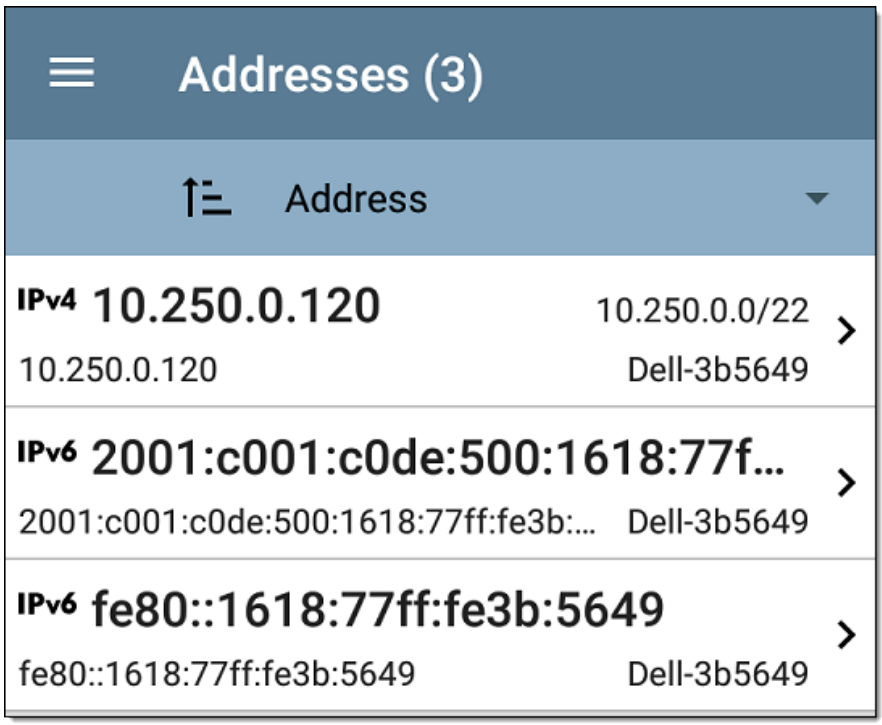


To clear a problem, tap the action overflow button ⋮ at the top right of the Problem list or description screen, and then tap **Clear Problem**.

See Problem Settings to select which problems are detected and displayed by your unit.

Addresses

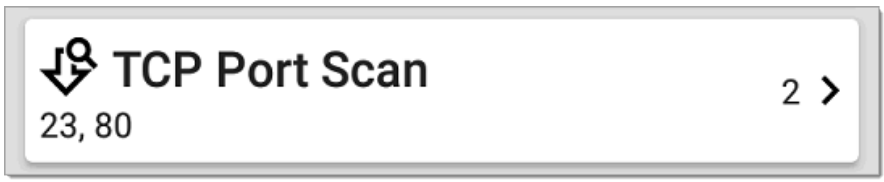
The Addresses card displays the number of each type of address discovered: IPv4, IPv6, MAC, and/or BSSID. Tap to view the addresses and related information.



From the Addresses list screen, you can sort the list order and tap any of the discovered addresses to investigate the address further.

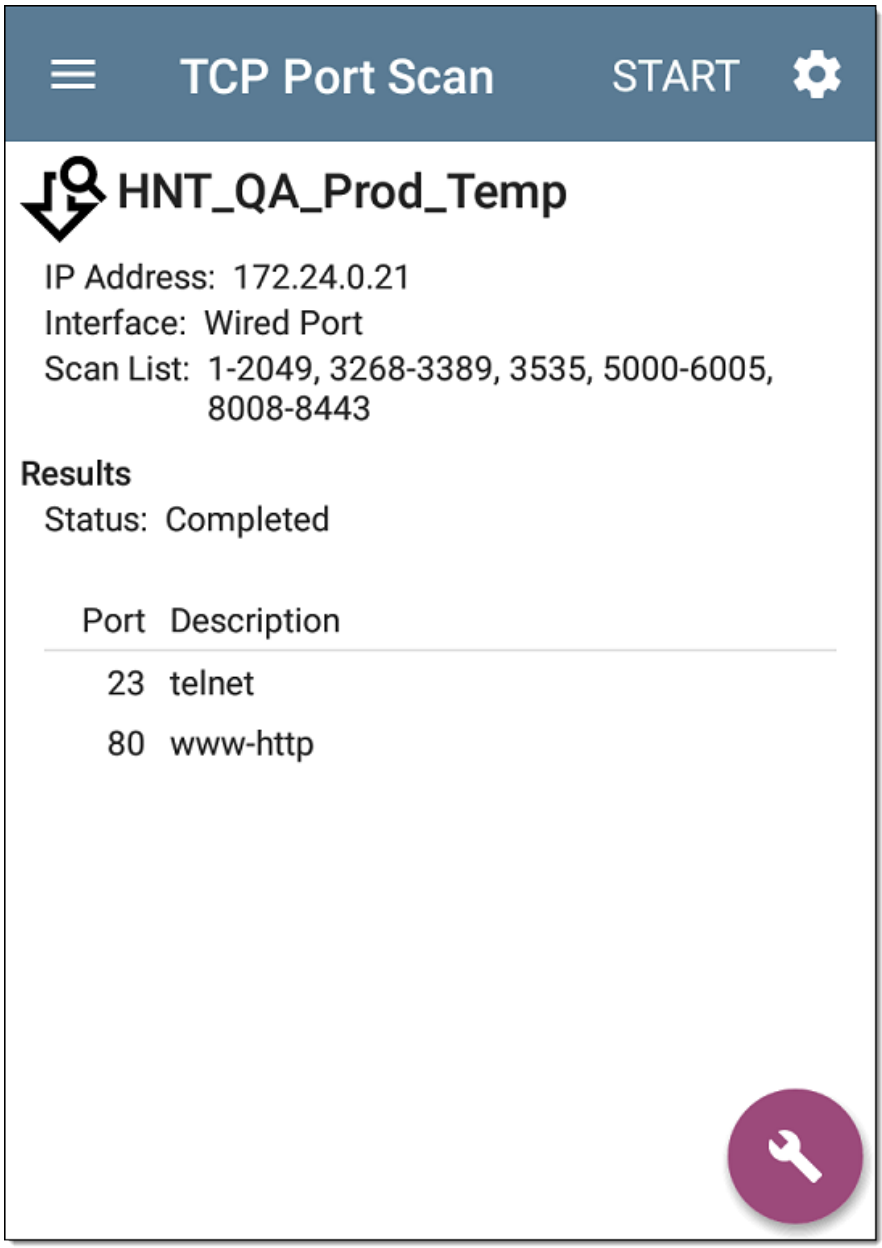
TCP Port Scan

If you have run a TCP Port Scan (from the Discovery FAB) on a device or IP address, a TCP Port Scan card appears on the device's Details screen.



This card lists open port numbers and shows the total quantity of open ports. Tap the card to open the TCP Port Scan screen.

You can also open this screen from the Discovery floating action menu.



The top of the TCP Port Scan results screen shows the name or IP address of the tested device and the following fields:

IP address: IP address of the device that was scanned

Interface: Test or management port from which the test ran, set in the TCP Port Scan settings

Scan List: List of port numbers tested

Results

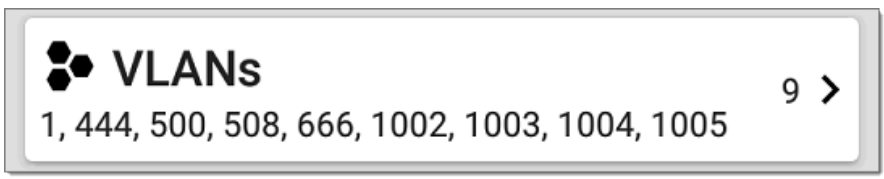
Status: Current status of the port scan

Port/Description: List of all the detected open ports with their descriptions

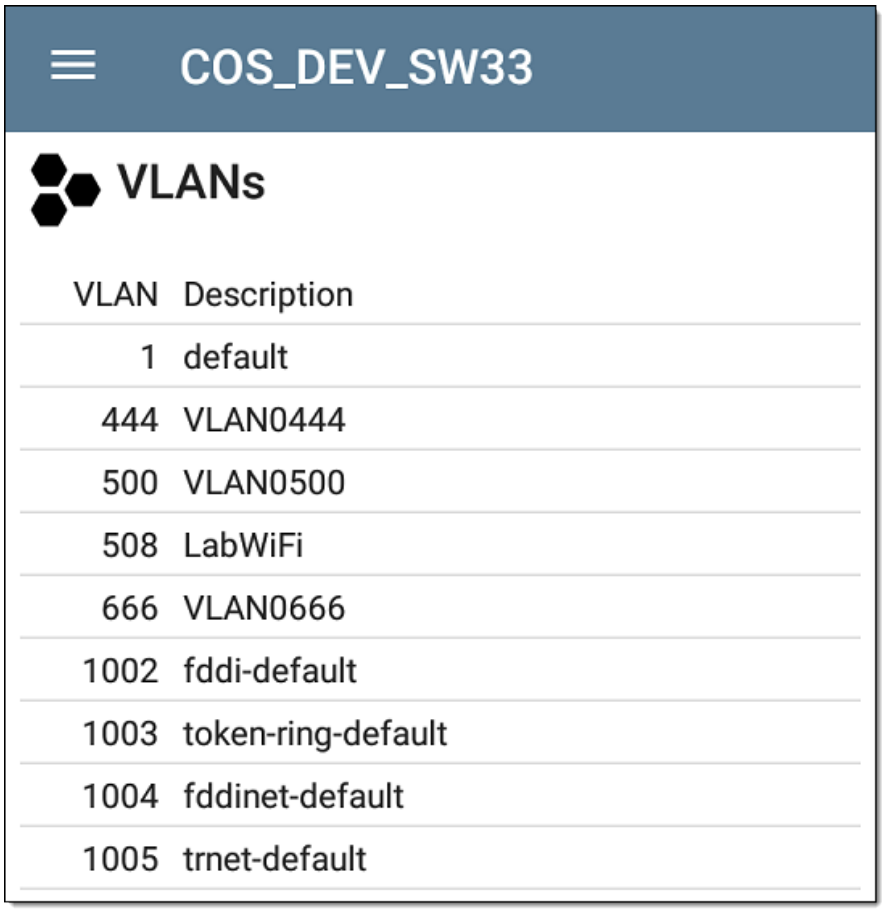
See also TCP Port Scan Settings.

VLANs

The VLANs card displays the VLAN IDs this device is using or for which it is configured.



This card does not appear if no VLANs are detected or configured. Tap the card to open the VLANs screen.



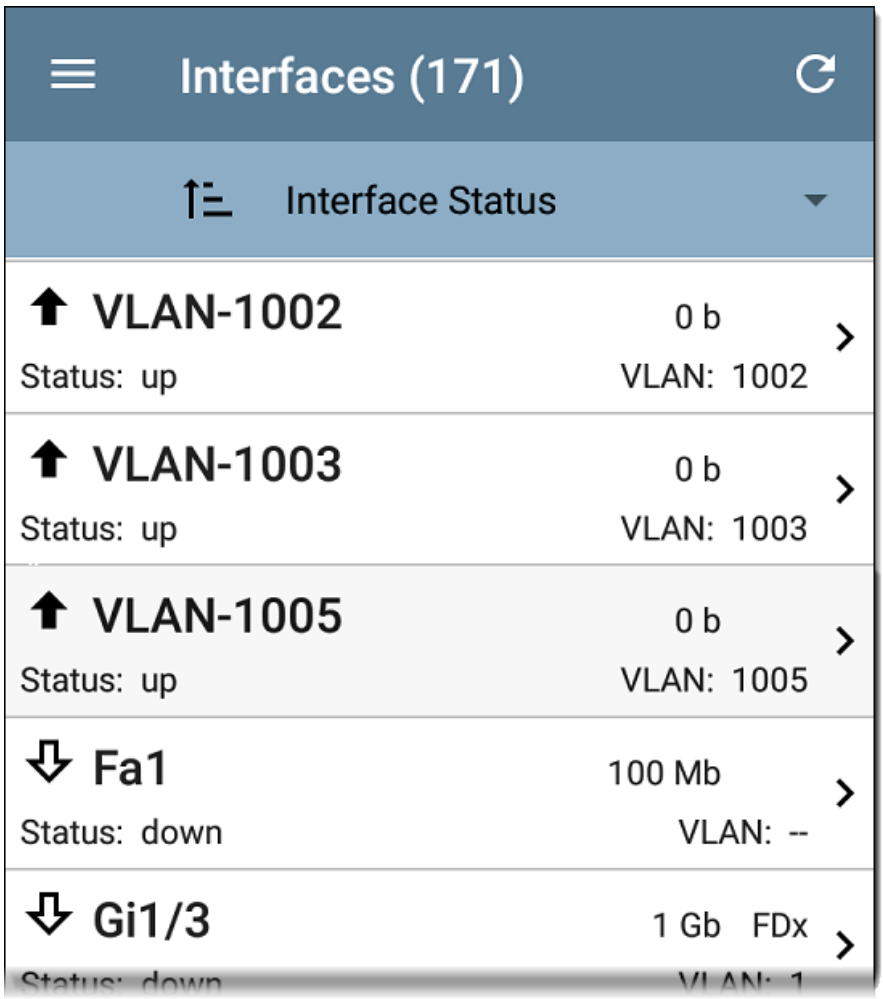
The VLANs Details screen also shows the description with each VLAN ID.

Interfaces

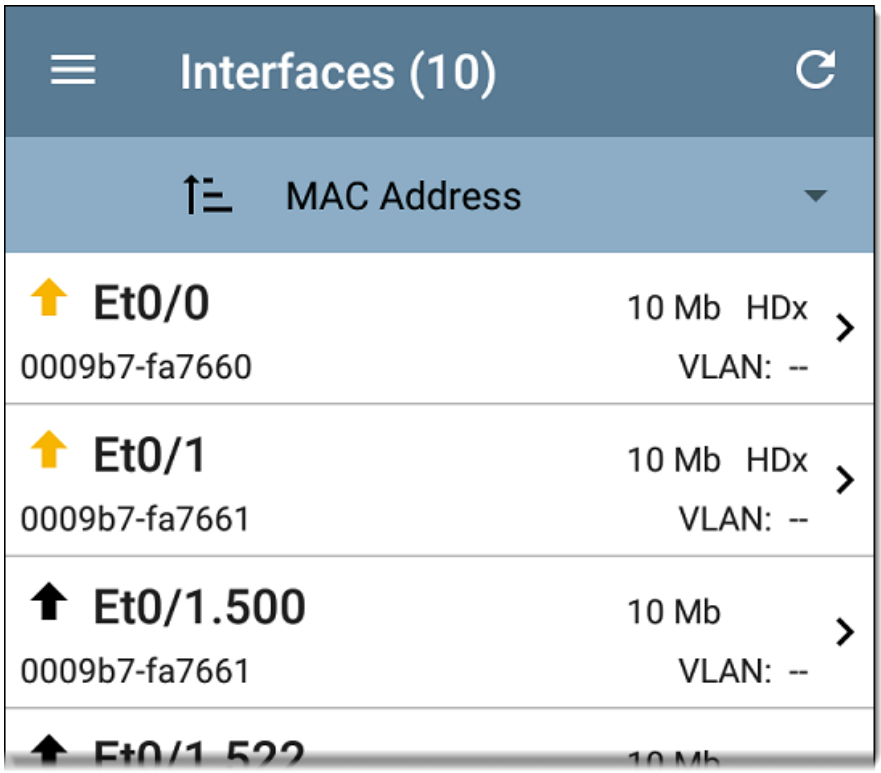
Interface are discovered using SNMP.

The Interfaces card shows the number of Up and Down interfaces and the total number of Interfaces to the right.

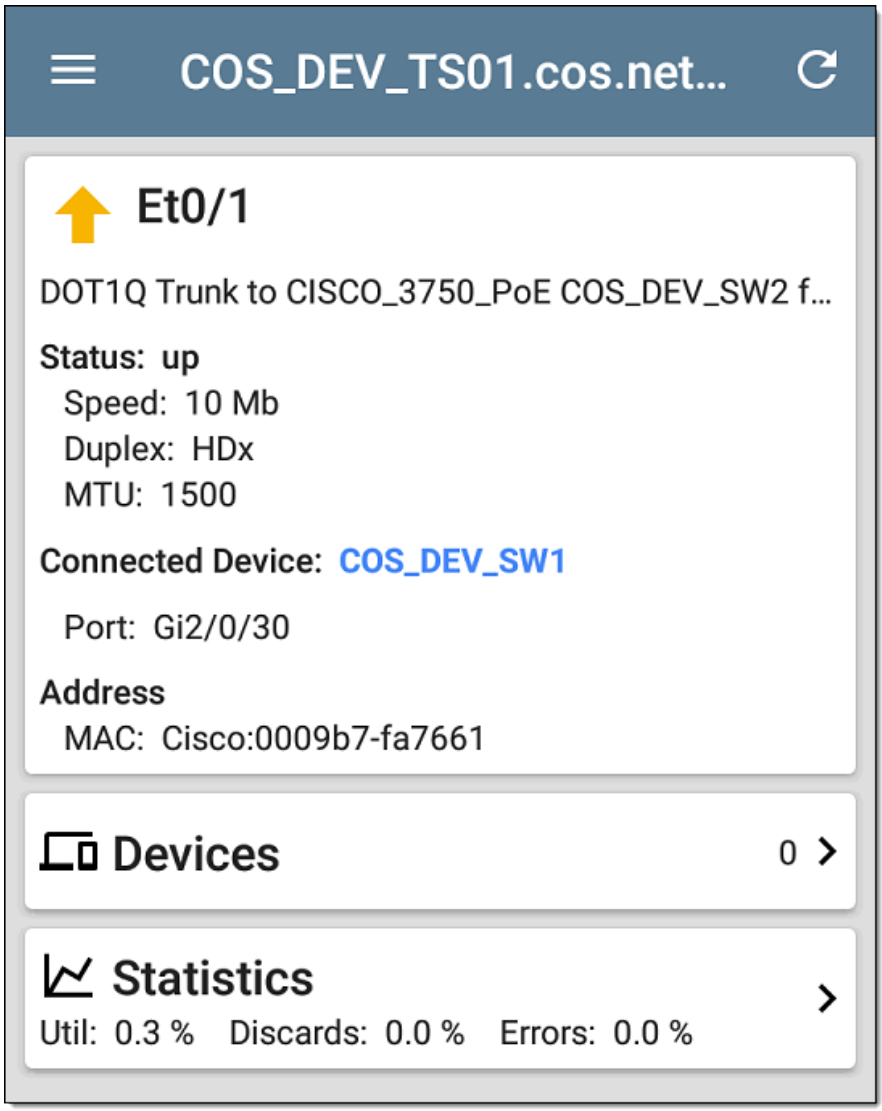
Tap the card to view the list of Interfaces.



Like other Discovery list screens, the Interfaces list provides a number of Sort options, and the selected sort option affects the type of information displayed. The image above shows Interfaces sorted by Status (up or down). The image below shows Interfaces sorted by MAC Address, so each Interface's MAC address is displayed.



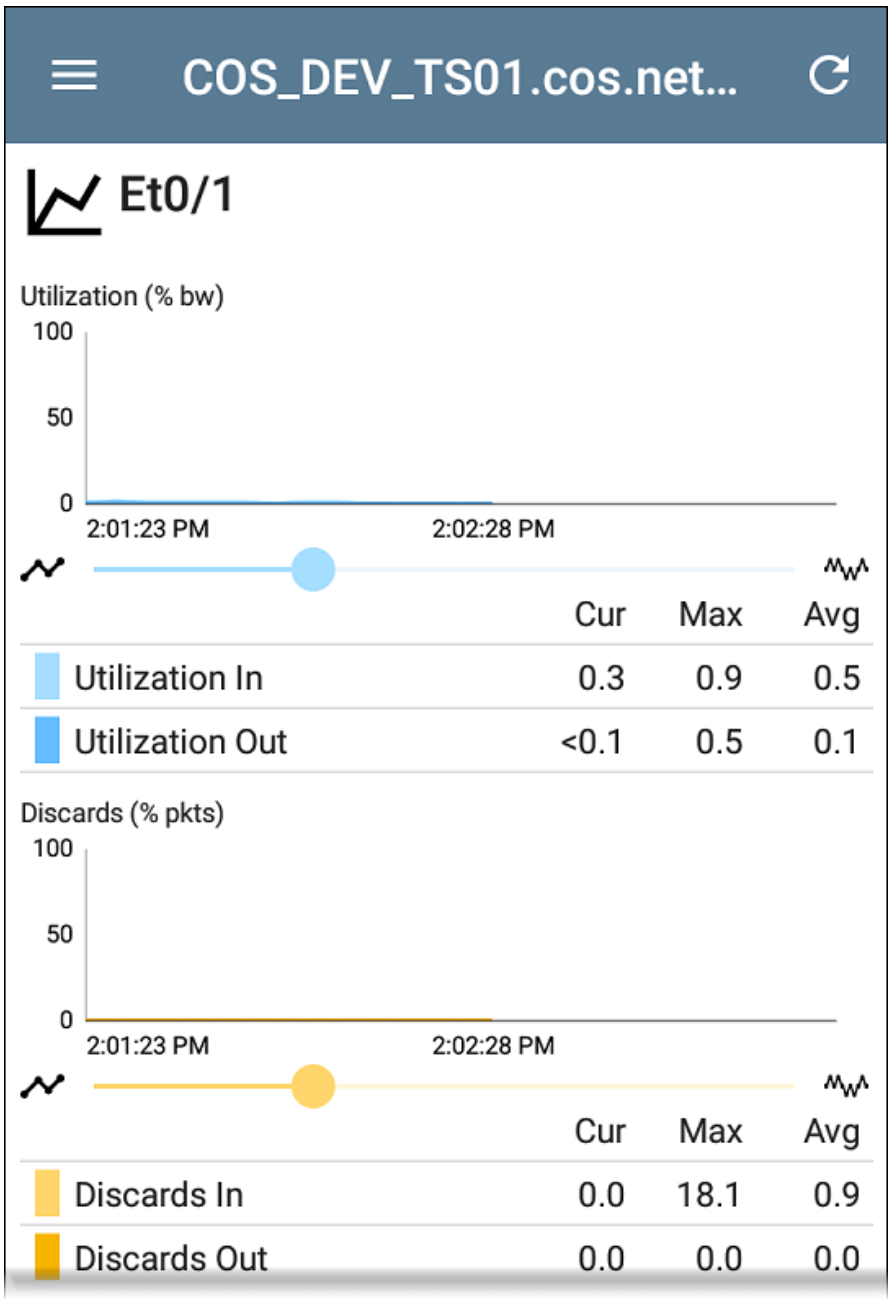
Tap an Interface row to open a new Discovery Details screen for that Interface.



The Interface Details screen contains a description of the interface and information about its Status, Connected Device and Port, and Address.

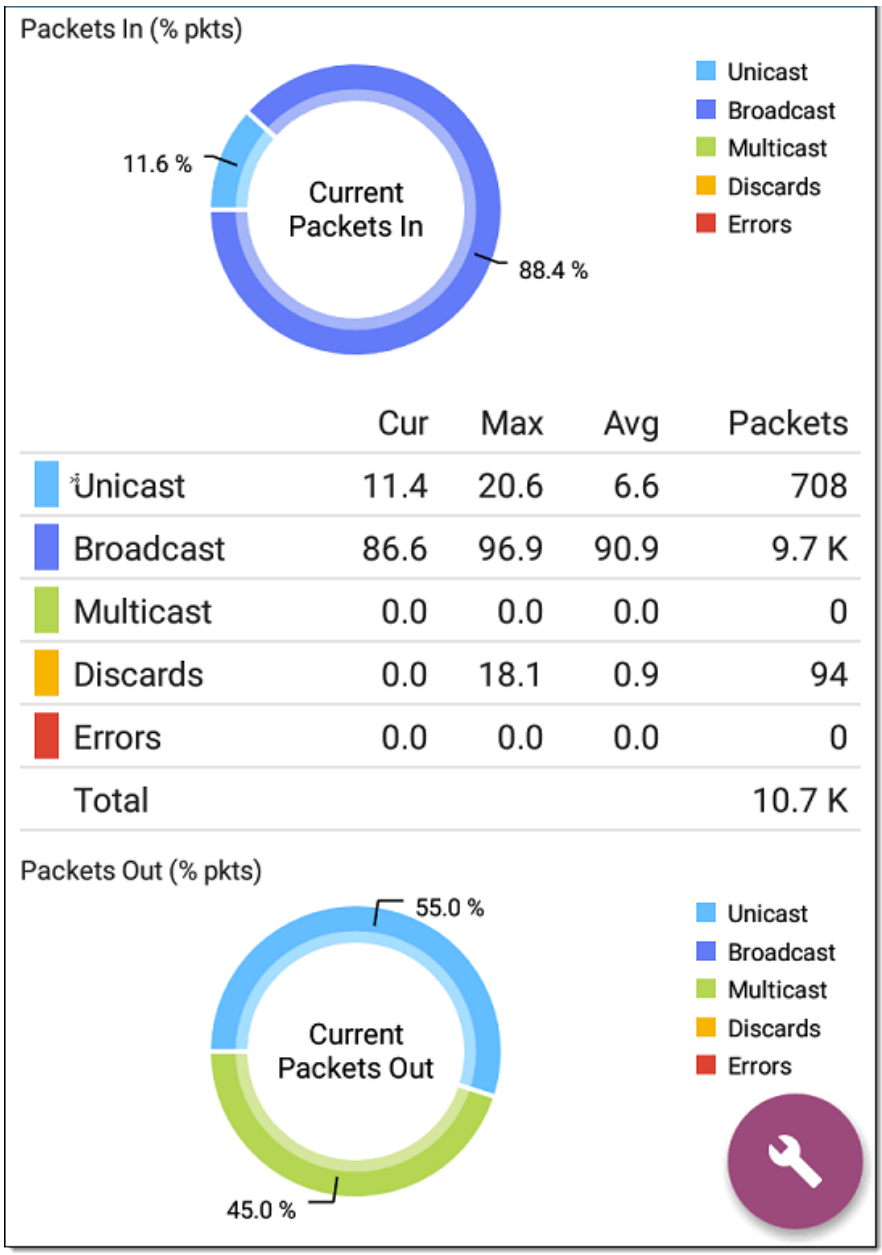
MTU: Maximum Transmission Unit, the maximum packet frame size configured on the interface port

From this screen, you can tap the lower cards to review any discovery **VLANs** and **Devices** for the Interface as well as graphs of the Interface **Statistics**.

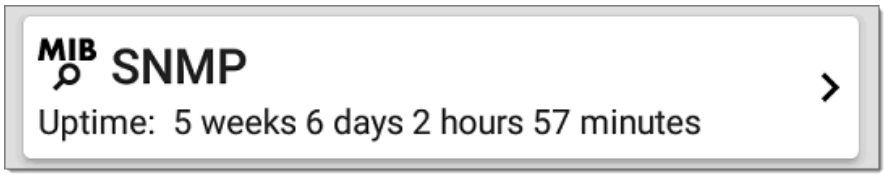


The Statistics screen displays real-time trending graphs of Utilization, Packet Discards, Packet Errors. See the Trending Graphs topic for an overview of the graphs' pan and zoom controls.

Below the trending graphs are pie charts of Packet transfers to and from the Interface.



SNMP



This card shows SNMP Uptime. Tap the card for additional details.

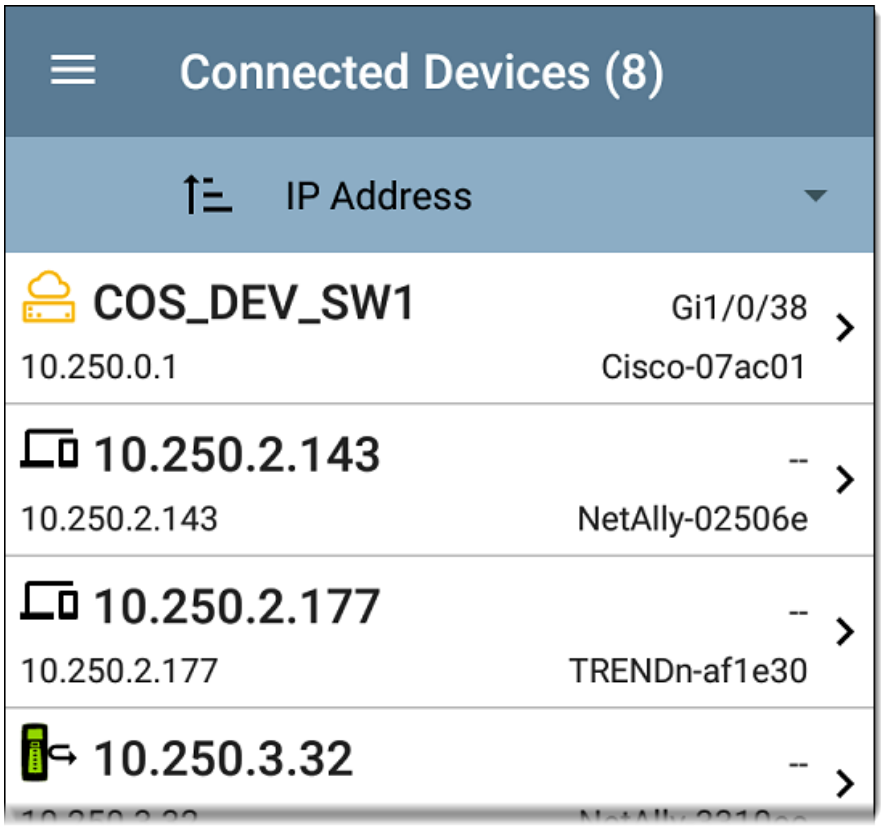
SNMP System Group: These data fields are gathered from the system group and other key device version information.

SNMP: SNMP versions the device supports, Engine ID (for v3), and how the EtherScope is currently communicating with the device, along with credentials, including the Community String in use

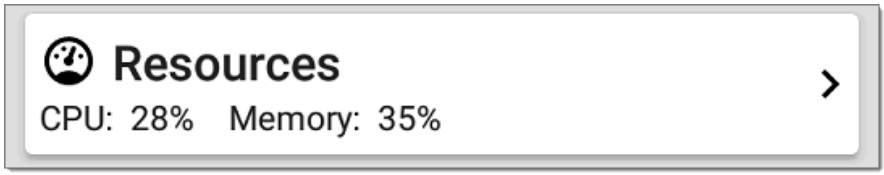
Connected Devices

The Connected Devices card appears on the Details screen for Unknown Switches. While the EtherScope may be unable to directly identify the connected switch, the devices connected to it provide clues about where the switch is operating.

The Connected Devices card shows the number of discovered devices that are connected to the Unknown Switch. Tapping the card opens a Discovery list screen with the connected devices.

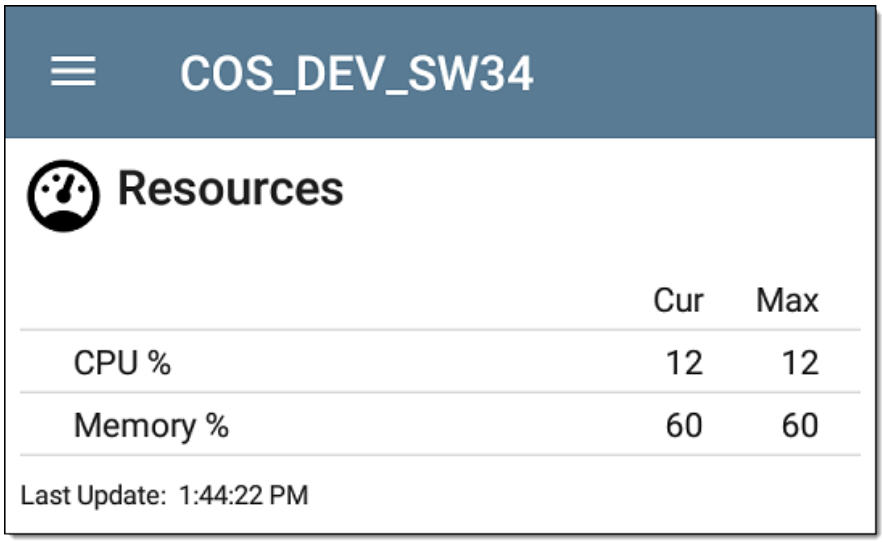


Resources



The Resources card shows the percentages of CPU, memory, and storage usage on the device. This information is gathered via SNMP.

Tap the card to view current and maximum resource utilization measurements.

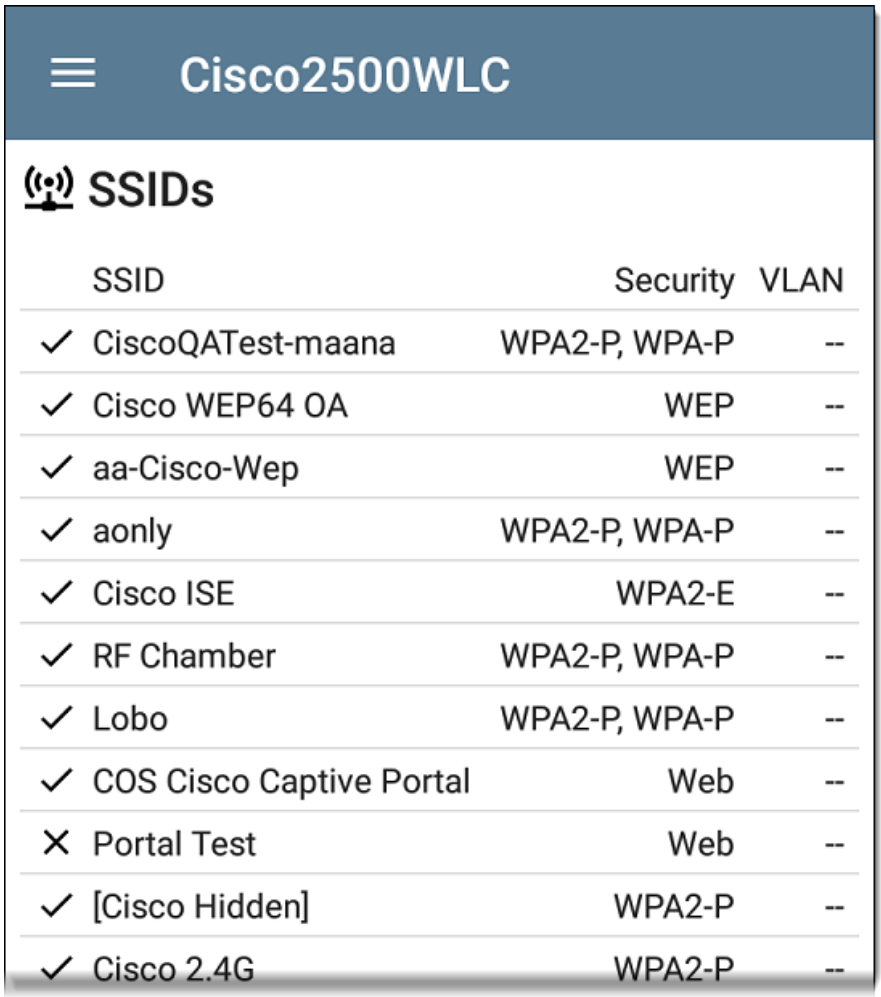


By default, EtherScope displays a **Warning** condition if CPU, Memory, or Storage utilization is above 90%. You can adjust problem detection and thresholds in the Problem Settings accessed from the Discovery navigation drawer.

SSIDs

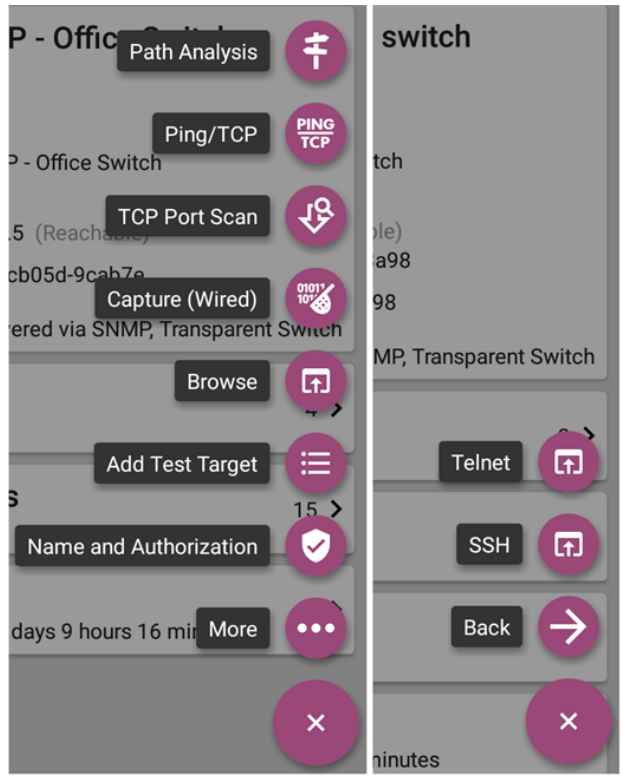
The SSIDs card appears in the Details for Wi-Fi Controllers. This information is gathered via SNMP.

This card shows the number of SSIDs gathered from SNMP. Tap the card to view the list of SSIDs.



On the SSIDs screen, each SSID is shown with its Security type(s) and any VLANs. SSIDs with a checkmark to the left are enabled, and those with an ✕ are disabled.

Discovery App Floating Action Menu



The floating action button (FAB) on Details screens offers additional actions depending on the device type and connection available.

Opening other NetAlly apps, such as Path Analysis, Ping/TCP, or Capture from a Details screen auto-populates the new app with the device's name and/or address. In this way, both the Discovery and Wi-Fi apps provide a helpful shortcut and that avoids making you retype the target addresses or hostnames in other testing apps.

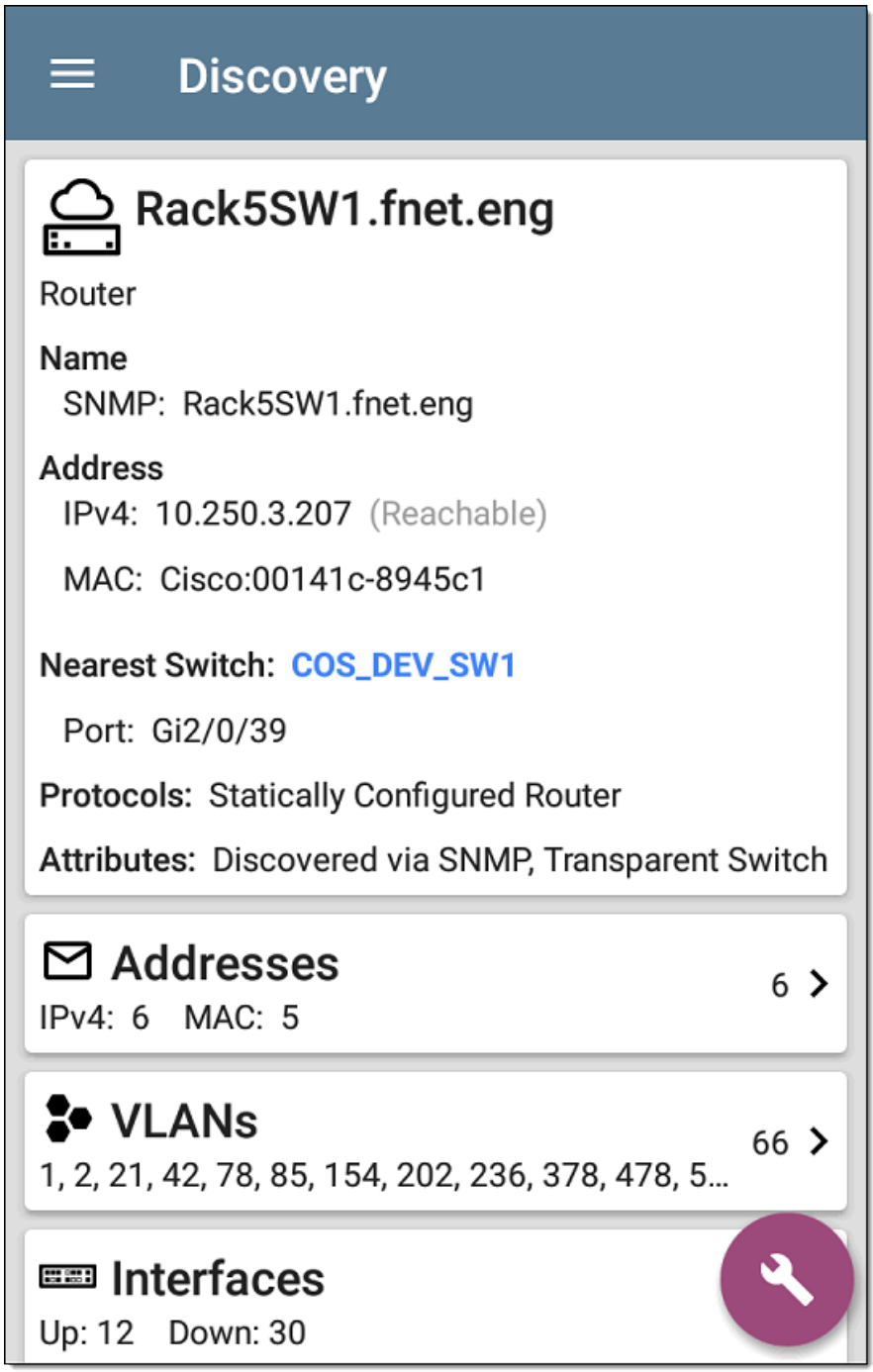
- Tap **TCP Port Scan** to open the TCP Port Scan screen in the Discovery app.
- Tap **Browse** to open the Chromium browser.

- Tap **Add Test Target** to create a new AutoTest target matching the currently selected device. A dialog first displays to select the test type, then the AutoTest app opens, displaying the newly added target's settings. You can then further customize the target.
- For devices with a MAC address or BSSID, tap **Name** and **Authorization** to open a dialog that lets you assign a custom user name and Authorization status. See Assigning a Name and Authorization to a Device in the Wi-Fi app chapter.
- Tap **More** to open a secondary list of floating action buttons:
  - Tap **Telnet** or **SSH** to open the JuiceSSH app.
  - Tap **Back** to return to the primary FAB list.

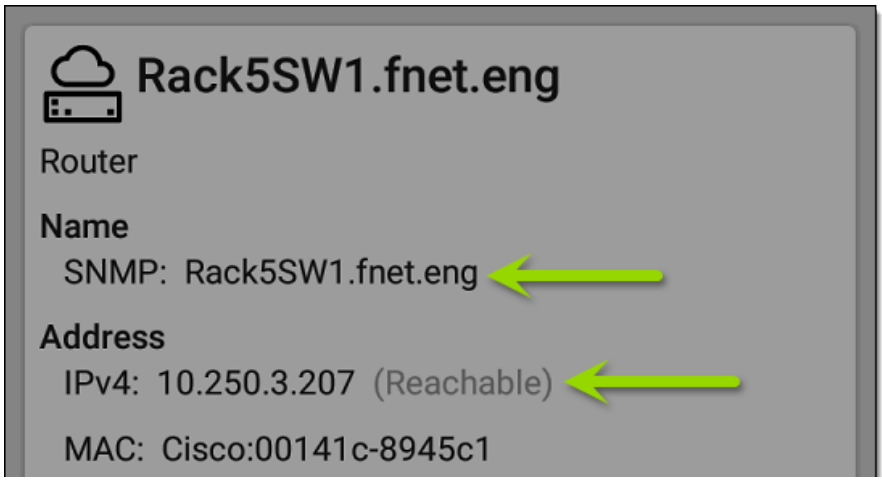
Auto-Populating Device Addresses

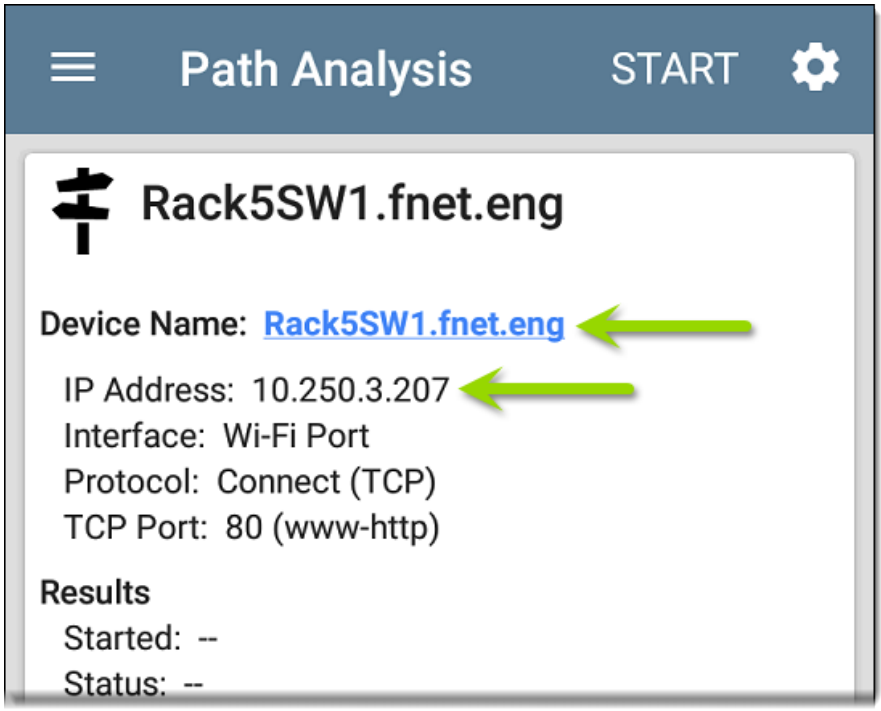
When another app is opened from the FAB, the default address and name shown on the Top Details Card are the targets populated.

For example, the Router shown in the Details screen below has multiple IPv4 and MAC addresses (which can be viewed by tapping the Addresses card).



When you open the FAB and select a different app, such as Path Analysis, only the address and name listed at the top of the Details screen are populated in the Path Analysis app.





To open another screen or app with a different address, open the Addresses card, and select another address to view its Details screen.

Back to Title and Contents

Device Types

The Discovery app lists and analyzes the types of devices explained in this section. Different data may be available to the EtherScope depending on the device type, how it was discovered, and your configured settings.

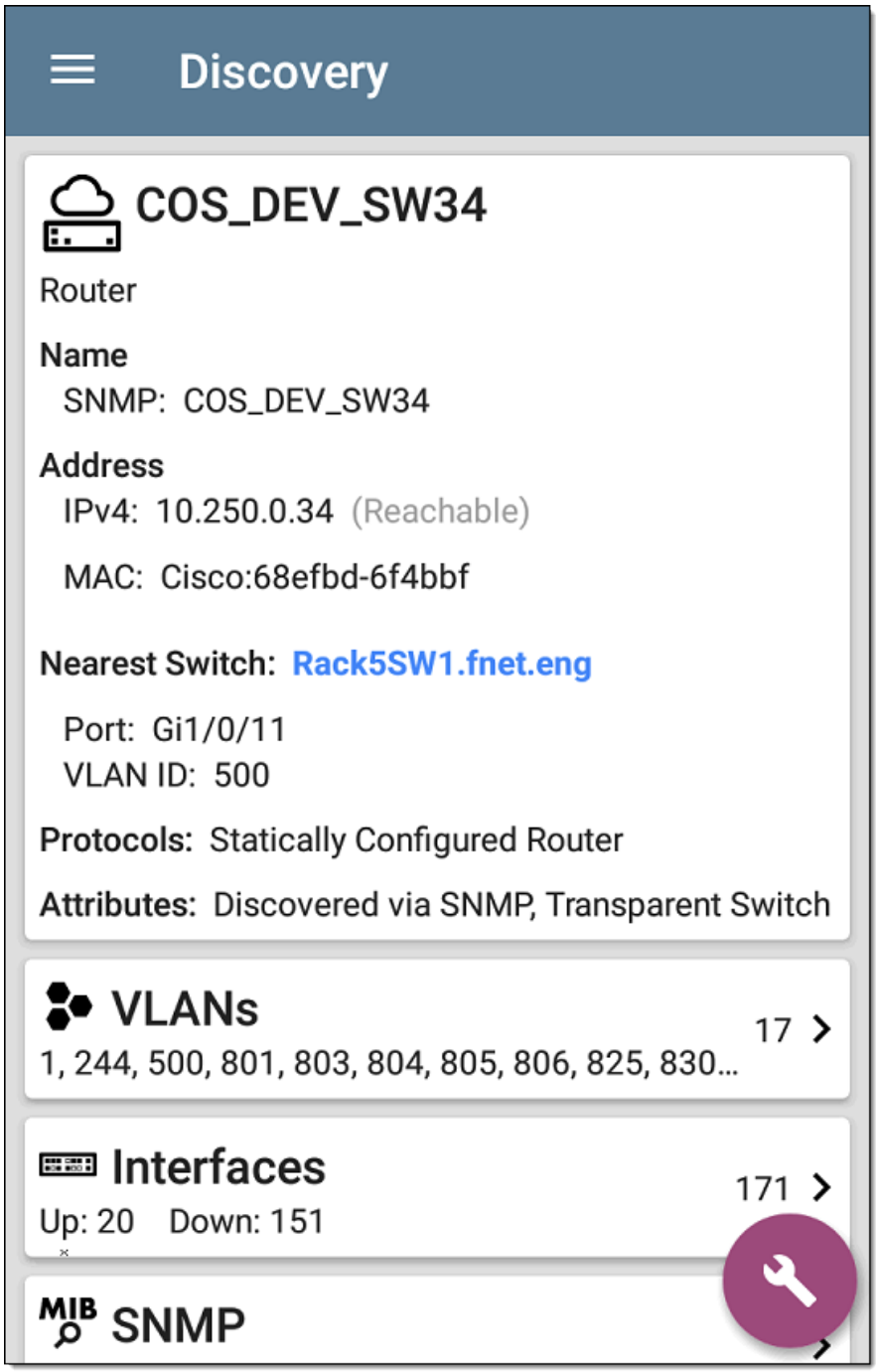
See Discovery Settings for SNMP Configuration and Devices Discovered Through Other Devices options.

For descriptions of the different Details cards and screens, see Discovery Details.

The images in the rest of this section represent an example of the data Discovery that may display for each device type.

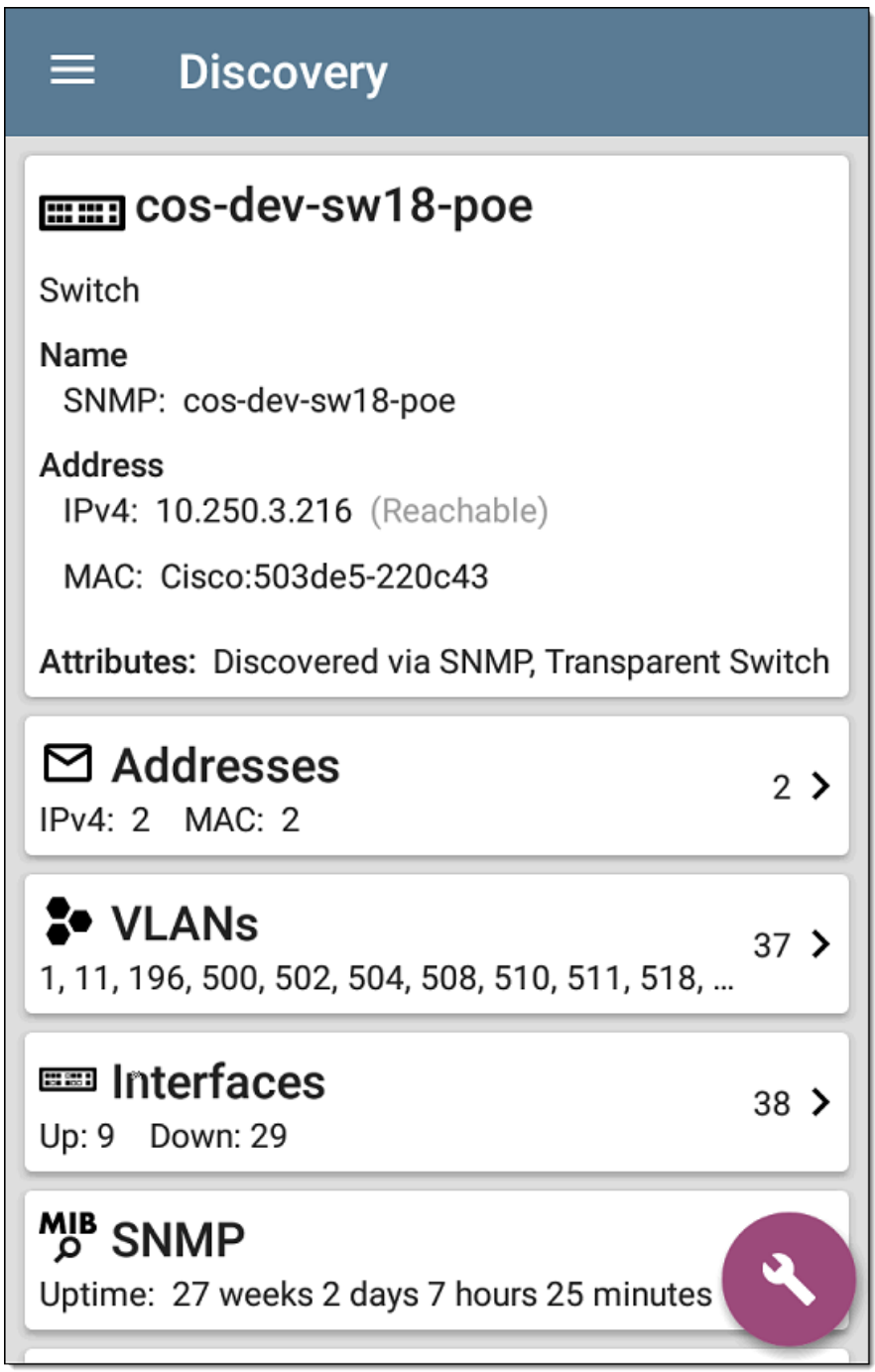
Routers

EtherScope discovers IP routers by monitoring traffic and querying hosts.



Switches

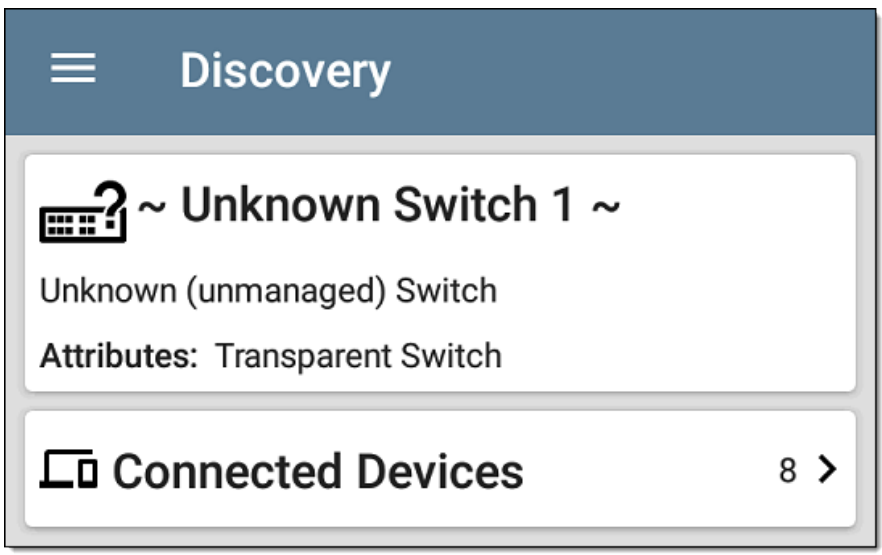
Switches are also discovered by monitoring traffic and querying hosts.



Unknown Switches

Unknown switches are detected indirectly by analyzing traffic going through surrounding switches. The EtherScope cannot identify the switch, but it can sense where a switch is active on the network via the device MAC addresses in that space.

The EtherScope numbers the switches as they are discovered. (These numbers may change each time the discovery process runs.)



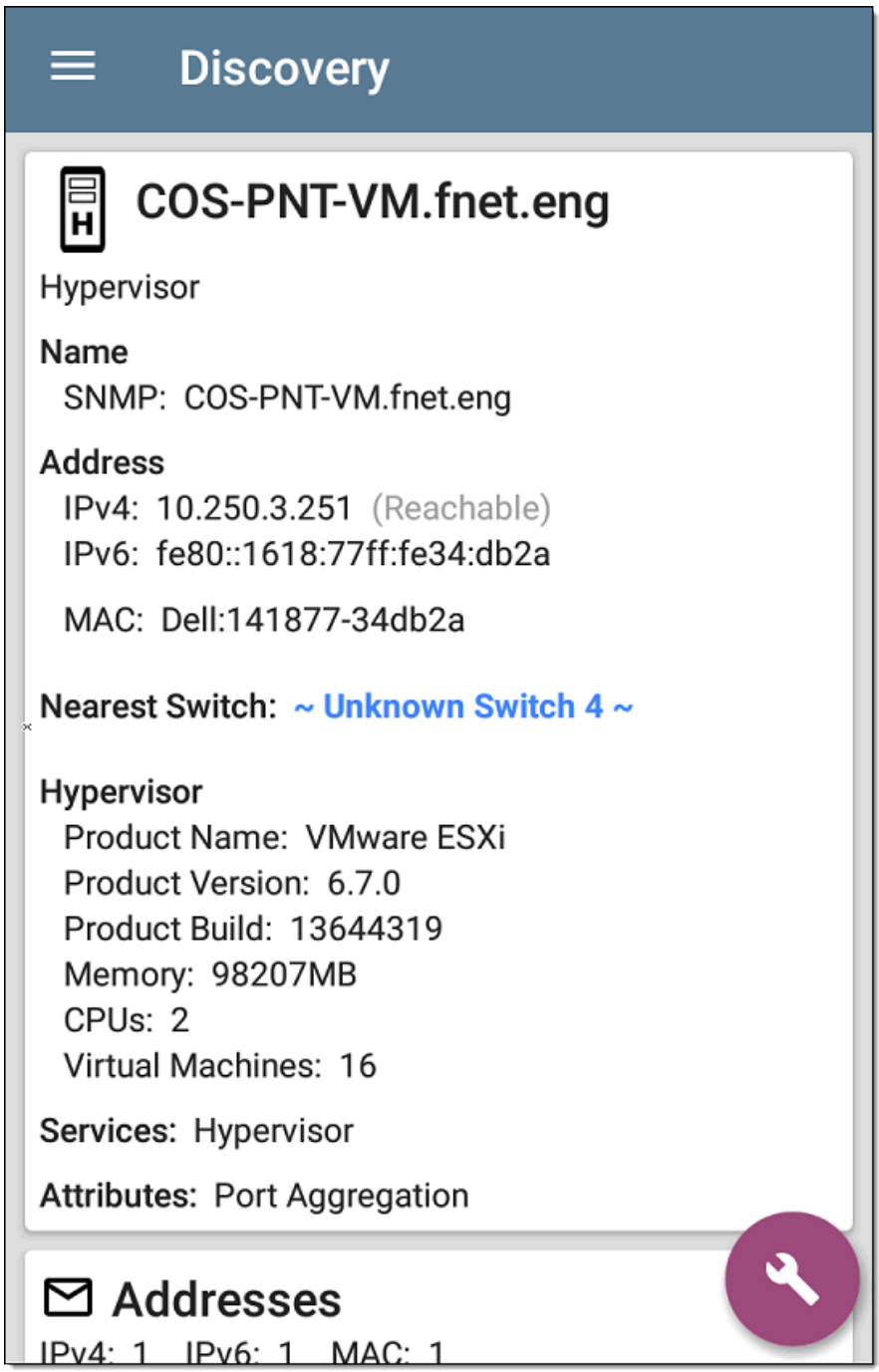
The Unknown Switches Details screen shows the number of devices connected to the switch. Tap the Connected Devices card to view the connected devices, which may provide clues about the location of the unknown switch.

Network Servers

Network servers include NetBIOS, DHCP, and DNS servers.

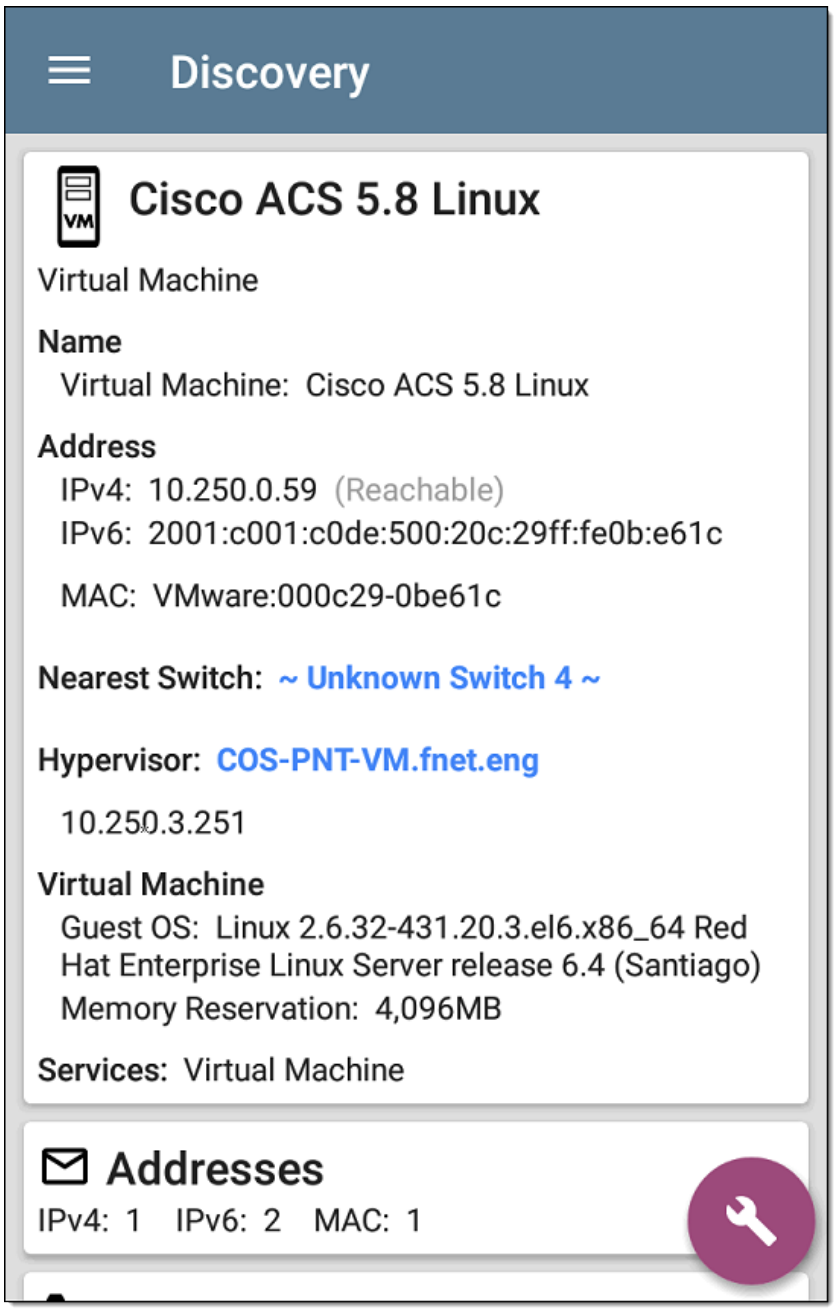
Hypervisors

VMware hypervisors are discovered via SNMP. The hypervisor's SNMP agent must be enabled for the EtherScope to discover it and classify it as a hypervisor.



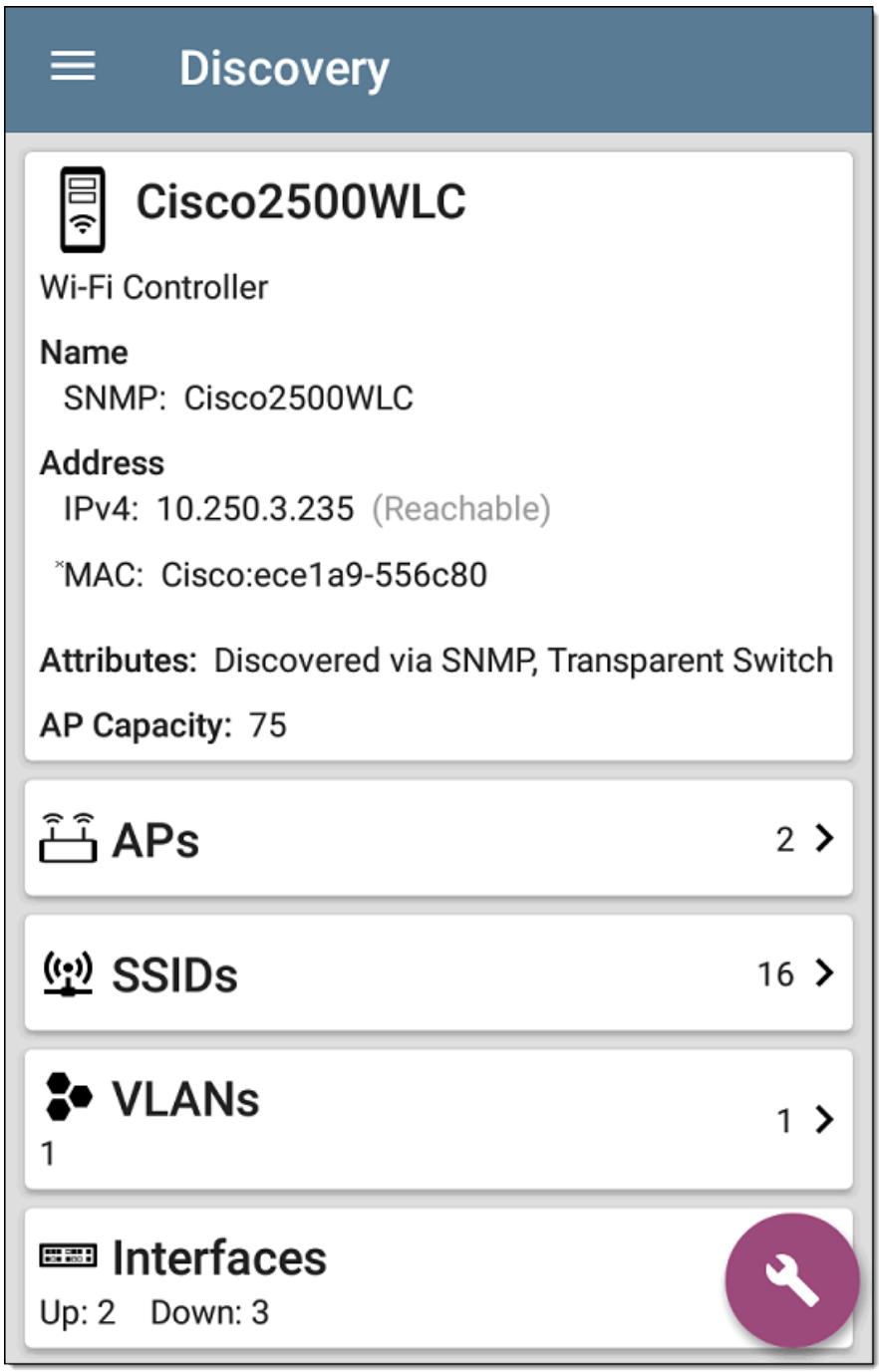
Virtual Machines

VMware virtual machines are discovered from VMware client table in SNMP-enabled VMware hypervisors. Devices are also classified as Virtual Machines if they have a VMware MAC.



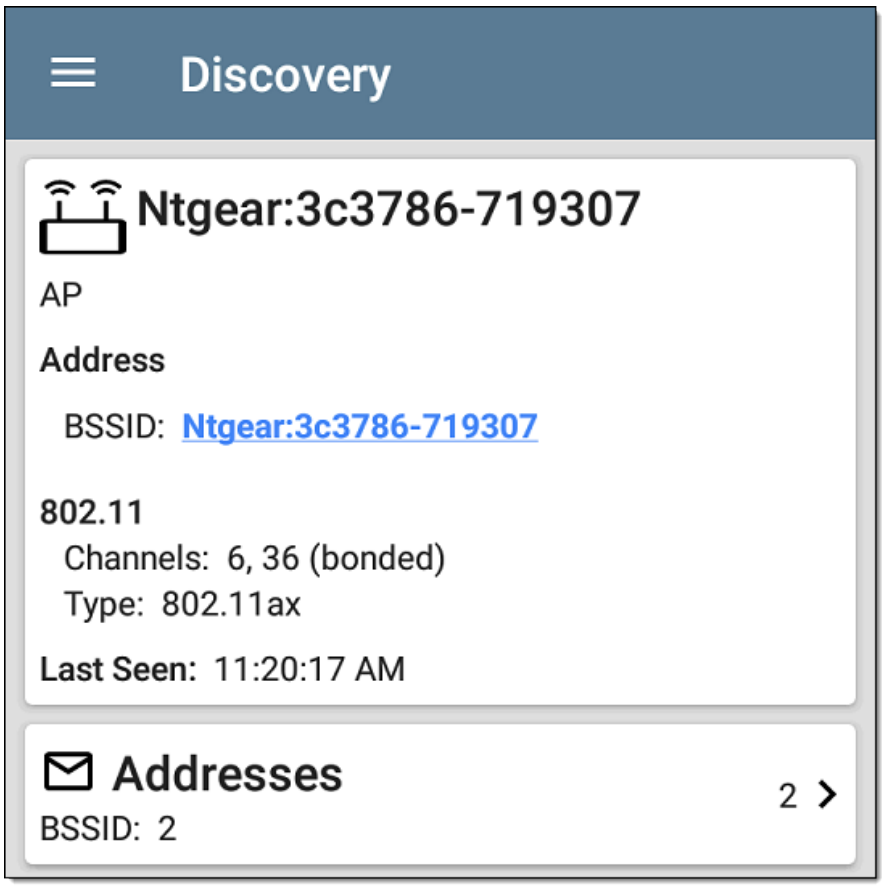
Wi-Fi Controllers

EtherScope can discover SNMP enabled Wi-Fi controllers, including Cisco and Aruba Wi-Fi Controllers.



Access Points (APs)

The EtherScope discovers APs through wireless packet analysis and SNMP queries with a linked connection through a management or test port.

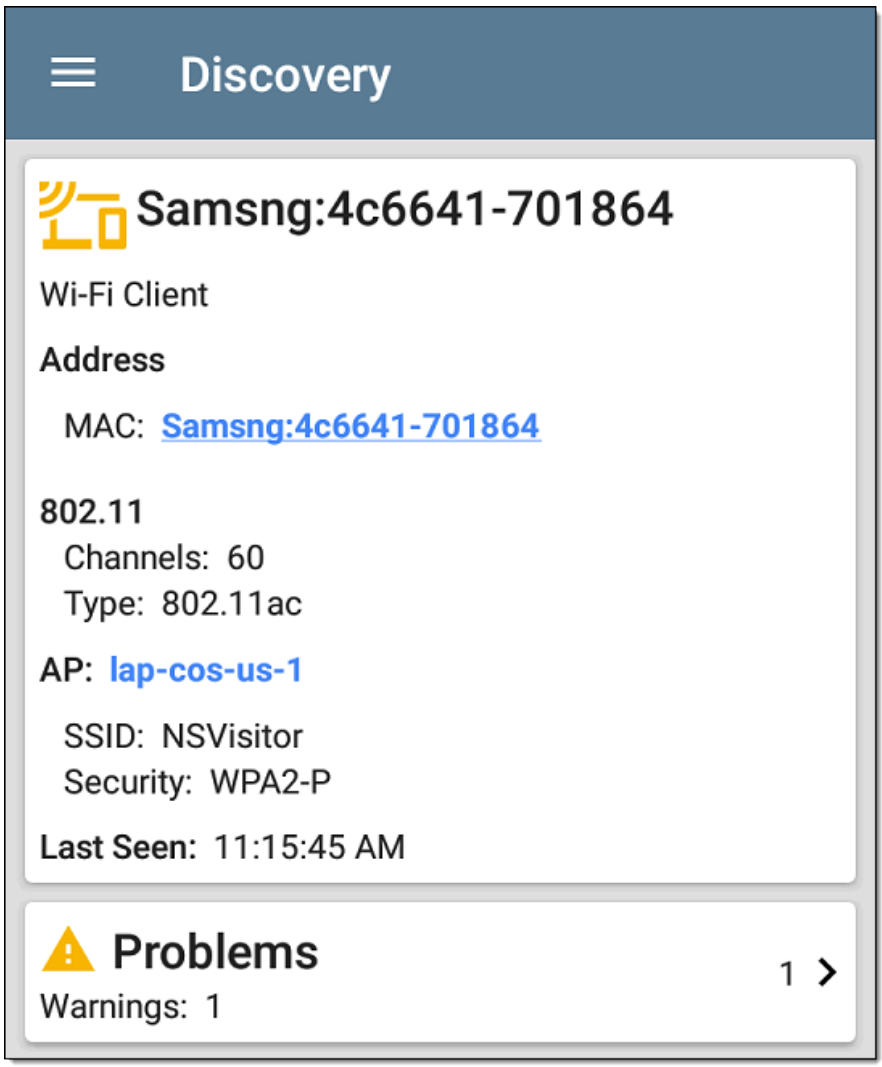


See also APs in the Wi-Fi analysis app.

Back to Title and Contents

Wi-Fi Clients

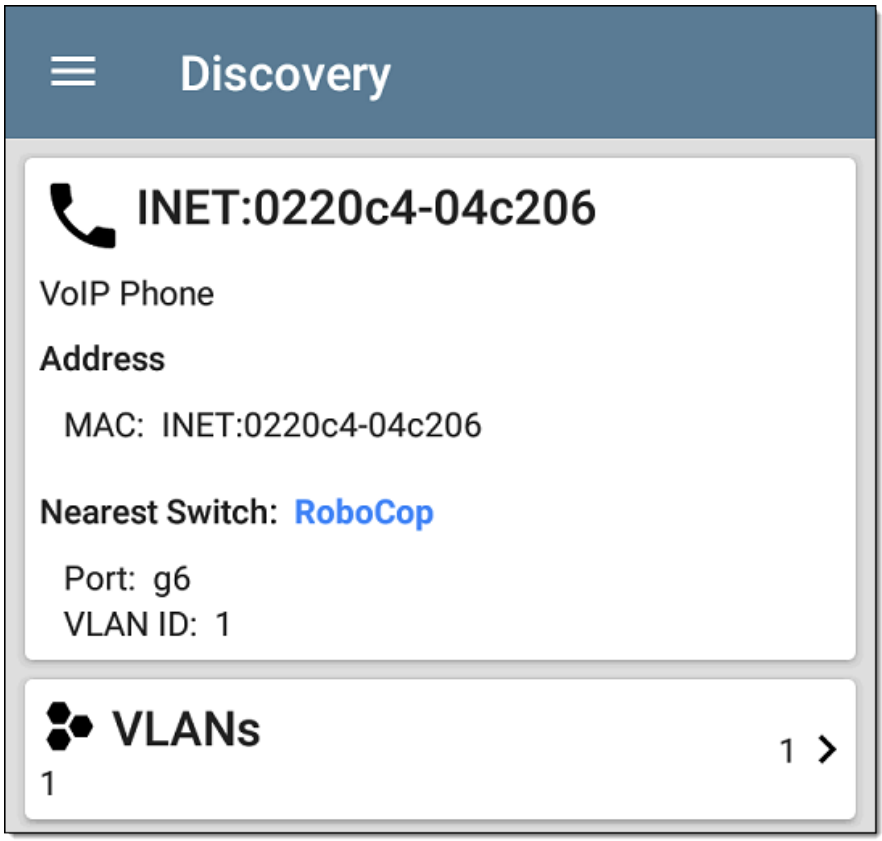
Wireless clients are discovered through wireless packet analysis and SNMP queries with a linked connection through a management or test port.



See also Clients in the Wi-Fi analysis app.

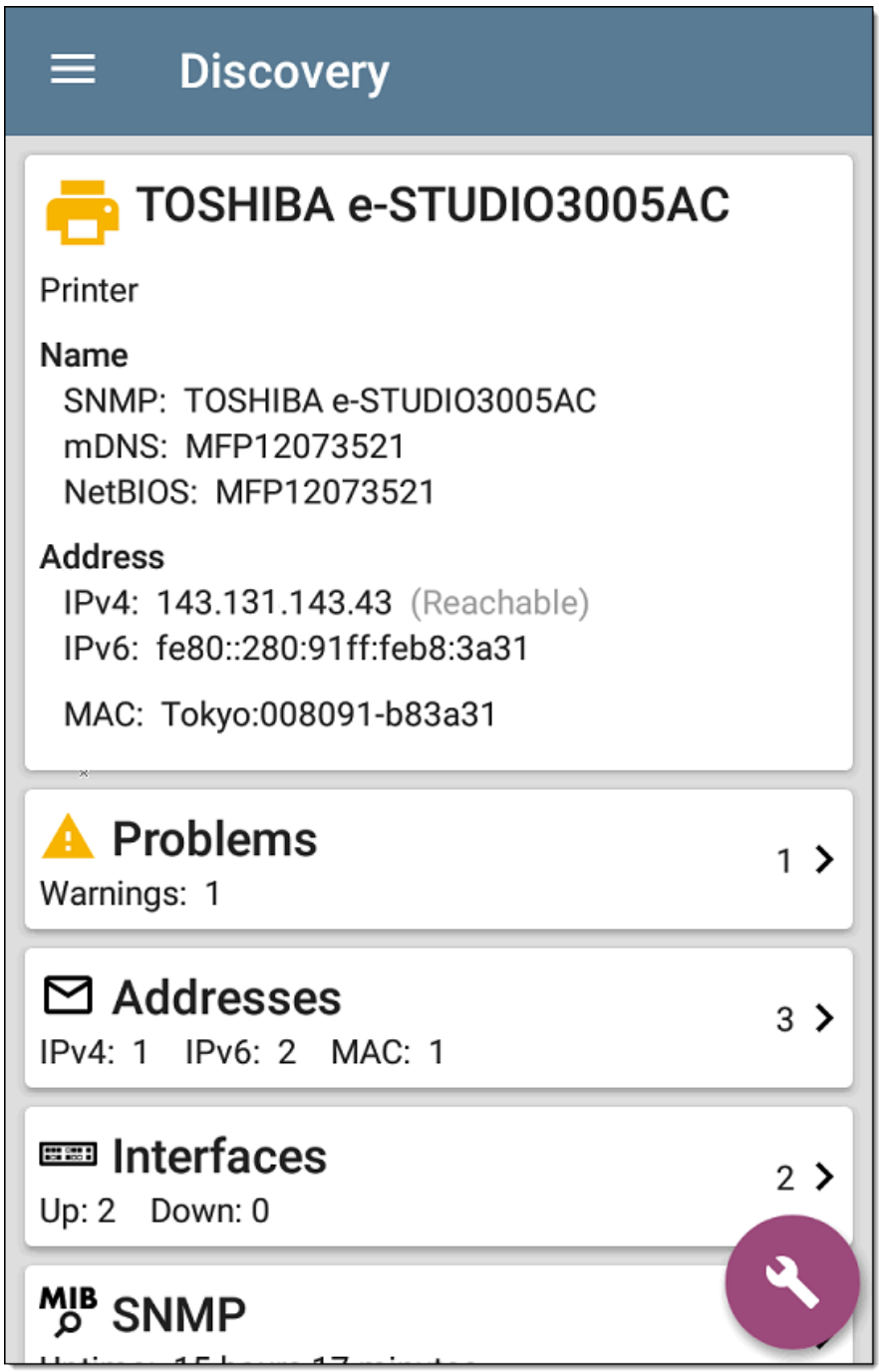
VoIP Phones

VoIP discovery provides visibility into the VoIP and layer 2/3 configuration of the network.



Printers

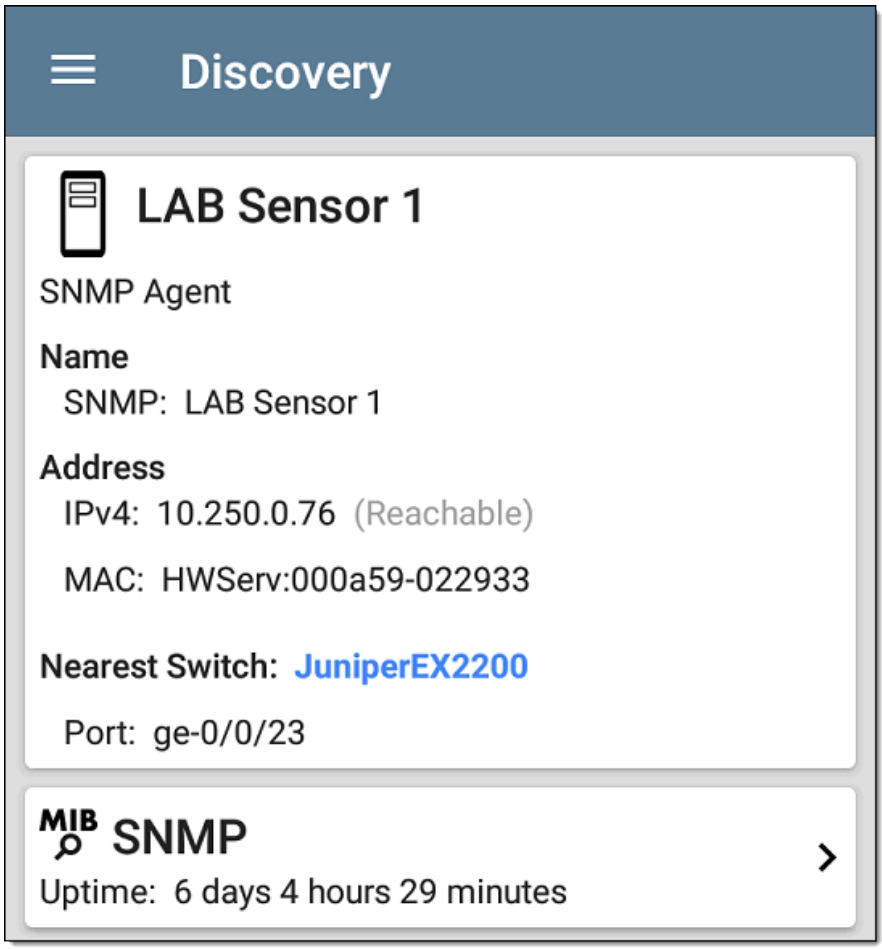
The EtherScope identifies IP printers via the SNMP Printer MIB and IPX printers via diagnostic requests and queries.



SNMP Agents

SNMP agents are discovered using SNMP queries. See SNMP Configuration.

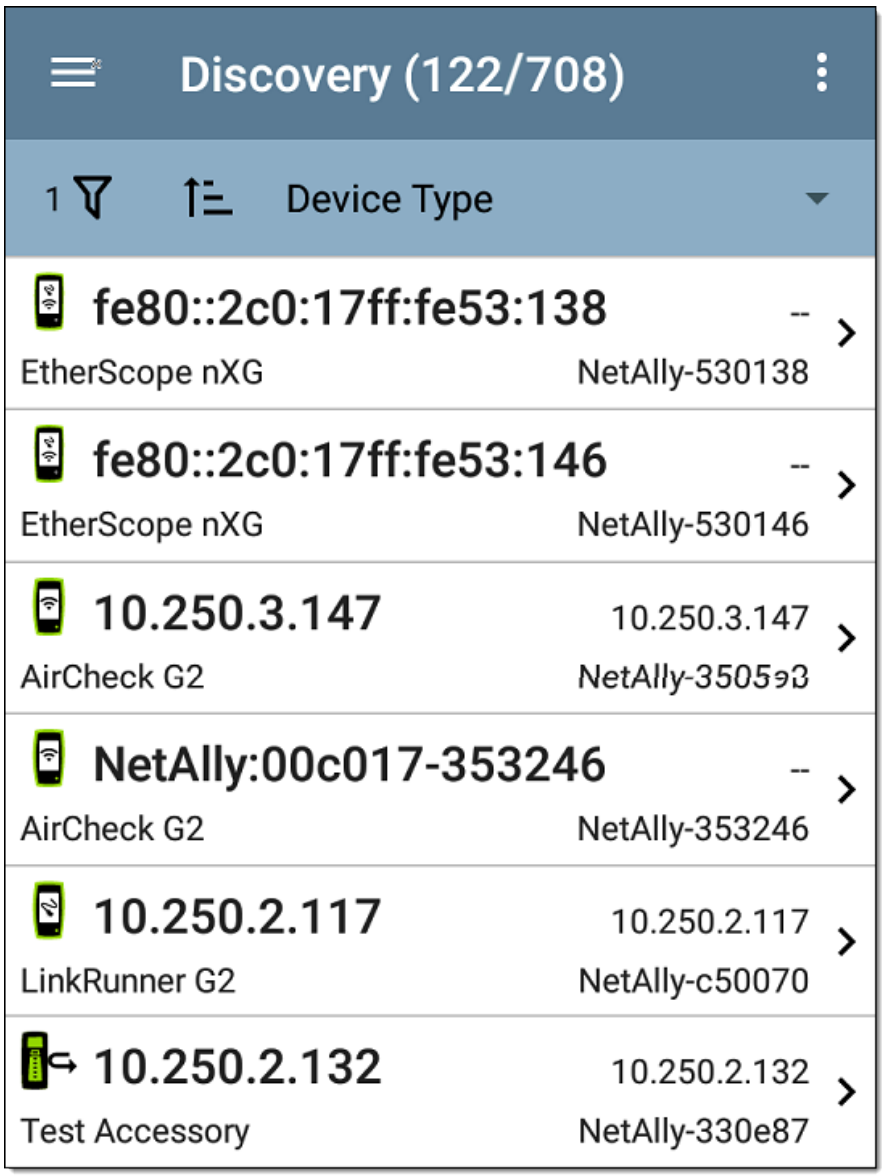
> NOTE: If EtherScope cannot discover the SNMP agents on your devices, they may be connected to another subnet, like a management subnet. Solve this issue by adding the subnet to Extended Ranges.



See also SNMP Details.

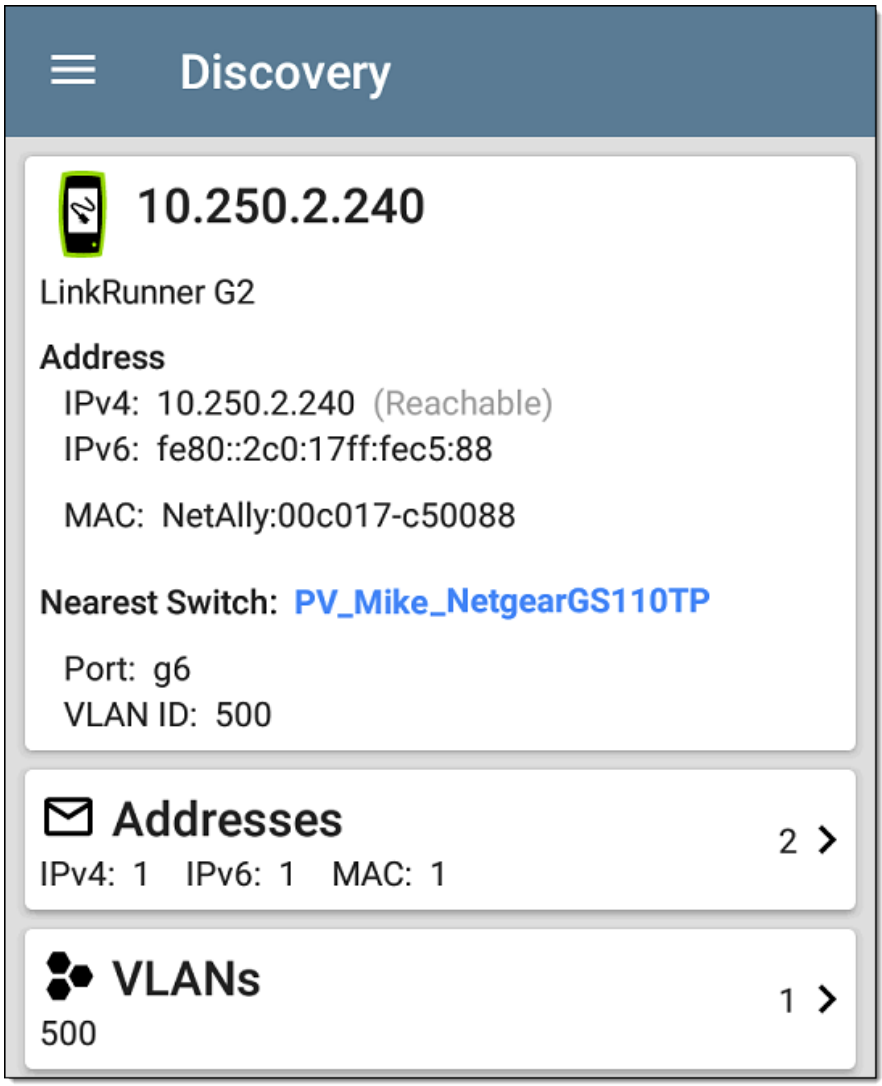
Network Tools

The EtherScope can also identify other NetAlly network testers, including EtherScope, AirCheck G2, OneTouch AT, LinkRunner (AT and G2), and Test Accessory.



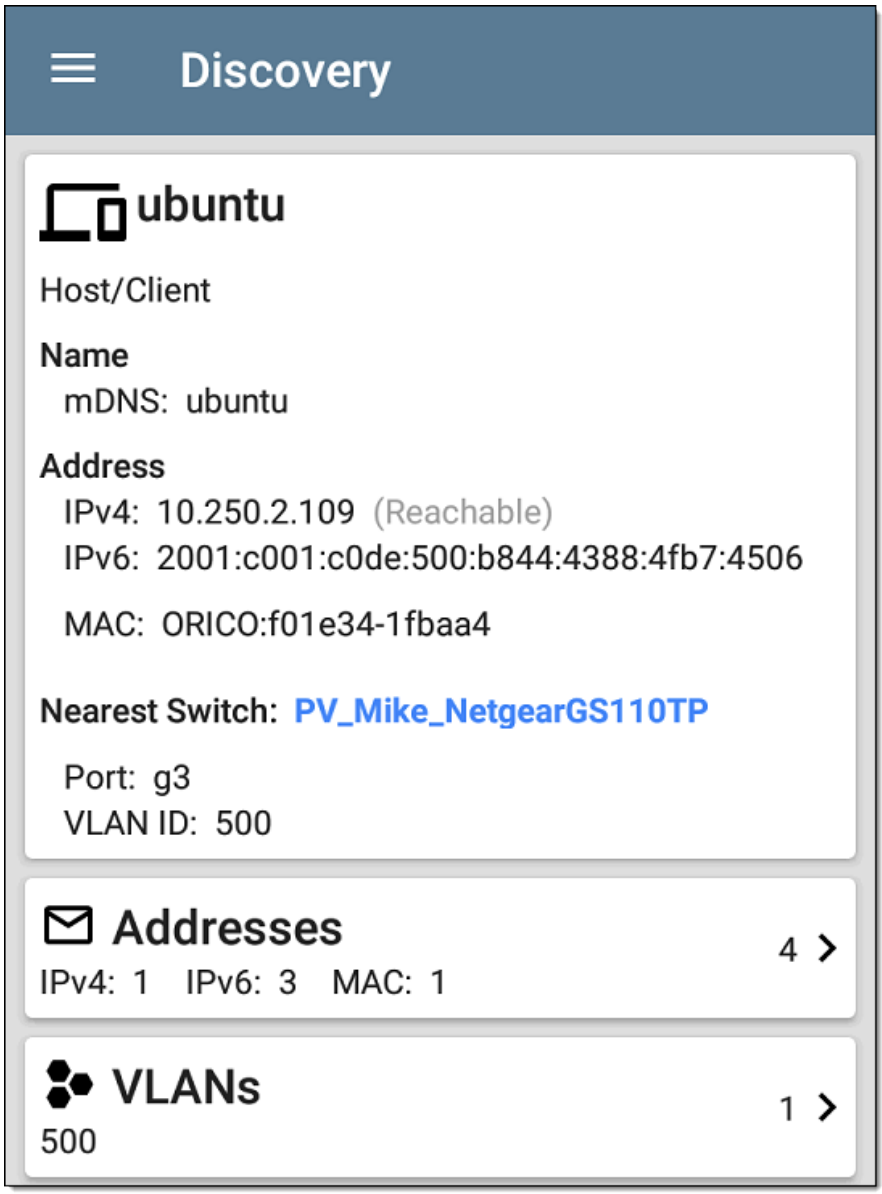
The image above shows several NetAlly tools as they appear in the main Discovery list.

EtherScope displays all the information it can gather about each tool on the Details screen.

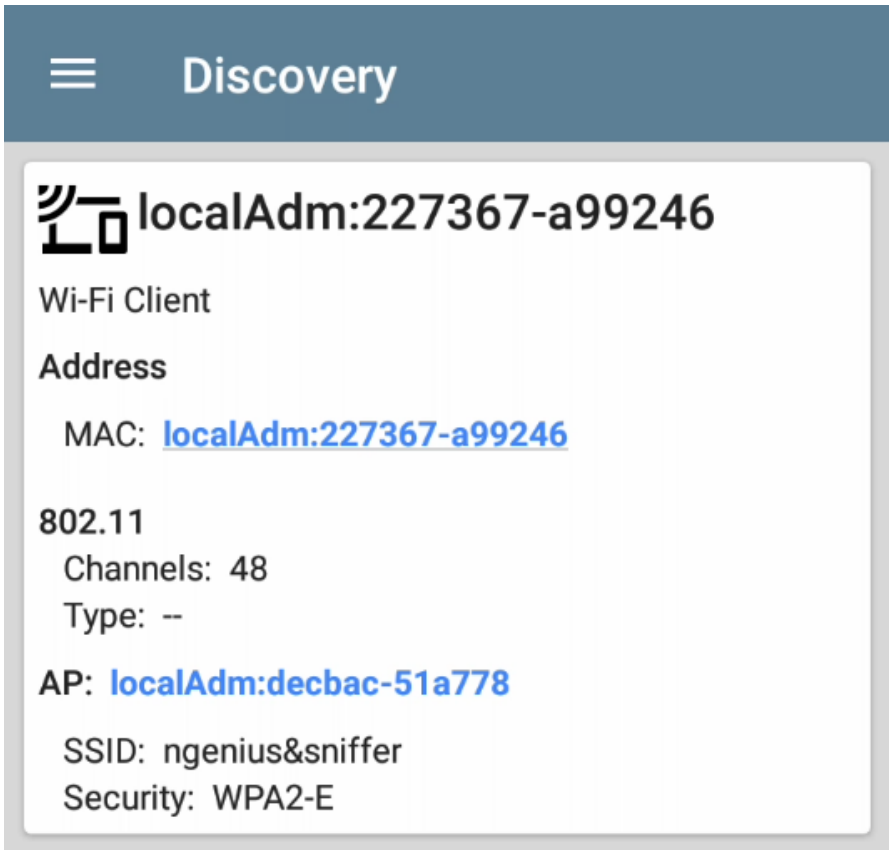


Hosts/Clients

Other hosts and clients are discovered by traffic monitoring and querying. If a host cannot be identified as belonging to one of the other categories (Switch, Router, VoIP device, etc.) then it is categorized as Host/Client.



NOTE: A MAC address that begins with LocalAdm indicates that the address has been locally randomized to prevent unauthorized tracking.



Back to Title and Contents

Device Names and Authorization

Assigning a Name and Authorization to a Device

The Wi-Fi and Discovery apps provide the option to assign a **Name and Authorization** to any discovered device with a MAC Address or BSSID.

Assigning a User Name and/or Authorization status does not change any of the information on the actual device, only how the device's information displays on the EtherScope on which the Name and Authorization are assigned.

You only need to assign a Name and/or Authorization to one BSSID or MAC address for a device with multiple addresses. Names and Authorizations are saved in the internal authname.txt file and remain set as the unit powers off and on.

This feature allows you to quickly identify your known devices and categorize them with the following statuses:

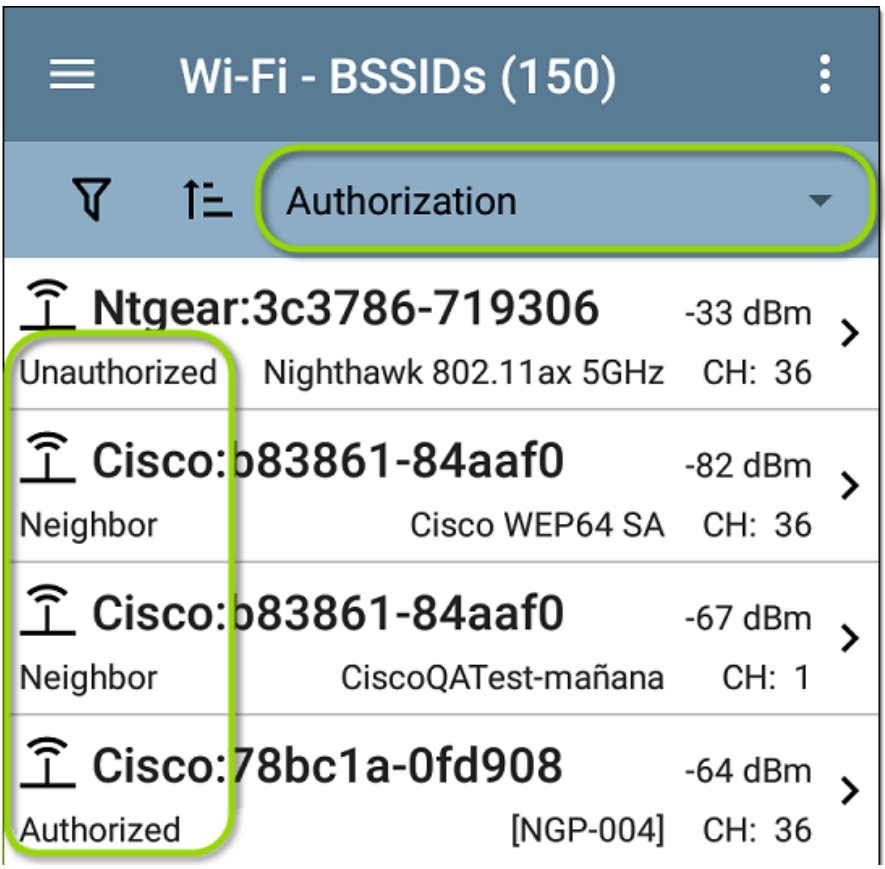
- **Authorized**: For devices approved for use on your network
- **Neighbor**: For devices owned and controlled by neighboring organizations
- **Flagged**: To give visibility to a specific device
- **Unknown**: For devices that have not been identified or classified
- **Unauthorized**: For devices that should not be on the network and may present a security risk
- **Unspecified**: Default unassigned Authorization status

While the Authorization statuses are designed with these intended meanings, you can use them however you like for your purposes.

Once set, the custom User Name is shown in other NetAlly apps wherever device information is displayed. The Authorization is displayed in the Discovery and Wi-Fi apps.

You can sort and filter by the assigned Authorization in the Wi-Fi and Discovery apps. When a list is sorted by Authorization (in normal sort

order), the devices with Authorizations of highest concern appear at the top. The image below shows a list screen sorted this way:



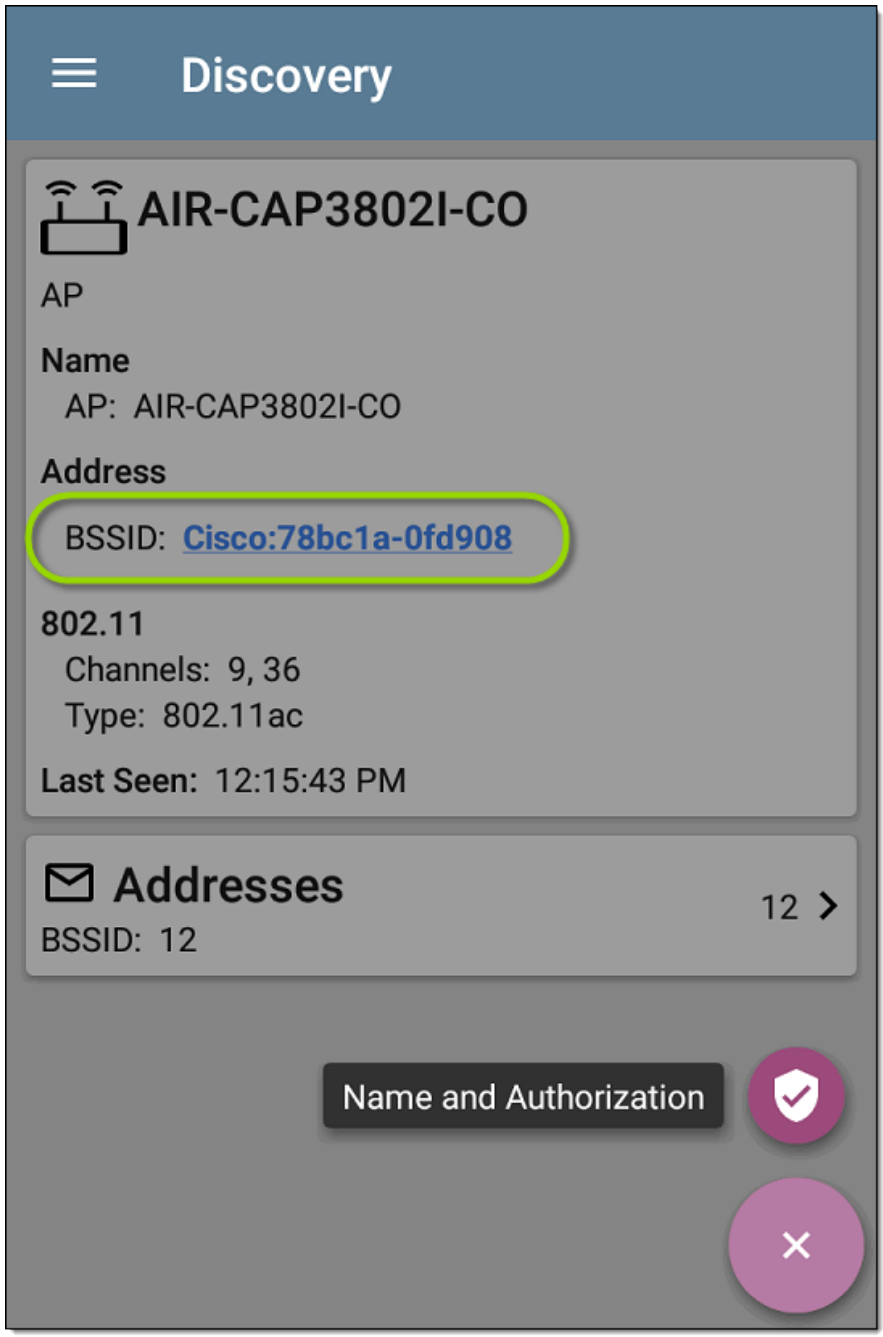
Applying a Name and/or Authorization

Access the **Name and Authorization** function from the floating action menu on a Discovery Details screen or a Wi-Fi Details screen for a BSSID or Client.

> NOTE: When applying an Authorization to a device with multiple BSSIDs or MAC addresses, the Authorization status is only

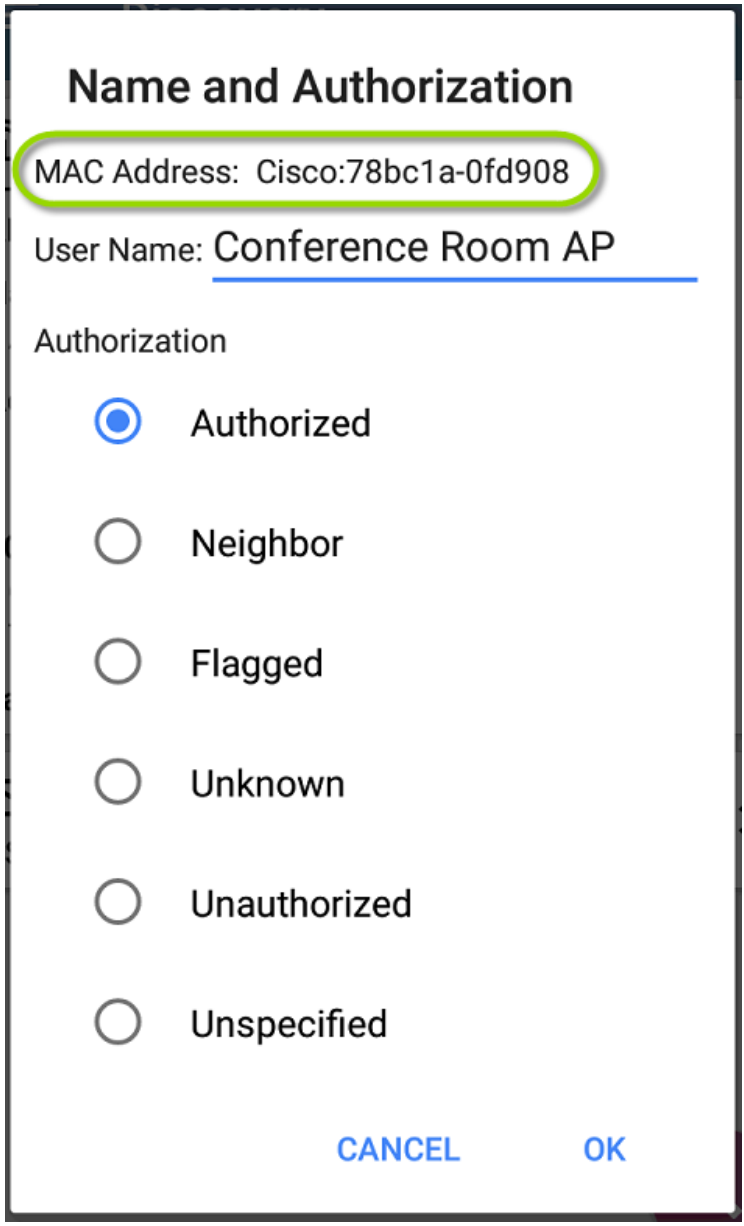
applied to the MAC address or BSSID displayed on the Details screen, as shown in this section.

1. Tap the FAB on a Discovery or Wi-Fi Details screen for a device with a discovered MAC/BSSID.



The example above shows an AP's Details screen in the Discovery app.

2. Select **Name and Authorization** to open the dialog.

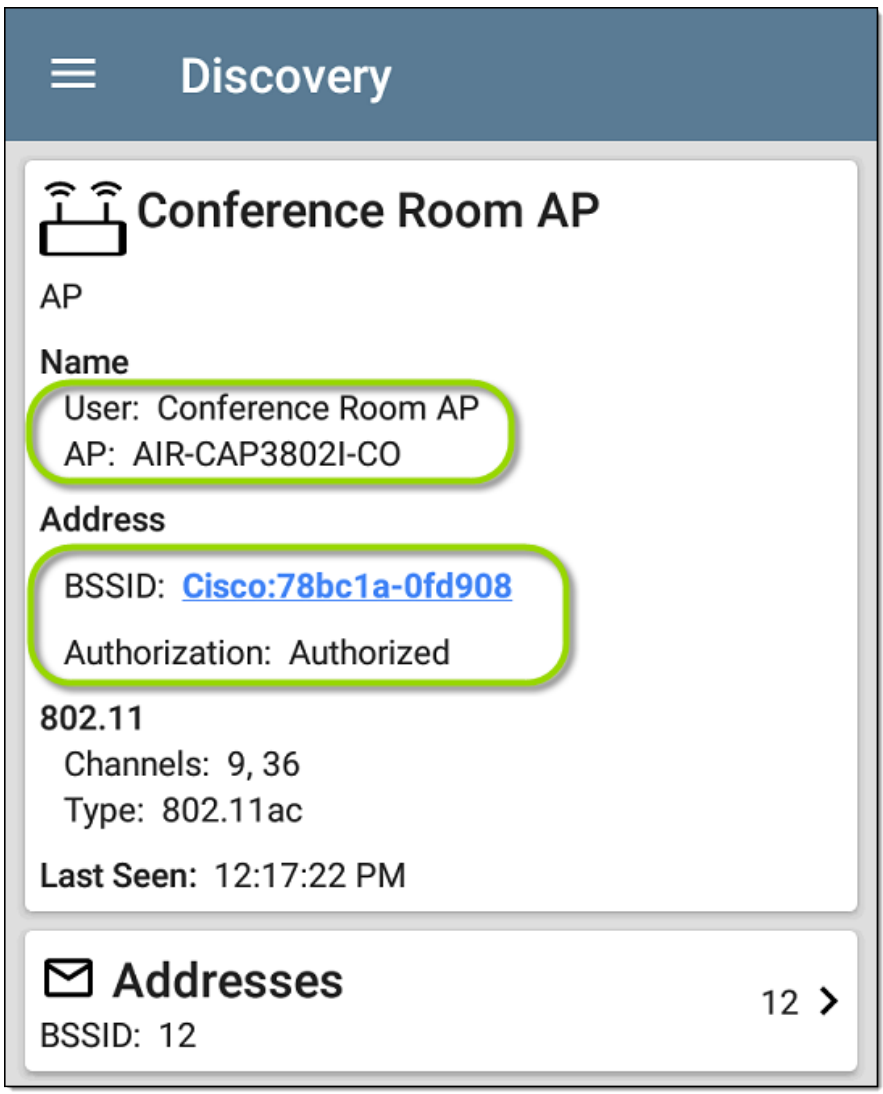


3. In the Name and Authorization dialog, tap the **User Name** field to enter a customized name, if desired. In the image above, the user has entered the name "Conference Room AP."

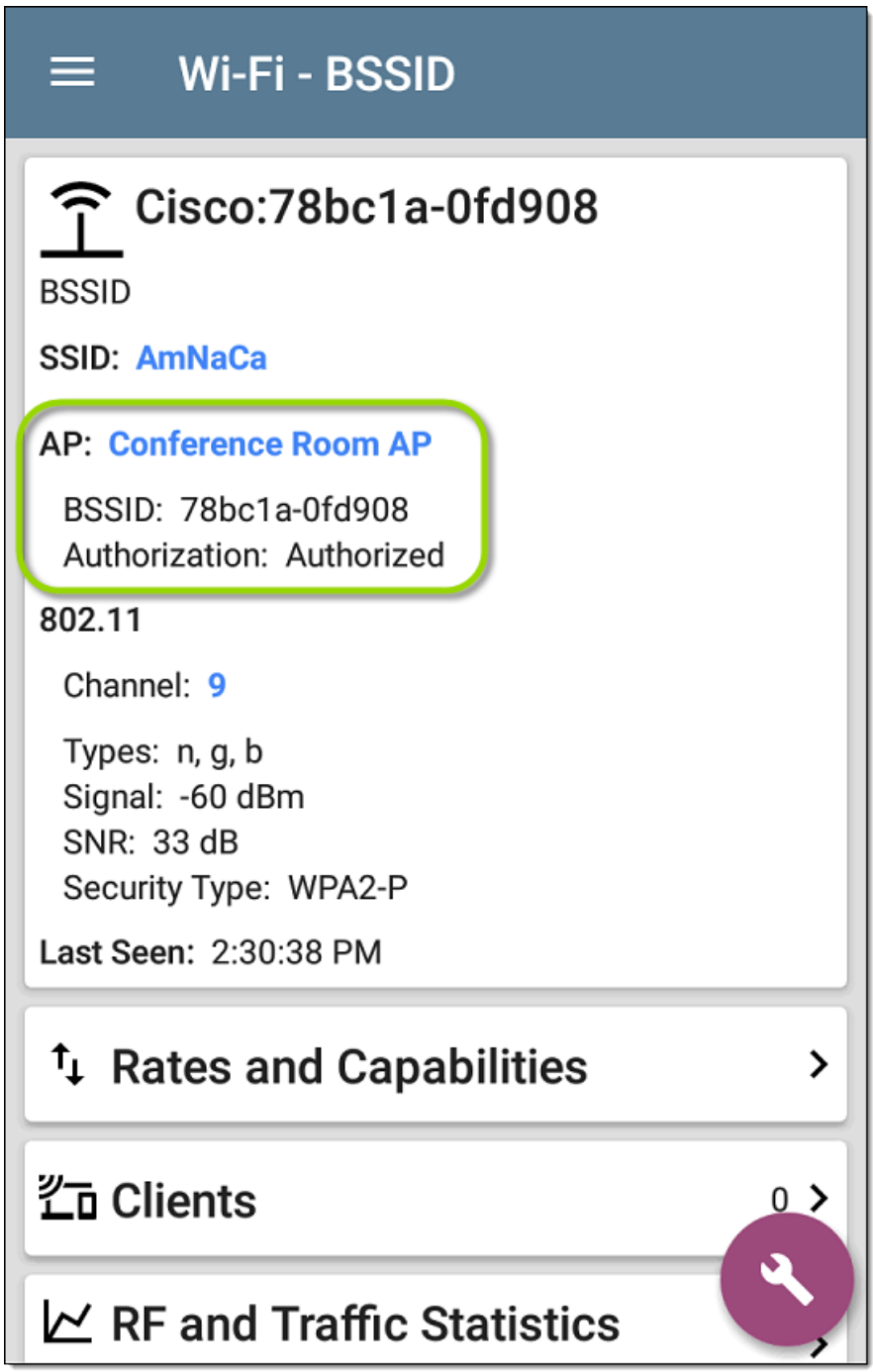
NOTE: It is possible to *either* enter a user name or select an Authorization. You do not have to do both.

4. Select the radio button to assign an **Authorization** status as needed.
5. Tap **OK** to apply.

Once applied, the User Name and Authorization are displayed on the Discovery Details screen.



The user-assigned name for the AP and Authorization for the BSSID also appear on the Wi-Fi BSSID Details screen, as shown below.

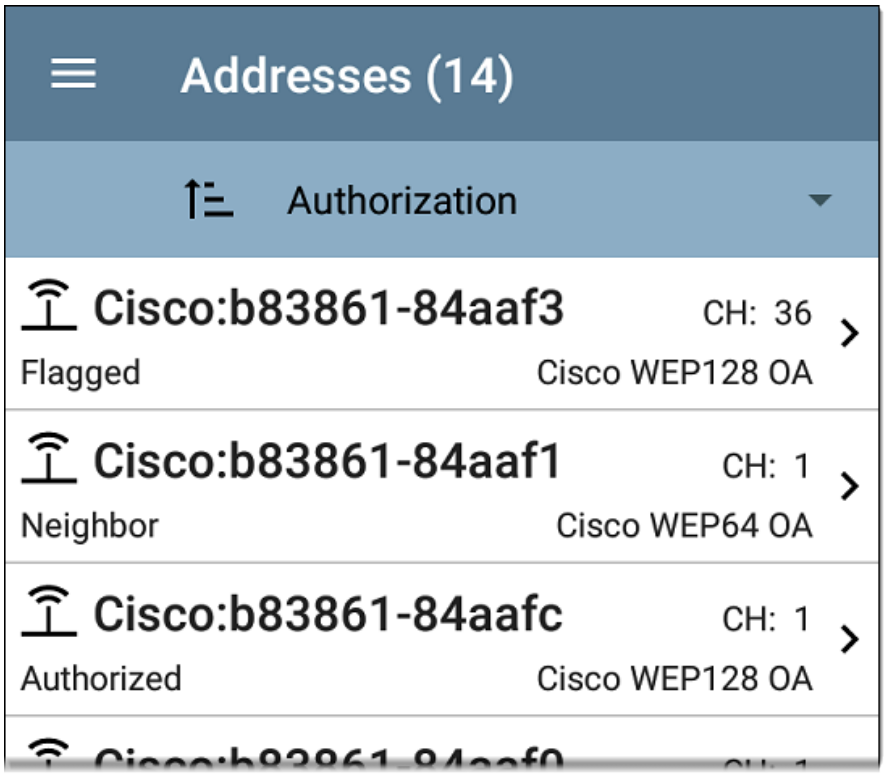


NOTE: If different Authorization statuses are assigned for different BSSIDs or MAC addresses on the same device, the Authorization of highest concern appears on the device's Details screens.

Changing or Clearing a User Name or Authorization

Open the Name and Authorization dialog again *for the same BSSID or MAC address* on a device to reassign or clear the assigned User Name or Authorization. If the Name or Authorization do not update as expected after a few minutes, you may have assigned them to multiple addresses for the same device.

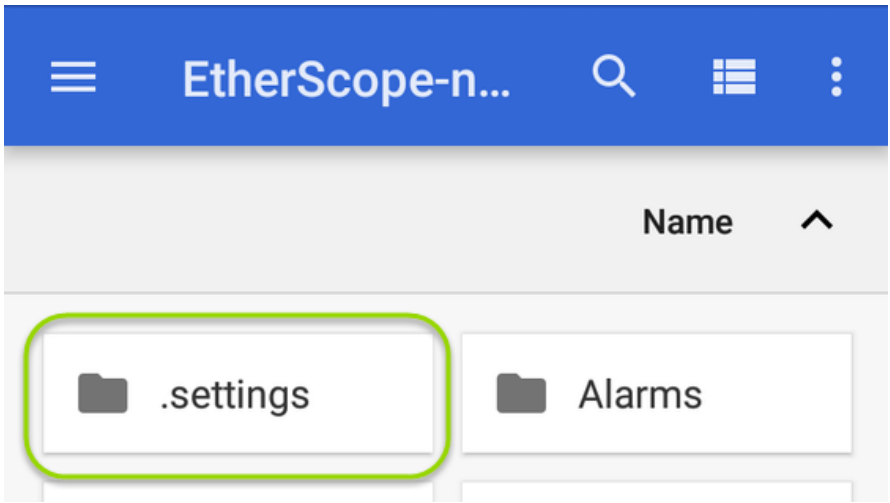
To view all assigned Authorizations for a device, open the Discovery or Wi-Fi Details screen for the device and view the Addresses or BSSIDs screen. Then, sort by Authorization.

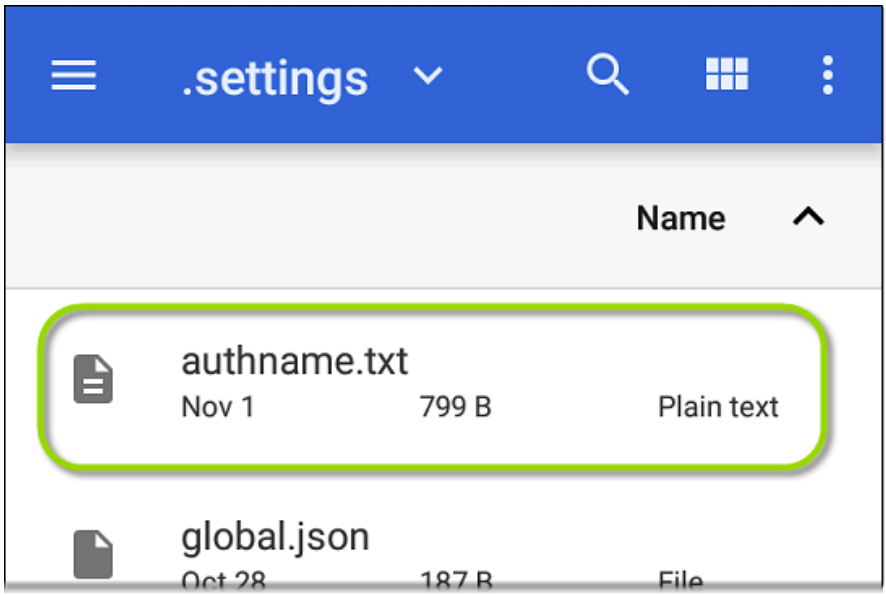


To reset a device's User Name and/or Authorization to the unassigned defaults, open the Name and Authorization dialog, clear the User Name field and leave it blank, and select the **Unspecified** Authorization. Then, tap **OK**.

Revising or Importing authname.txt

Custom Names and Authorizations are stored in the **authname.txt** file in the EtherScope's internal storage **.settings** folder, accessible from the Files app.





NOTE: In the Files app, you may need to tap the action overflow icon ⋮ at the top right and select **Show Internal Storage** to navigate to the **EtherScope-nXG** folder and sub-folders.

If desired, you can manually edit this file on the EtherScope unit, or you can create a new auth-name.txt file on a PC and import it onto your

unit in the same file location. (You can also push authname.txt files from Link-Live to your test unit.)

> NOTE: Your EtherScope nXG can parse ? wildcard characters in the authname.txt file (although * wildcard characters are not allowed).

The default authname.txt file on your unit contains instructions on how to format your Name and Authorization entries:

- Each line defines one MAC/BSSID in the format:
  `MAC/BSSID, [Authorization][, Customized Name]`
- Authorization is case insensitive and can be one of these strings:
  - Authorized
  - Neighbor
  - Flagged
  - Unauthorized
  - Unknown

    - Unspecified (or blank)
- You can substitute a question mark **?** for a MAC digit to match any value for that digit.

A sample authname file could look like this:

```
00c017-330ea3, Authorized, iPerf3-server
bc:e9:2f:41:df:b4, Authorized, HP-Deskjet
b827eb-??????, Unauthorized, Raspberry-PI
7c:10:c9:??:??:??, Neighbor, ASUS-AP
18b169-c84600, Flagged, Who is this?
```

The line `18b169-c84600, Flagged, Who is this?` would result in a Discovery details for the device as follows:

To edit the authname.txt file on the EtherScope, third-party apps, such QuickEdit Text Editor, are available from the NetAllyApp Store ▶ .

For help importing a file, see the Managing Files topic.

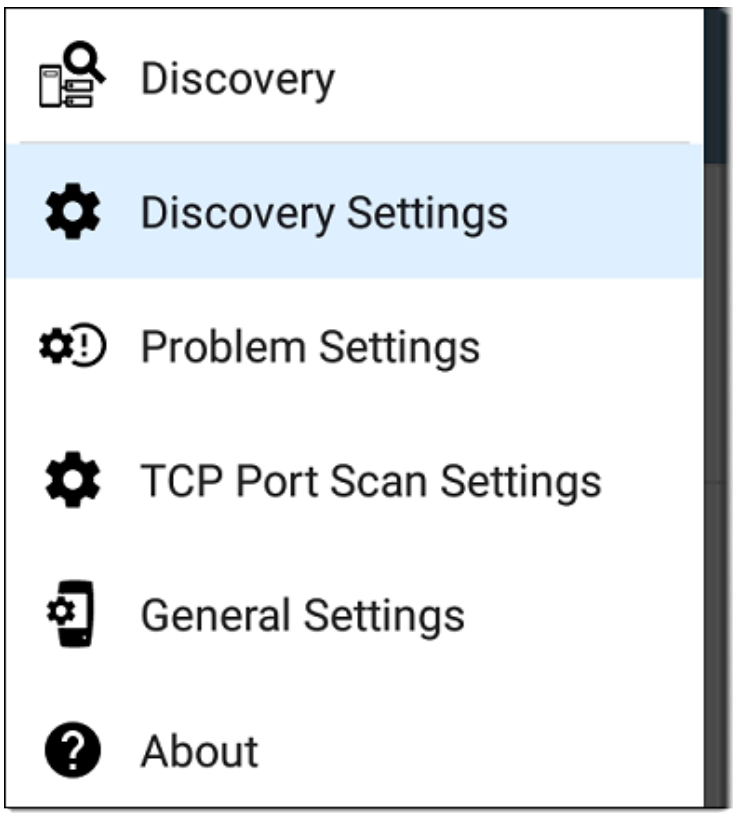
> NOTE: After importing and overriding the authname.txt file, NetAlly recommends

Refreshing Discovery in the Discovery app or restarting your unit.

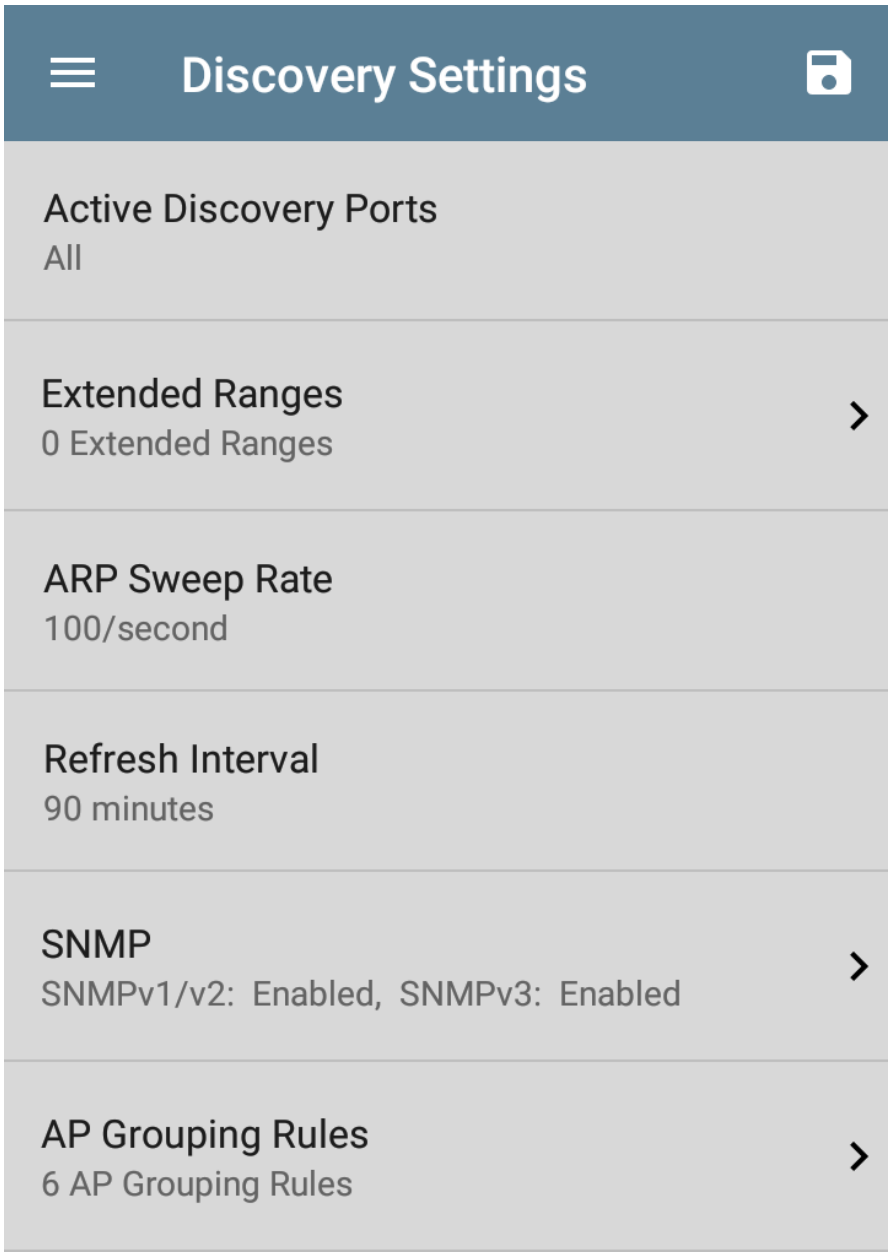
Discovery Settings

Discovery configurations include SNMP settings, Community Strings and the order in which they are used, Credential Sets, Ports, Extended Ranges, and process intervals.

Access the Discovery settings screen by sliding out the left-side navigation drawer or tapping the menu icon, and selecting **Discovery Settings**.



(Tap here to skip to Problem Settings, TCP Port Scan, or back to General Settings.)



To adjust Discovery Settings:

1. On the **Discovery Settings** screen, tap each field described in this topic, as needed, to select or enter your required configuration elements.

2. When you finish configuring, tap the back button  to return to the main Discovery List screen.
3. Then, Refresh Discovery from the action overflow menu  to apply the new configuration.

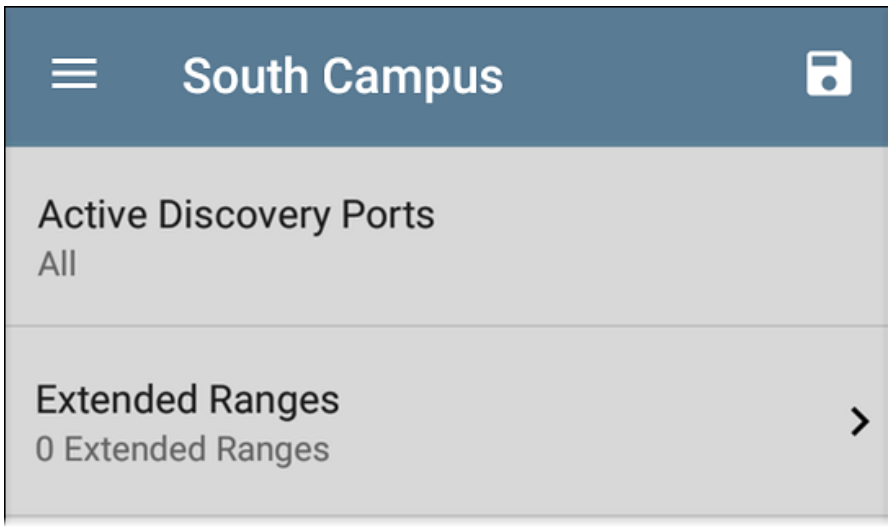
You can load, save, import, and export configured Discovery settings by tapping the save button  on this screen.

- **Load** opens a previously saved Discovery configuration.
- **Save As** saves the current configuration with an existing name or a new custom name.
- **Import**: Import a previously exported settings file.
- **Export Selected** or **Export All**: Create an export file of current settings, and save it to internal or connected external storage.

See Managing Testing App Settings for more instructions.

After you have saved a configuration, the custom name you entered appears in the title of the

Discovery Settings screen. In the image below, a user has saved a custom configuration named "South Campus," which replaces the "Discovery Settings" screen title.



Active Discovery Ports

Tap **Active Discovery Ports** to select which port Discovery uses to gather data. (Discovery uses all of the ports by default. Uncheck them to limit which ports are used.) Discovery runs through the enabled ports only if an active network link is available. See Selecting Ports for explanations of the different ports.

Extended Ranges

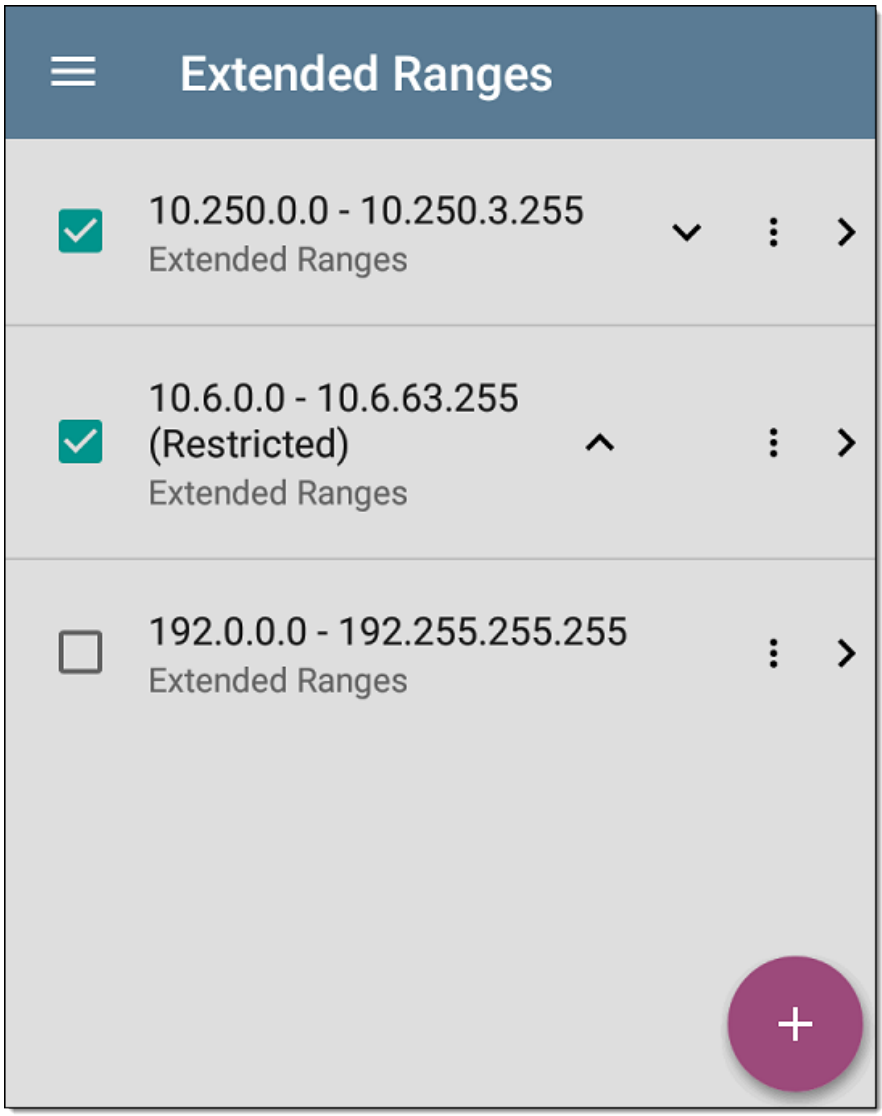
The Extended Ranges screen allows you to enter addresses of non-local subnets on which you want the Discovery process to run. Discovery sweeps all of the enabled Extended Ranges for devices, whether directly connected or off-net. The EtherScope performs Ping sweeps on subnets that are not directly connected and ARP sweeps on connected subnets.

When the SNMP agents are on a subnet that is separate from the hosts (PC's and servers) subnet, additional networks must be configured for discovery:

- The network address of the remote subnet you want to discover, meaning the host (PC and server) network.
- The network address of the switch and router SNMP agents in the remote subnet, e.g. a management subnet.

Configure both SNMP **Credential Sets** and **Extended Ranges** to ensure that the EtherScope always discovers management subnets, regardless of your network port connections.

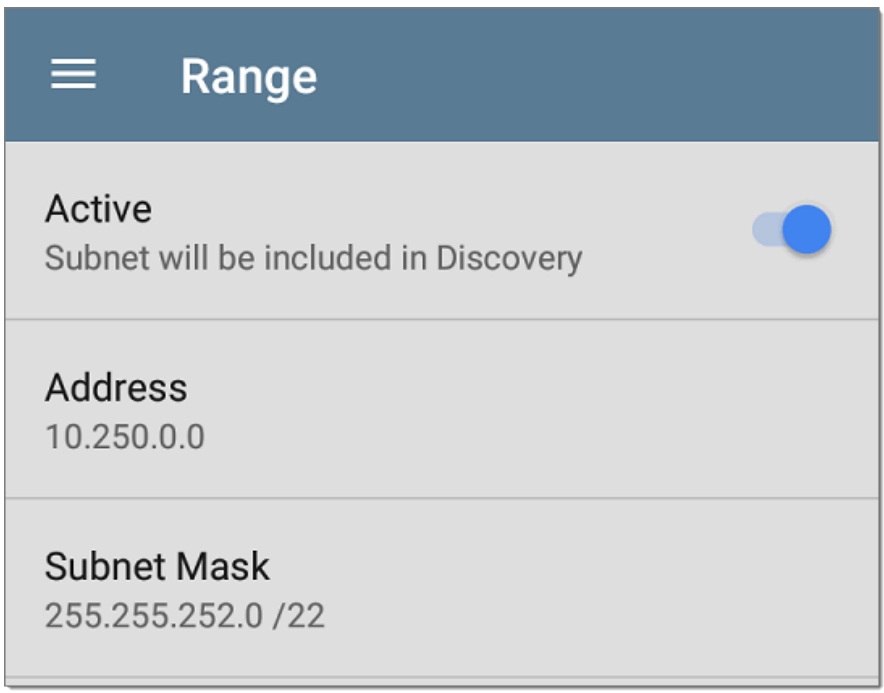
Tap the field to open the Extended Ranges list screen.



- Check or uncheck the boxes to include or exclude an extended range from the current Discovery configuration. Unchecked Extended Ranges do not affect the default Discovery behavior in the current

configuration, but they may be used in other Discovery configurations (like Community Strings and Credentials).

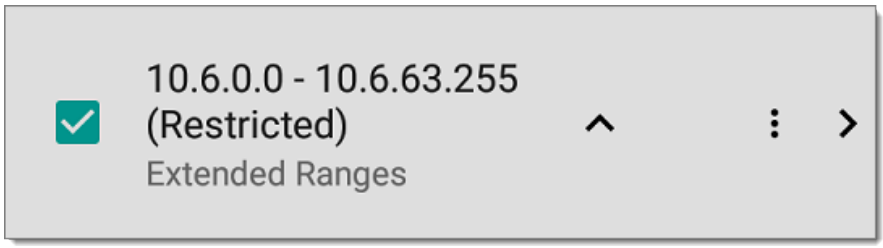
- Tap any Extended Range's row to edit its address and subnet.
- Tap the FAB + to add new extended ranges.



Active vs. Restricted Subnets

For each configured Extended Range, you can tap the toggle button to switch from **Active** to **Restricted**. Discovery is performed on Active Ranges. Setting a Range to **Restricted** disables the discovery process on that network or subnet,

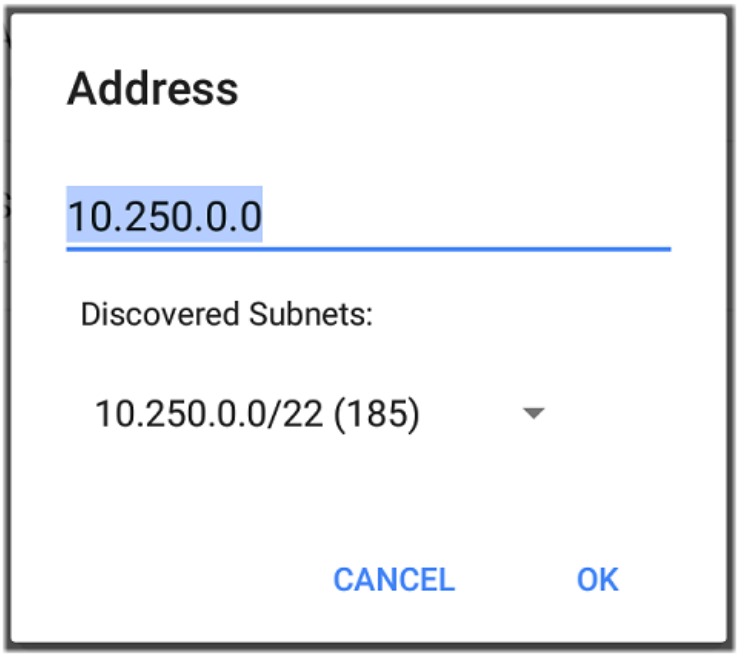
meaning the EtherScope will *not* communicate with devices within the restricted range.



- Restricted Ranges take precedence regardless of the order in which they are listed on the Extended Ranges screen.
- You can Restrict a part of a configured Active Extended Range.
- You can also restrict a single device, whether it is part of an Active Range or not. To enter a single device that you do not want discovered, enter its IP address in the Address field, and set the Subnet Mask field to 255.255.255.255.

Address

Tap the **Address** field to enter or select an IP address range.



Tap the drop-down menu to select a previously Discovered Subnet. The Address field is automatically populated with your selection.

Subnet Mask

Tap this field to select a subnet mask. If you select an already Discovered Subnet, the Subnet Mask is also pre-populated.

ARP Sweep Rate

Tap the ARP Sweep Rate field to select a rate between 5 and 100 ARP requests per second.

This setting can prevent the EtherScope from shutting down ports that sense too many ARPs being sent.

Refresh Interval

This setting controls the time between runs of the Discovery process. By default, Discovery runs every 90 minutes. Tap the **Refresh Interval** field to select a different interval, up to 8 hours.

The **Manual** option turns off regular automatic Discovery, and the process refreshes only if you select **Refresh Discovery** from the main Discovery list screen.

SNMP Configuration

The MIB (Management Information Base) of SNMP managed devices contains information such as device configuration, interface configuration and statistics, SNMP tables (like host resource and route tables) and VLAN details. Through the Discovery process, the EtherScope interrogates MIBs to determine the device type, ports, connected subnets, and other data.

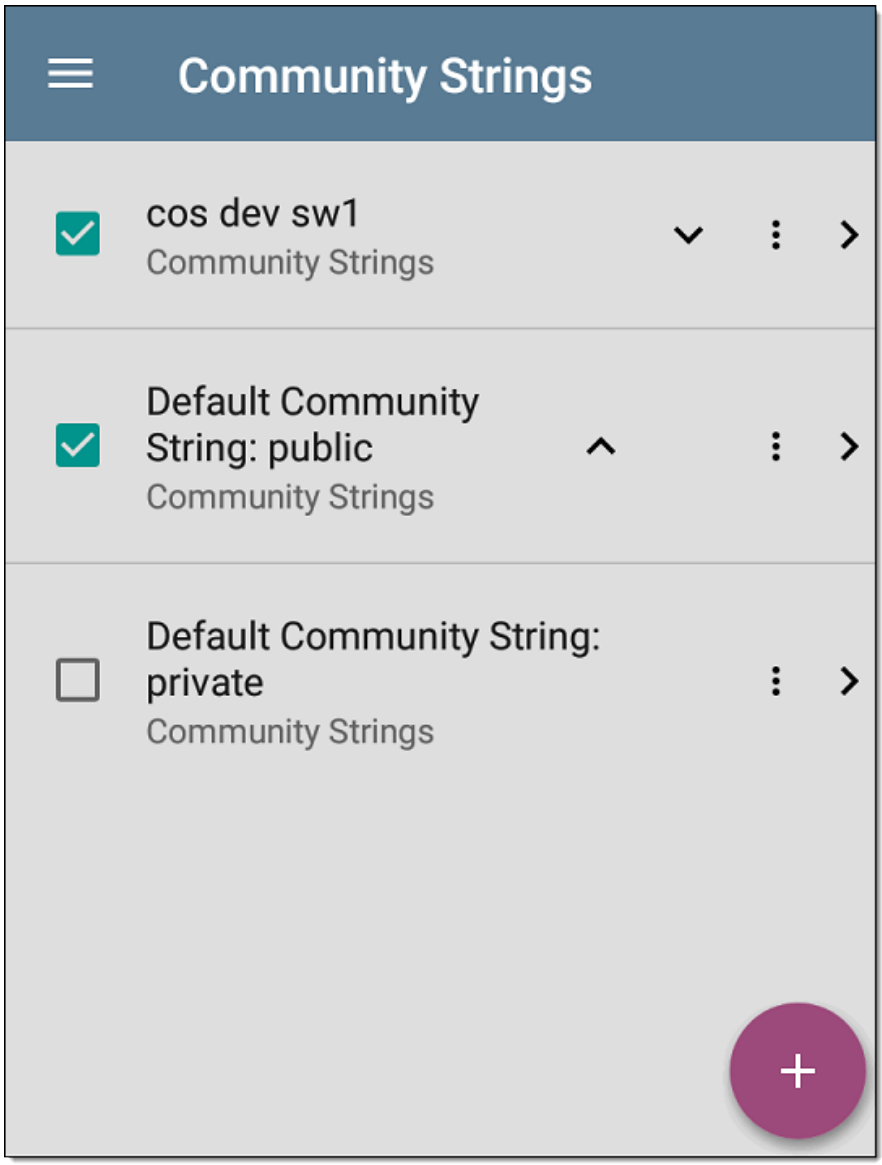
SNMP credentials are required to communicate with the SNMP agents on your interconnect devices, such as switches and routers. The Discovery Settings allow you to enter the SNMP community strings and credential sets the EtherScope uses to communicate with those devices.

SNMPv1/v2

Tap the toggle button to enable or disable SNMPv1 and v2 queries. This setting is enabled by default and uses the Community Strings configured in the next setting.

Community Strings

Tap this field to open the Community Strings list screen and add, edit, or remove community strings.



The EtherScope uses the checked strings in the order shown on this screen. If it does not receive a response from the queried device using one string, it sends the next string.

> NOTE: This screen and others in the Discovery settings operate much like the AutoTest Profile Group screen.

On the Community Strings screen, you can perform these actions:

- Check or uncheck the boxes to include or exclude a string from use in the current Discovery configuration.
- Tap the up and down arrows  to change the order in which the EtherScope uses the strings to query a device.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a Community String.
  CAUTION: Deleting a string removes it from all saved Discovery configurations. To remove a string from the current Discovery configuration only, simply uncheck it.
- Tap the FAB  to add new Community Strings.
- Tap any Community String's row to edit the string and its description.

  TIP: To minimize discovery time, uncheck or delete all unused community strings, as every failed query extends the discovery time. You can also arrange the community strings in the order they are used most.

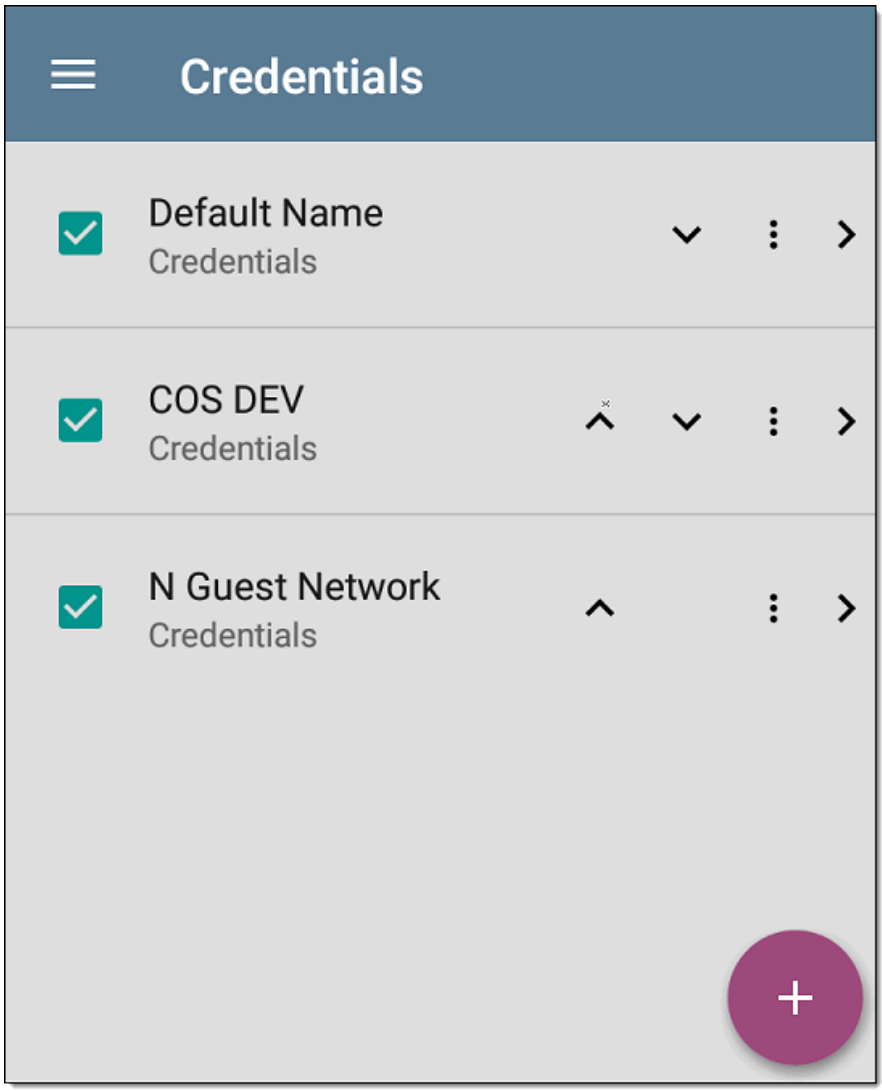
SNMPv3

Tap the toggle button to enable or disable SNMPv3 queries. This setting is enabled by default and uses the Credentials configured in the next setting.

> NOTE: If this setting is enabled, but no SNMPv3 credentials are configured, the EtherScope discovers the engine IDs of all SNMPv3 agents. This is a good way to discover if a device supports SNMPv3.

Credentials

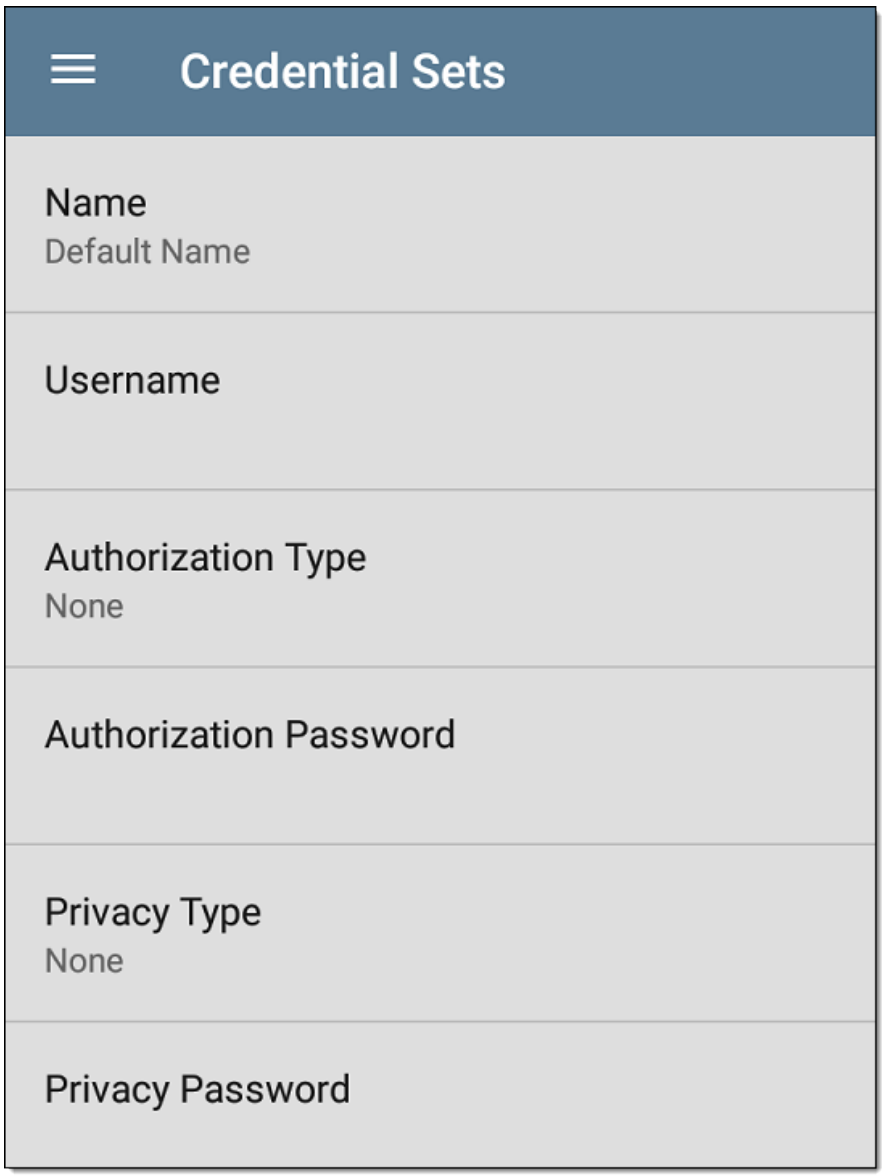
Tap this field to open the Credentials list screen.



This screen interface works like the Community Strings screen above. EtherScope uses the Credentials in the order shown.

- Check or uncheck the boxes to include or exclude a set of Credentials from use in the current Discovery configuration.
- Tap a row to edit its credentials.

- Tap the FAB + to add new credentials.



On the Credentials Sets screen, tap each field to select or enter the credentials required.

Name

Tap the **Name** field to enter a custom name for the Credential Set.

Username

Tap to enter the SNMPv3 username.

Authorization Type and Password

EtherScope Discovery supports two SNMPv3 Authorization types: HMAC-SHA and HMAC-MD5. If Authorization is required, enter the appropriate password.

Privacy Type and Password

EtherScope Discovery supports four Privacy Types: CBC-DES, AES-128, AES-192, AND AES-256. If needed, enter the appropriate Privacy Password.

SNMP Query Delay

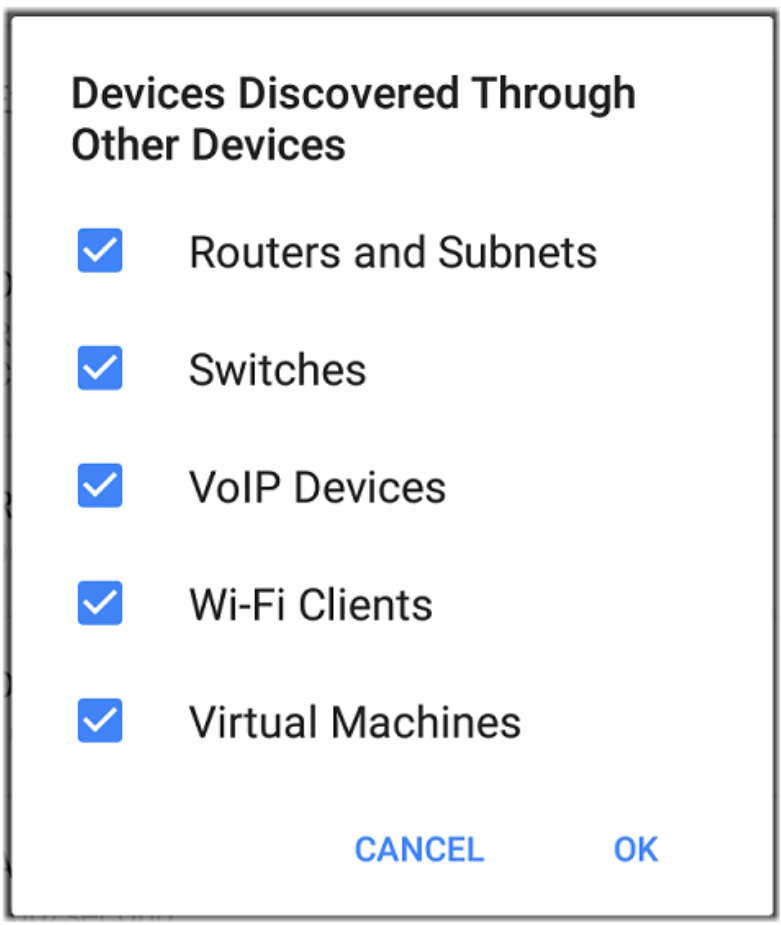
This function controls how long your EtherScope waits between SNMP queries to key tables that can cause CPU spikes in the SNMP agents, including the ARP cache, IP address table, routing tables, and FDB tables.

The default SNMP Query delay is No Delay. When querying the key large tables, the EtherScope asks for more data as soon as a response has

been received. You can select a 1 or 5 second delay if needed.

Devices Discovered Through Other Devices

By default, EtherScope discovers devices from SNMP tables of other devices. If you do not want Discovery to automatically find devices from SNMP tables of the device types listed here, you can uncheck their boxes.



Routers and Subnets

When the Routers and Subnets checkbox is enabled, any discovered routers are included in discovery results. In addition, if Discovery has SNMP access to a discovered router, its routing tables are read, and the next hop routers are added to the Discovery list. If any local subnets are available in the routing tables, these are also added to the Subnets list. This process continues until all the available SNMP credentials are tried for the added routers.

> NOTES: Discovery does not sweep every discovered subnet; discovered subnets are only added to the subnets list. To perform discovery in a specific subnet, see **Extended Ranges** above.
>
> If another site has routers you want to discover using this process but there isn't a local next hop link from this site, you can add one of the routers of that site to discovery. The process then runs from that router and finds the routers on that site as well. Add the subnet of the router or just the

router's IP address with a mask of /32 to Extended Ranges.

Switches

When the Switches checkbox is enabled, discovery adds any switches that it finds in SNMP neighbor tables of other devices to the Discovery list.

For example, when EtherScope is reading the CDP and LLDP caches of one switch, it contains other switches. If this option is enabled, the EtherScope adds those other switches, even if they are not in discovery ranges.

> NOTE: To Discover switches at another site, add one of the switches of that site to Discovery Extended Ranges.

VoIP Devices

When the VoIP Devices checkbox is enabled, discovery adds any VoIP devices that it finds in SNMP tables of other devices regardless of the subnet. These are usually found in the LLDP-MED tables of the switches. Enabling the Switches option provides the best chance of finding all your VoIP devices.

Wi-Fi Clients

When the Wi-Fi Clients checkbox is enabled, discovery adds any wireless clients it finds in SNMP tables of APs and Wireless LAN Controllers. Enabling this option along with Switches provides best chance of finding all Wi-Fi clients.

> NOTE: Enabling Wi-Fi Clients here may cause Wi-Fi devices to show in Discovery that do not appear in the Wi-Fi analysis app because Wi-Fi analysis only shows what it detects on wirelessly transmitted packets.

Virtual Machines

When the Virtual Machines checkbox is enabled, discovery adds any virtual machines that it finds in SNMP tables of other devices. These are usually found in the ESX host > SNMP tables. Adding the subnets of your ESX hosts to Extended Ranges helps with finding your virtual machines.

Device Health Interval

Discovery automatically runs a set of network health tests to search for network Problems,

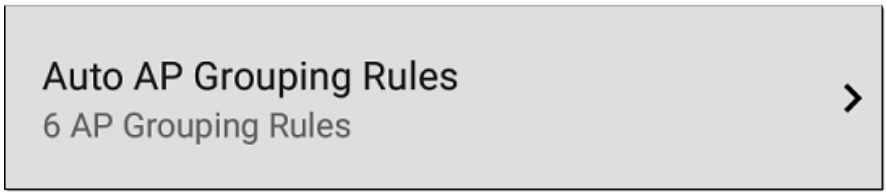
such as high utilization, discards, or errors on all discovered interfaces and device resources.

The selected time Refresh Interval is the minimum time between each run of the Device Health tests. Tap the field to disable Device Health testing or to change the interval from the default of 10 minutes to 30 or 60 minutes.

Disabling the Device Health testing affects the types of Problems that Discovery can detect.

See also Problem Settings.

Auto AP Grouping Rules

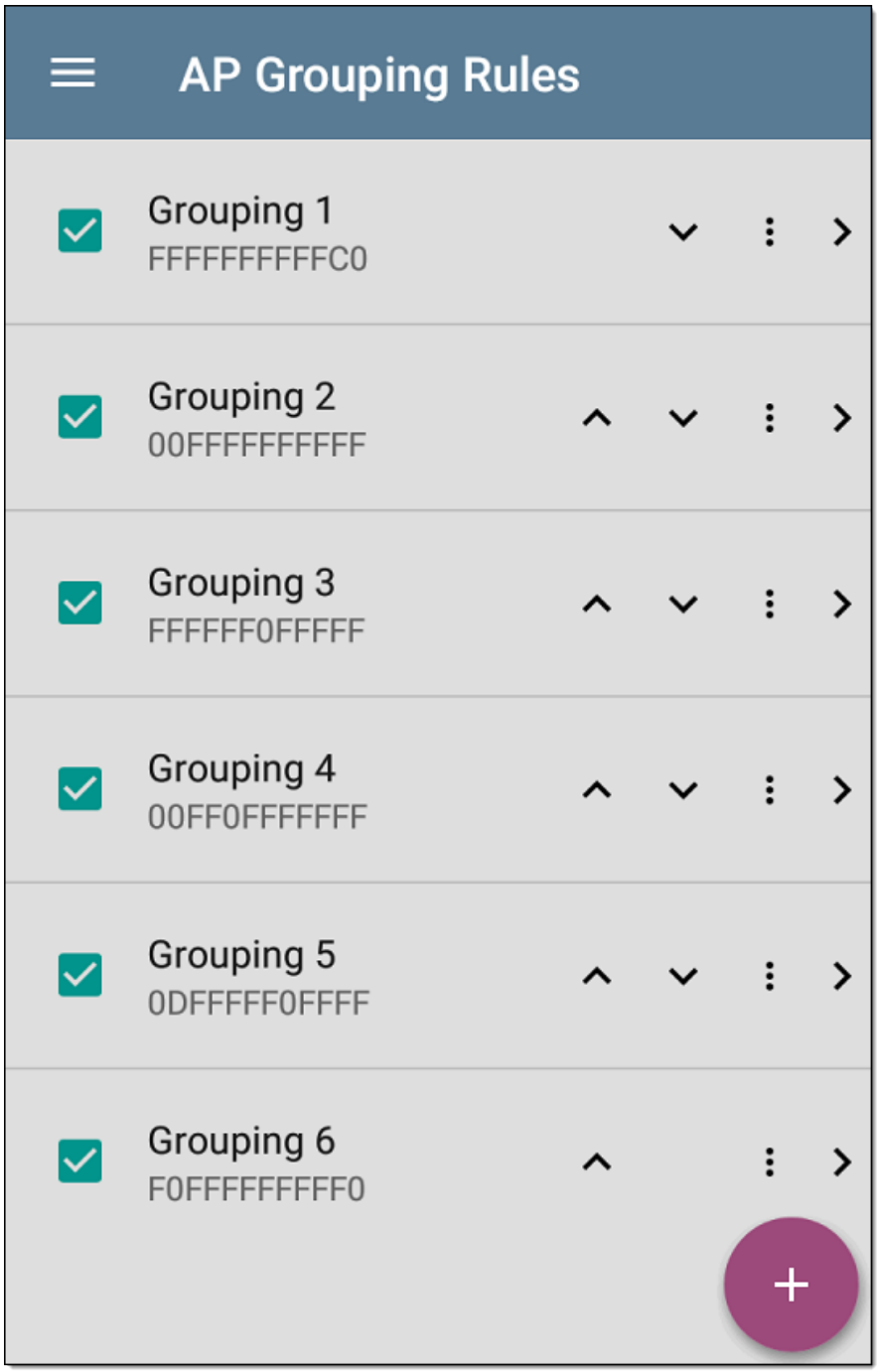


This feature allows you to adjust the AP Grouping Rules that control how the EtherScope groups BSSIDs with their Access Points, such that they are grouped appropriately for your AP types and environment.

For example, if BSSIDs from different APs are being grouped together inaccurately, you can disable the rule that is causing the grouping. If your AP manufacturer uses a BSSID variation

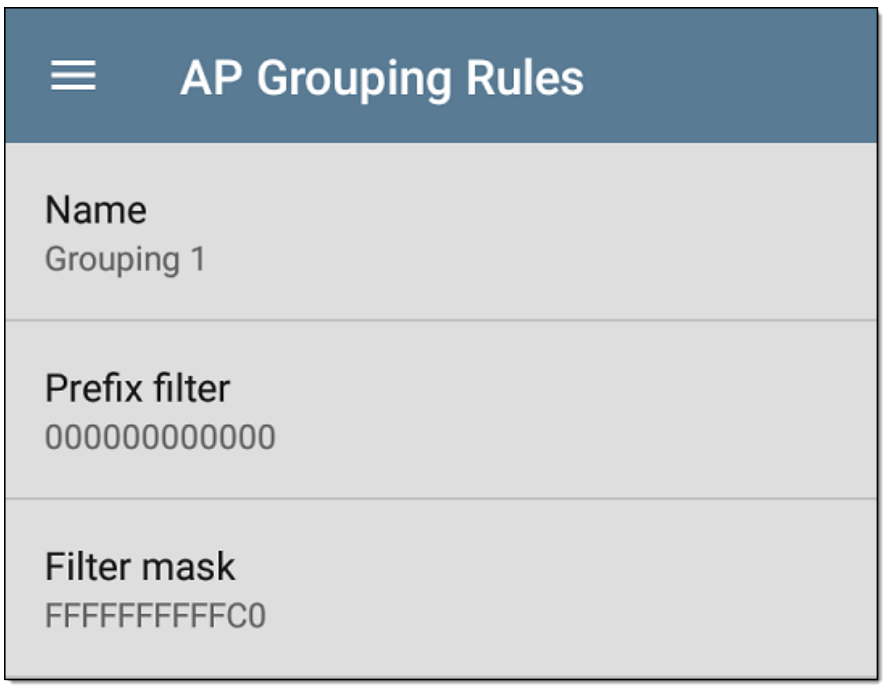
scheme that is not covered by one of the six default rules, you can add a new rule.

Tap the setting to open the AP Grouping Rules list screen. The image below shows the six default AP Grouping Rules on the EtherScope. The **Prefix filters** in all of the default grouping rules are set to 000000-000000.



As with other settings list screens on the EtherScope, you can enable or disable, add, delete, and edit the grouping rules from this screen.

- Check or uncheck the boxes to include or exclude a rule from use in the current Discovery configuration.
- Tap the action overflow icon ⋮ to **Duplicate** or **Delete** a rule.
  CAUTION: When you delete a rule, you delete it from all saved Discovery configurations. To remove a rule from those used by the current Discovery configuration, simply uncheck it.
- Tap the FAB + to add a new rule.
- Tap any rule's row to edit it.



Name

If desired, enter a custom name for a default or new rule. If you intend to use a Prefix filter, a best practice would be to name the rule with the AP manufacturer's name.

Prefix filter

Use the **Prefix filter** to create a rule for a specific AP manufacturer's BSSID scheme, meaning a rule for just one AP manufacturer prefix. The default rules all contain a default Prefix filter of 000000-000000.

If a Prefix filter is non-zero, its second and third bytes are compared to discovered BSSIDs before the **Filter mask** (described below) is applied. These two bytes must match exactly, or the two BSSIDs are not grouped together. This behavior allows you to specify a fairly open Filter mask, because the mask applies only to one manufacturer.

For example, you could have Cisco APs whose BSSIDs all start with b83861. By specifying a Prefix filter of 003861-000000, you limit the grouping rule to just those APs.

Filter mask

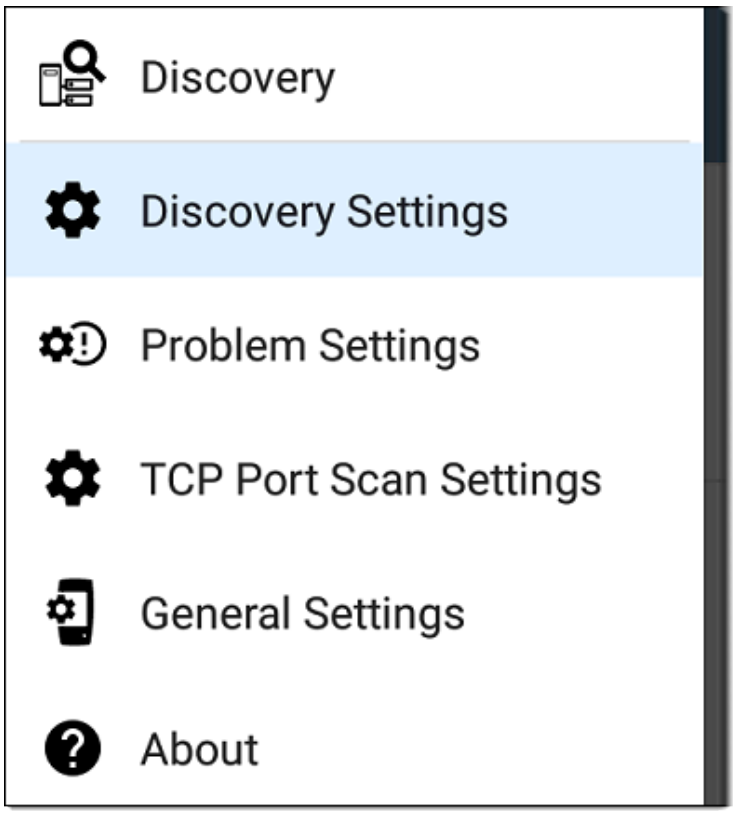
The Filter mask specifies what parts of the BSSIDs are compared when determining AP groupings.

For example, default **Grouping Rule 1** has a Filter mask of FFFFFF-FFFFC0, so any BSSIDs that vary only by the lower six bits are grouped together.

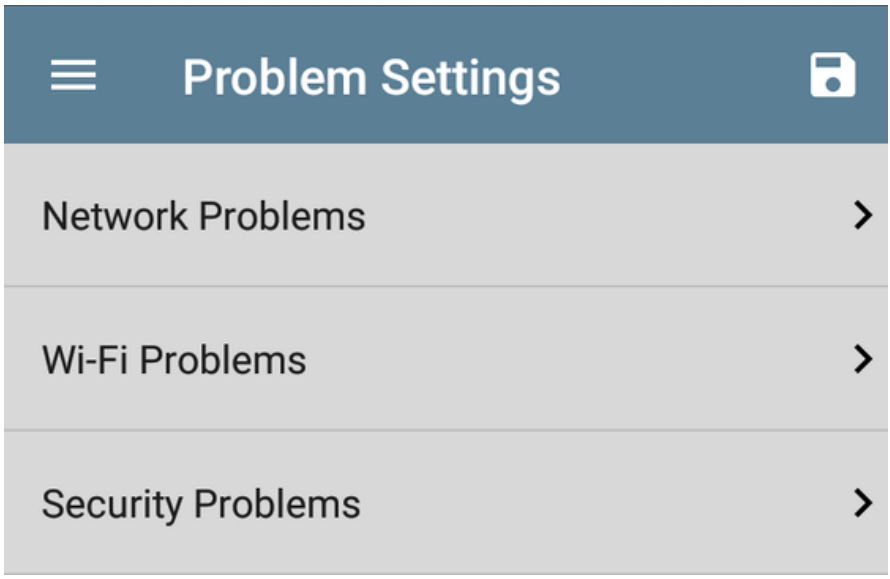
Problem Settings

The Problem settings determine which issues are detected and displayed by *both* the Discovery and Wi-Fi Analysis apps as well as the thresholds for enabled problems, such as Packet Discards and Utilization.

Access the Problem Settings screen by sliding out the left-side navigation drawer or tapping the menu icon in the Discovery app, and selecting **Problem Settings**.



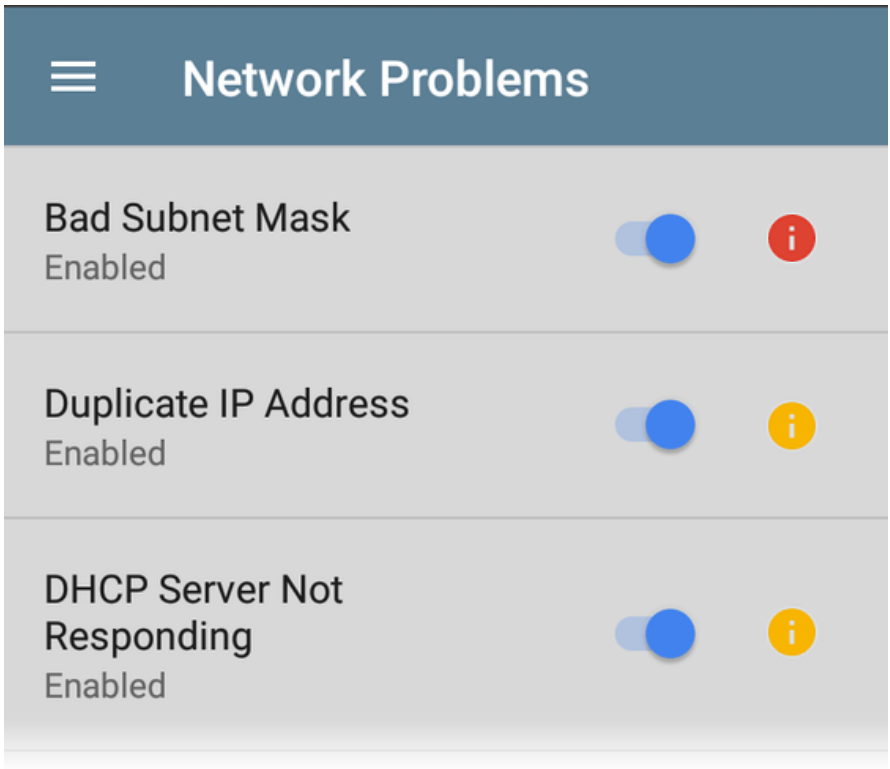
(Tap here to go to Discovery Settings or back to General Settings.)



Problems are categorized as Network, Wi-Fi, or Security.
NOTE: The Wi-Fi Problems configured here also control the Problems detected and displayed in the Wi-Fi Analysis app.

As with Discovery Settings, you can save, load, import, and export configured Problem Settings by tapping the save button on this screen. See Managing Testing App Settings for more instructions.

Tap the row for each to enable or disable the problem types and set thresholds where applicable.



All Problem types are enabled by default. Tap the toggle button to the right to disable each one.

Tap the red  or yellow  information icons to the right of each Problem to read a detailed description and recommended actions. **Red** icons indicate Failure conditions and **yellow** indicate Warning conditions.

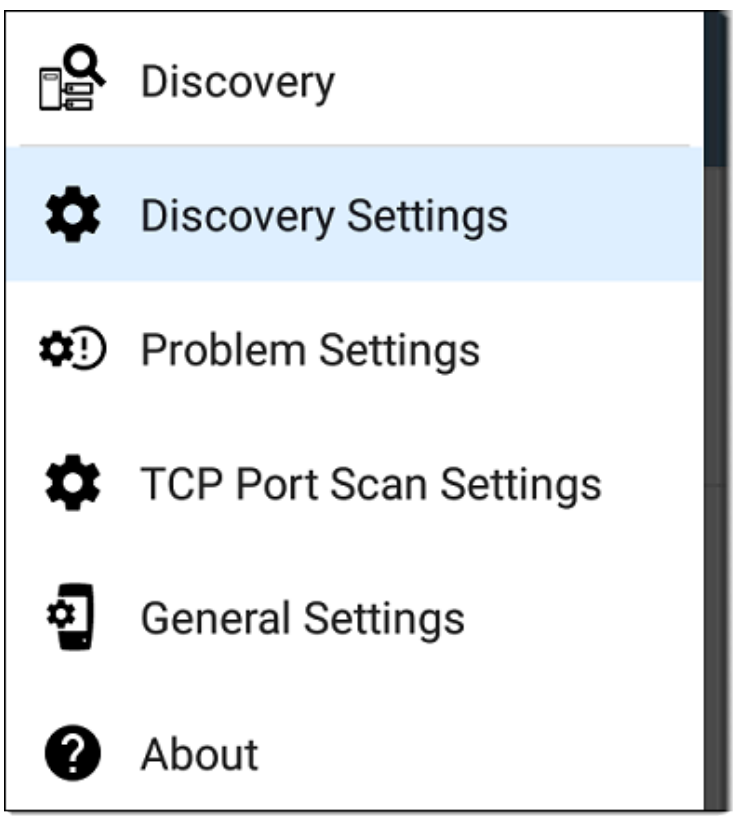
When you finish configuring, tap the back button  to return to the main Discovery screen.

Back to Title and Contents

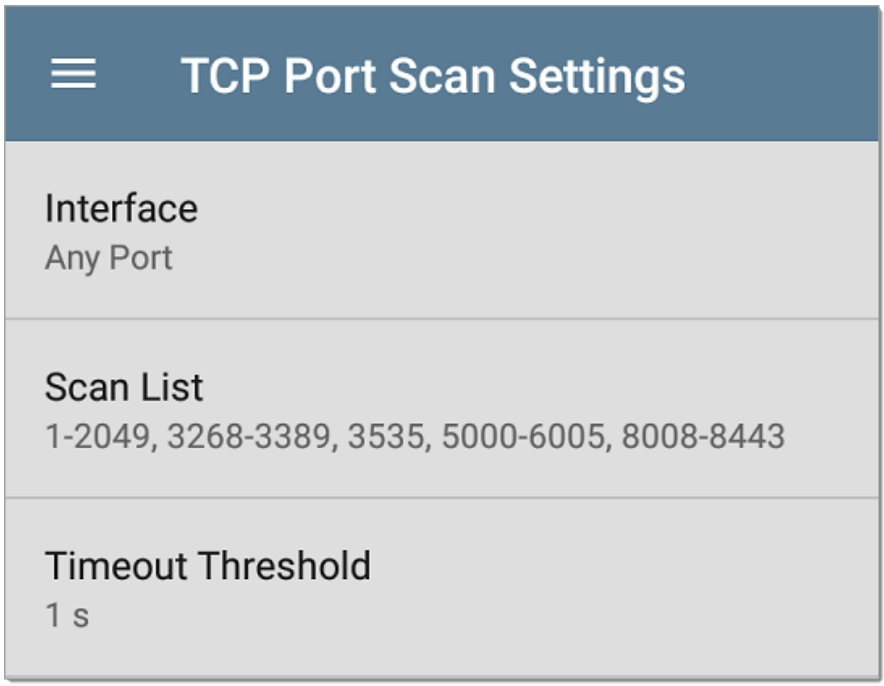
TCP Port Scan Settings

The TCP Port Scan feature checks for open ports on the current device. (Run the scan by tapping the FAB on a Discovery Details screen and then tapping **TCP Port Scan**.) The EtherScope scans many ports simultaneously and reports the open port's numbers.

Access the TCP Port Scan Settings by sliding out the left-side navigation drawer or by tapping the navigation menu icon, and then selecting **TCP Port Scan Settings**.



This displays the TCP Port Scan Settings screen.



Interface: Tap the field to select the EtherScope port from which the port scan runs. (See Selecting Ports for explanations of the different ports.)

Scan List: Tap this field to edit the list of port numbers that get tested during the port scan. You can enter port numbers or ranges, separated by commas.

Timeout Threshold: Tap this field to select a value for how long the EtherScope waits for a response from each port or to enter a custom value. The scan ends after all the ports in the Scan List have had this amount of time to

respond, and then the results screen lists the ports that responded within the threshold.

See also the TCP Port Scan results card and screen.

Wi-Fi Analysis App

The Wi-Fi Analysis app scans the wireless channels in your environment to discover and gather data about the devices and traffic on your Wi-Fi networks. Wi-Fi discovery begins when you power on the EtherScope, and measurements update with each channel scan cycle.

The EtherScope nXG supports 802.11a/b/g/n/ac/ax technologies. EtherScope can also detect and indicate the 802.11ax media type (known as Wi-Fi 6) being used on APs and Clients, as reported in the wireless management frames.

The Wi-Fi app features separate screens that list and display characteristics of the different devices and elements of your wireless environment. Tap a link below to go directly to the description of the screen listed:

- Channels Map
- Channels
- SSIDs
- APs
- BSSIDs
- Clients
- Bluetooth
- Interferers

Wi-Fi Analysis and Discovery

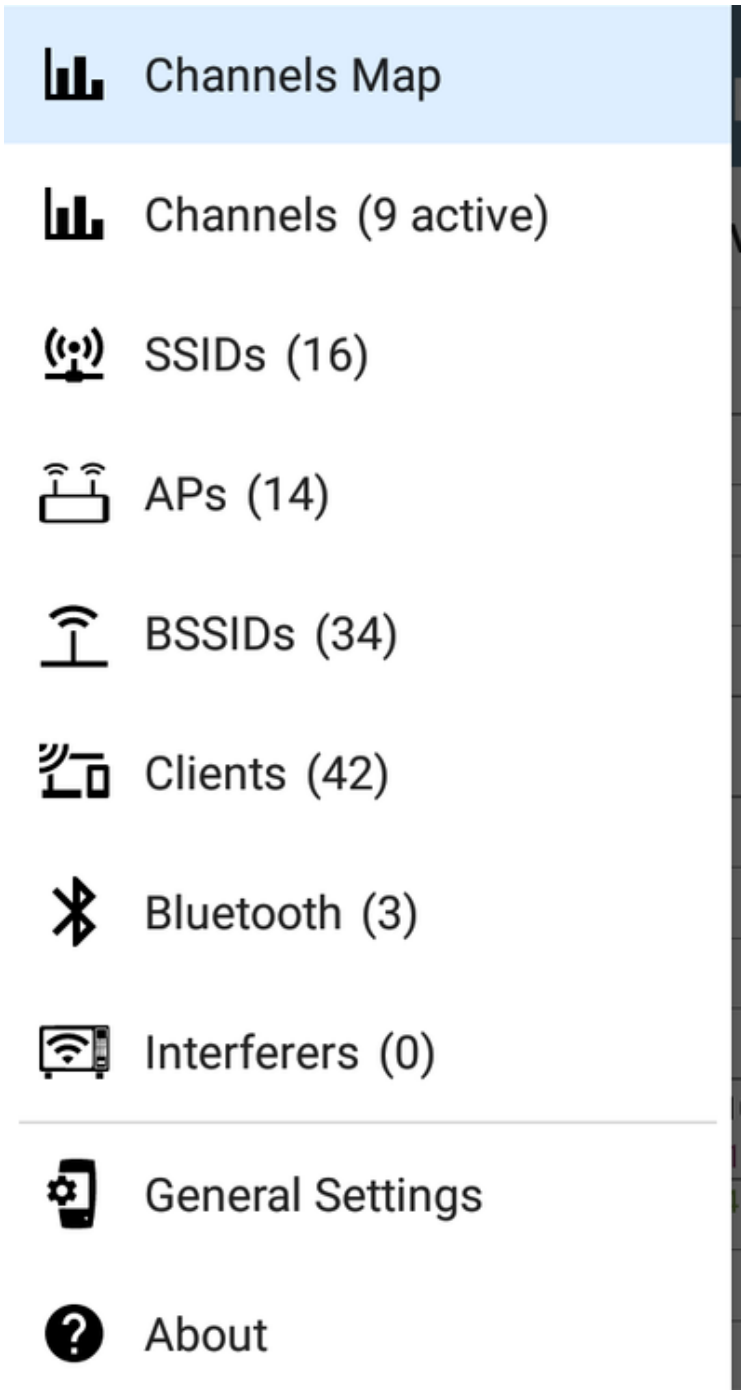
Wi-Fi Analysis uses the Wi-Fi Test Port to scan the channels and acquire information about your wireless networks. If the Wi-Fi Test Port is linked (for instance after running a Wi-Fi AutoTest Profile), the port unlinks and resumes scanning when you open the Wi-Fi Analysis app.

Wi-Fi Analysis is enhanced with data gathered by Discovery. When the EtherScope is linked to a network through any of the other three ports (Wi-Fi Management, Wired Test, or Wired Management), Discovery can obtain information from network layers 3 and above, such as IP addresses, Protocols, and SNMP data.

Therefore, the information Wi-Fi Analysis is able to display also depends on configured Discovery Settings, such as SNMP Community Strings and Credentials, Active Discovery Ports, Extended Ranges, and Device Health testing.

Wi-Fi App List Screens

To switch between the different Wi-Fi app screens, tap the menu icon (or swipe right) to open the left-side navigation drawer.



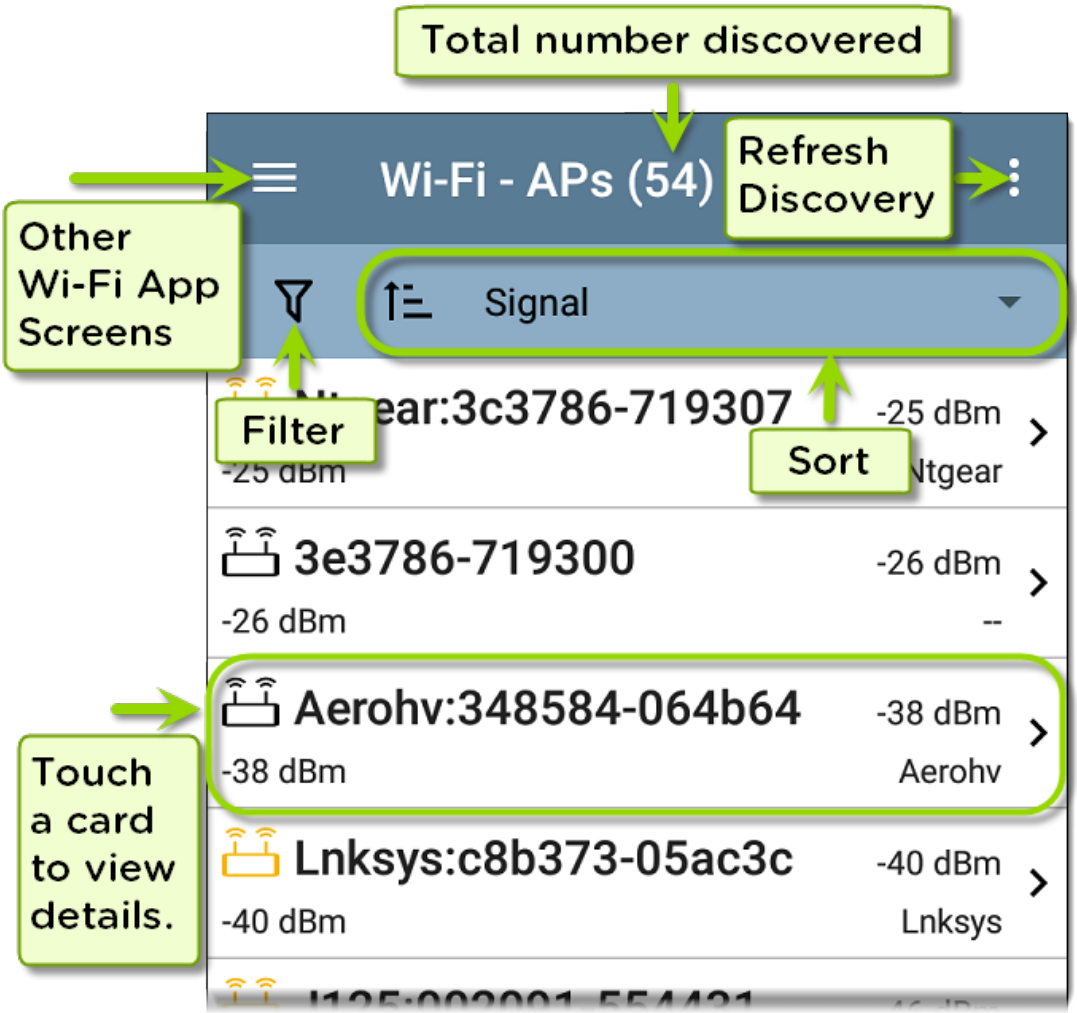
The Wi-Fi app's navigation drawer displays a real-time count (in parentheses) of each wireless component EtherScope has detected. Tap an option to open the corresponding screen.

> NOTE: The **General Settings** for Wi-Fi control which channels and bands are scanned to populate the Wi-Fi screens. See the General Settings topic for more explanation.

Wi-Fi App List Screens

The Wi-Fi app screens, except for Channels Map, display a list of discovered items, much like a Discovery App list screen. You can Filter and Sort the list by different characteristics and tap a network component's card to view its details.

The example image below shows the APs screen with common Wi-Fi app functions:

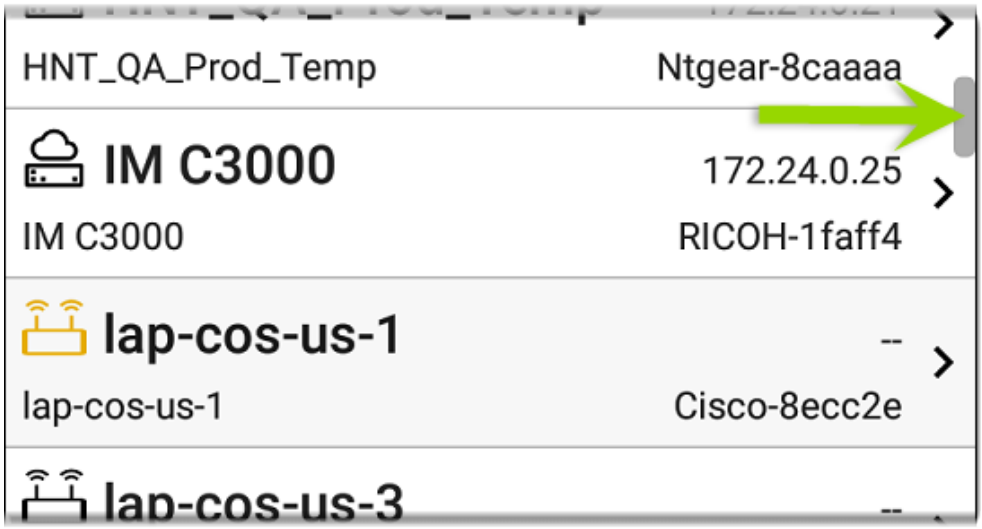


Like in AutoTest and other EtherScope screens, the icons in Wi-Fi analysis change color to indicate a **Warning** or **Failure** condition. The app also displays icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous Problem has been resolved.

> NOTE: To adjust the Problem Settings, access them from the Discovery app's left-side navigation drawer. Problem Settings in the

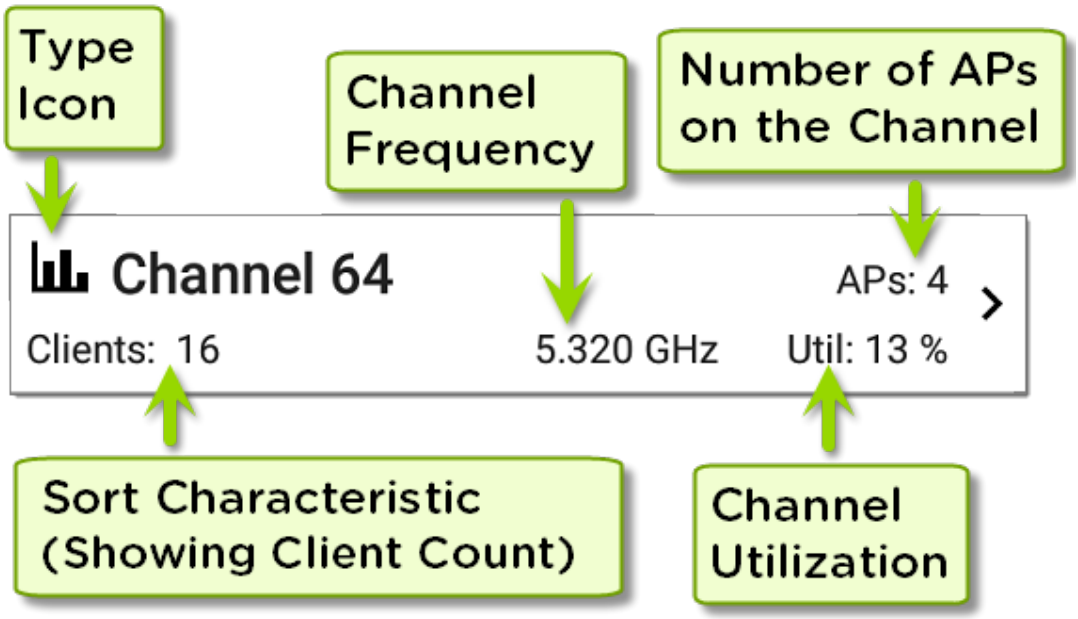
Discovery app are also applied to the Wi-Fi Analysis app.

The Wi-Fi list screens, and other app screens with long lists, support fast scrolling. Touch and drag the scrollbar handle to the right of the list to scroll quickly up and down.



Wi-Fi List Cards

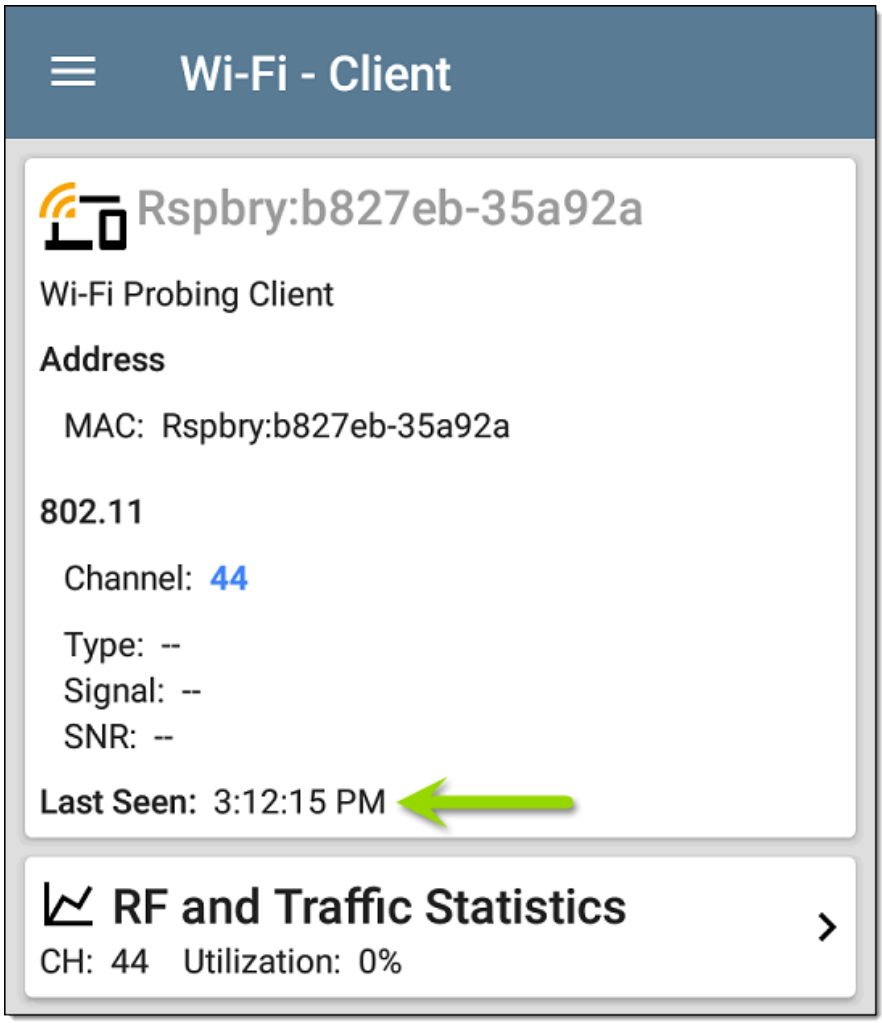
The information displayed on each card varies depending on the selected Sort characteristic and the data the EtherScope was able to discover. For example, a card on the Channels list screen displays the channel number, frequency, connected APs, and utilization.



The lower left field displays the characteristic by which the list screen is currently sorted. In the image above, the Channels list is sorted by Client Count.

If a device is grayed out, the EtherScope no longer detects a signal from it. The client card shown below indicates that the "Rspbry" client cannot be detected currently.

The time the device was Last Seen, meaning last detected by the EtherScope, is shown on the device's Details screen.

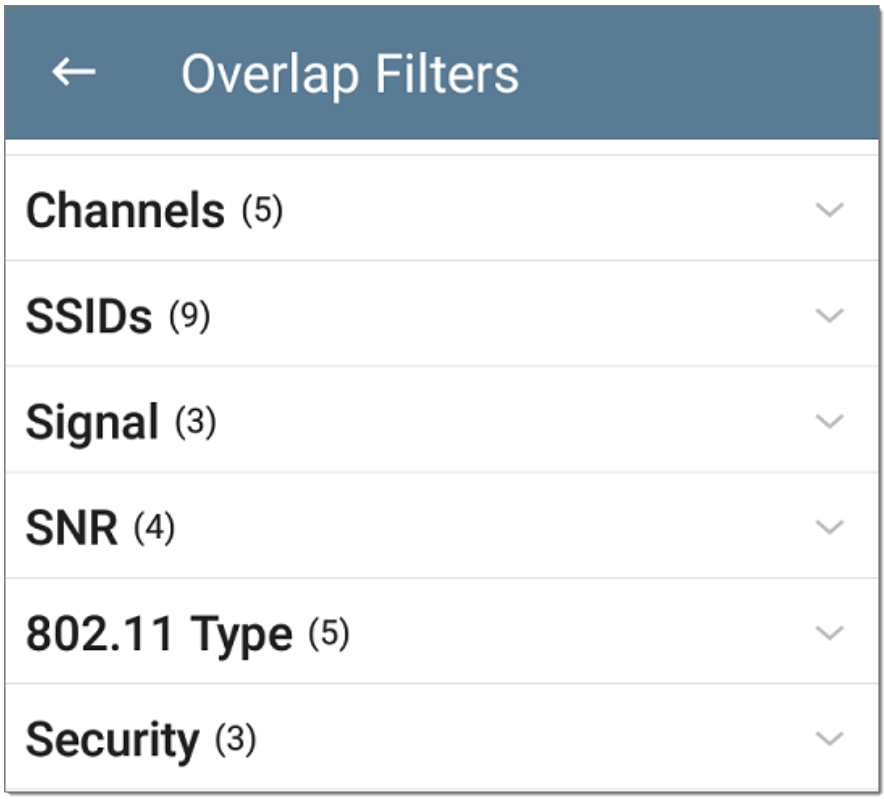


Filtering in the Wi-Fi App

Each Wi-Fi Analysis screen has different Filter options that are appropriate for the network component type you are analyzing.

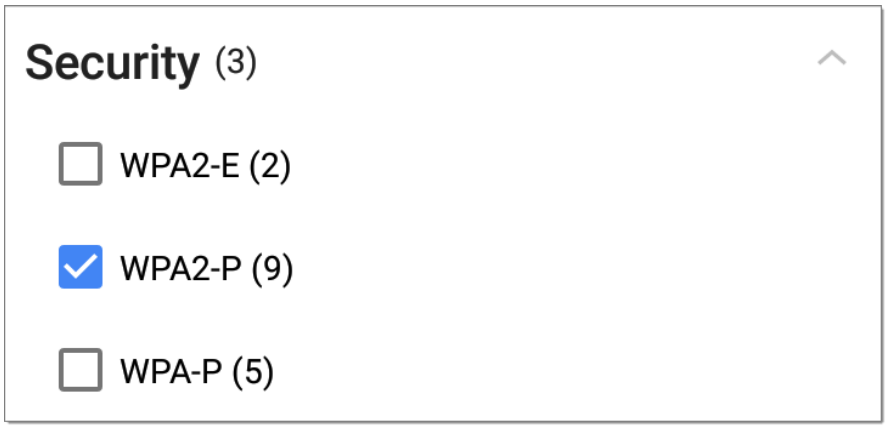
Tap the filter button near the top left of the Wi-Fi screens to set filters that control which network components are displayed. You can also

filter the **Channels Map > Overlap** screen, as shown below:



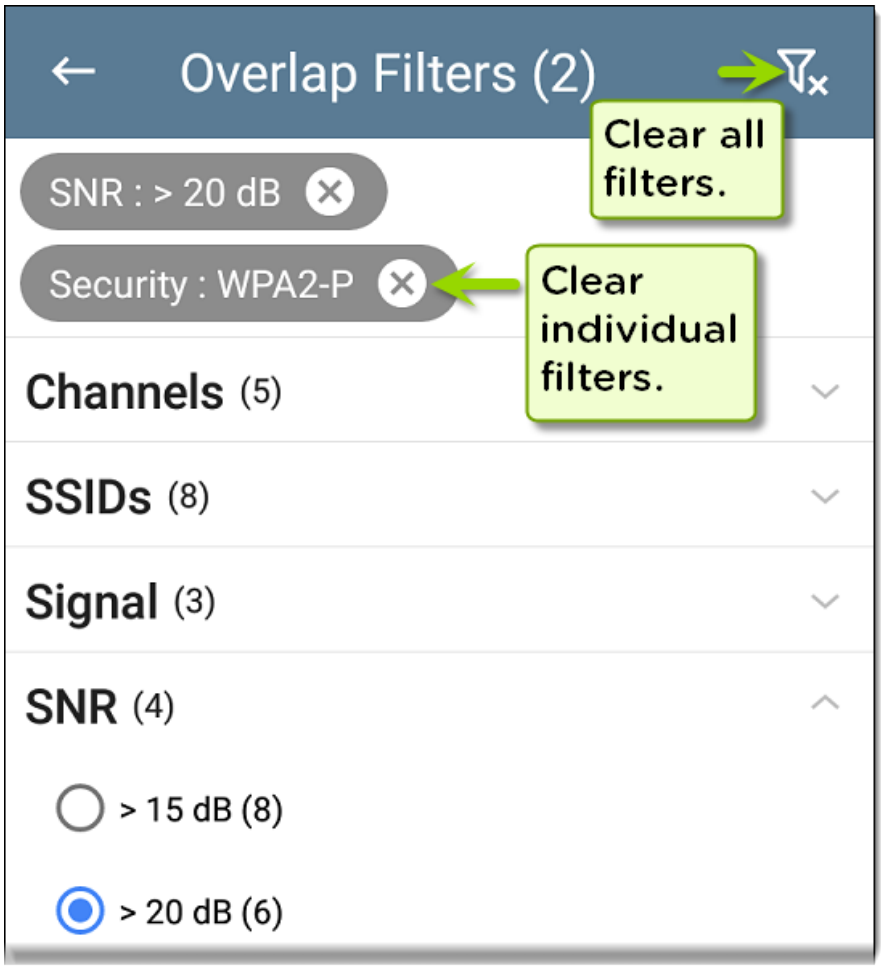
The number in parentheses shows how many active network characteristics are detected for each category. (The example shows (5) active Channels, (9) SSIDs, and so on.)

Tap a category to select filters by tapping the checkboxes or radio buttons.



Under each category, the number of discovered APs is shown for each characteristic. (In the example above, there are (3) Security types detected and (9) APs using the WPA2-P Security type.)

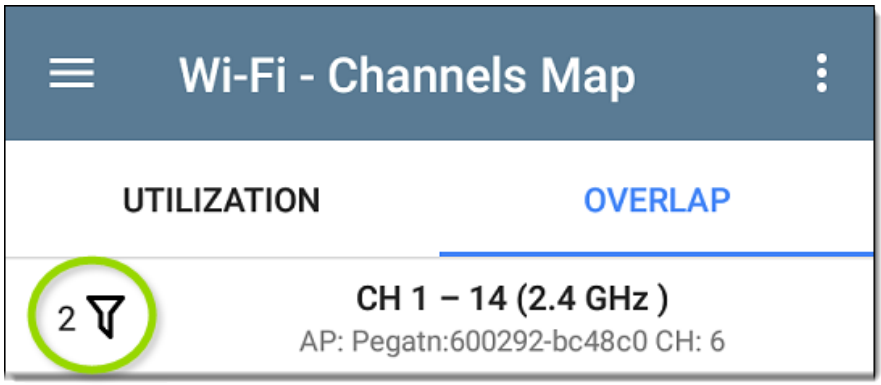
In this example, the Overlap screen shows only those APs that fall under your chosen filter parameters.



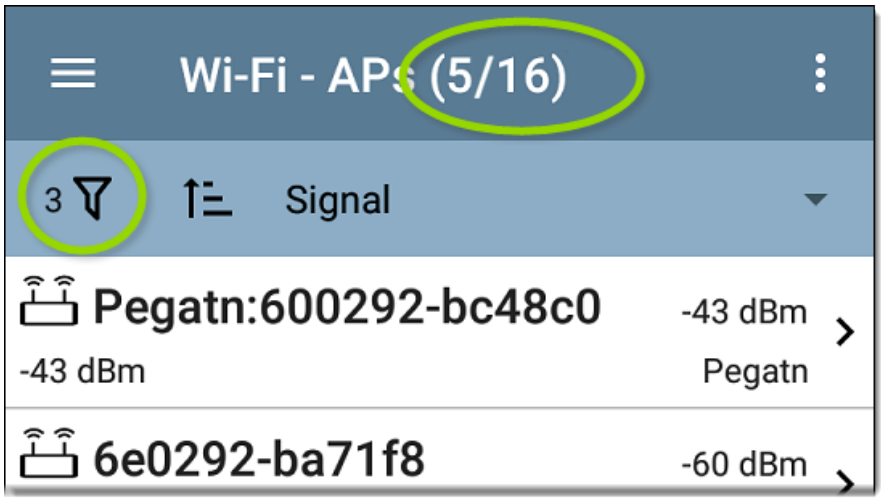
When filters are selected, those active filters are displayed at the top of the Filters screen.

- Tap the ✕ button to the right of each filter to clear it.
- Tap the clear filter icon at the top right to clear all filters.

Back on the Overlap screen, the number of active filters displays to the left of the filter icon, like this: 2 .

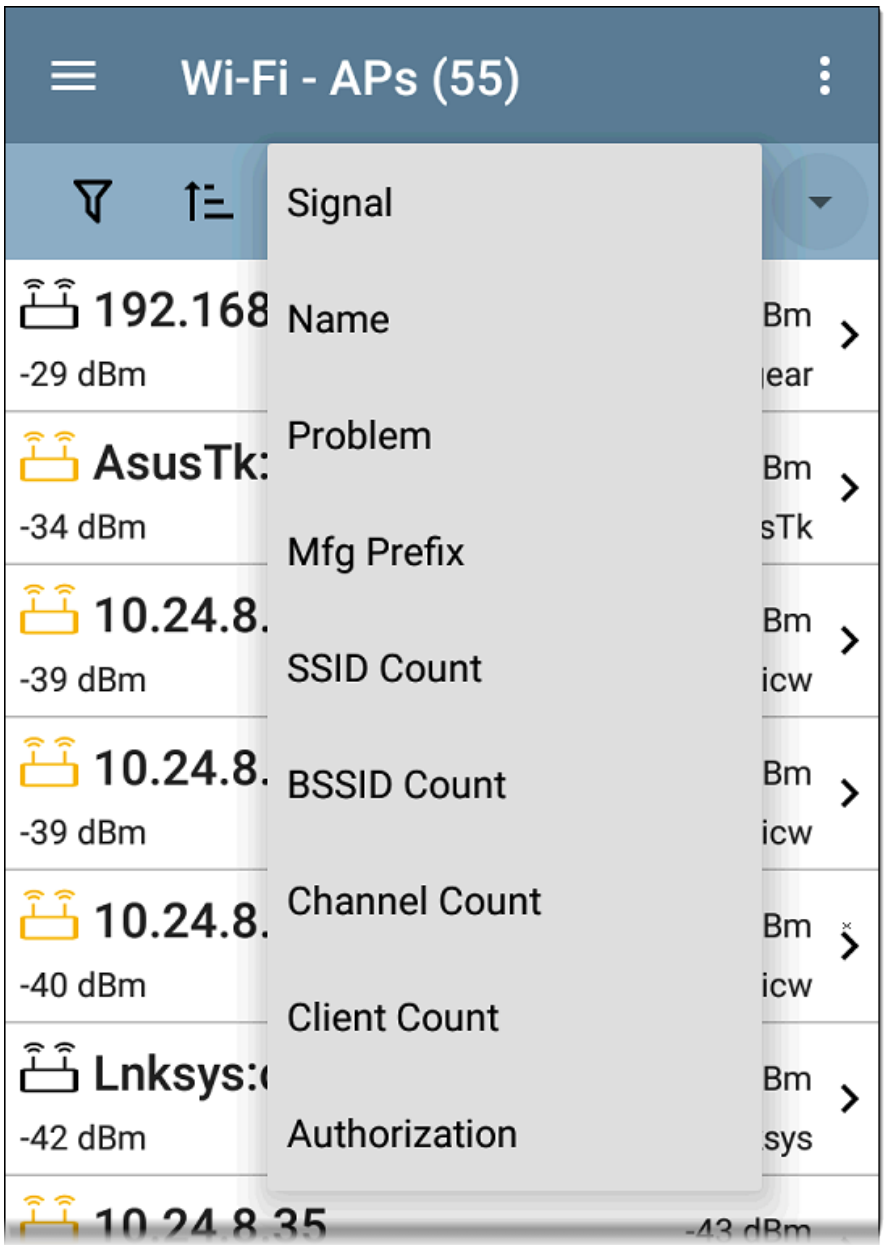


If the screen is a list, like the APs screen below, the screen title shows the number of filtered devices out of the total discovered devices (5 filtered devices out of 16 total).

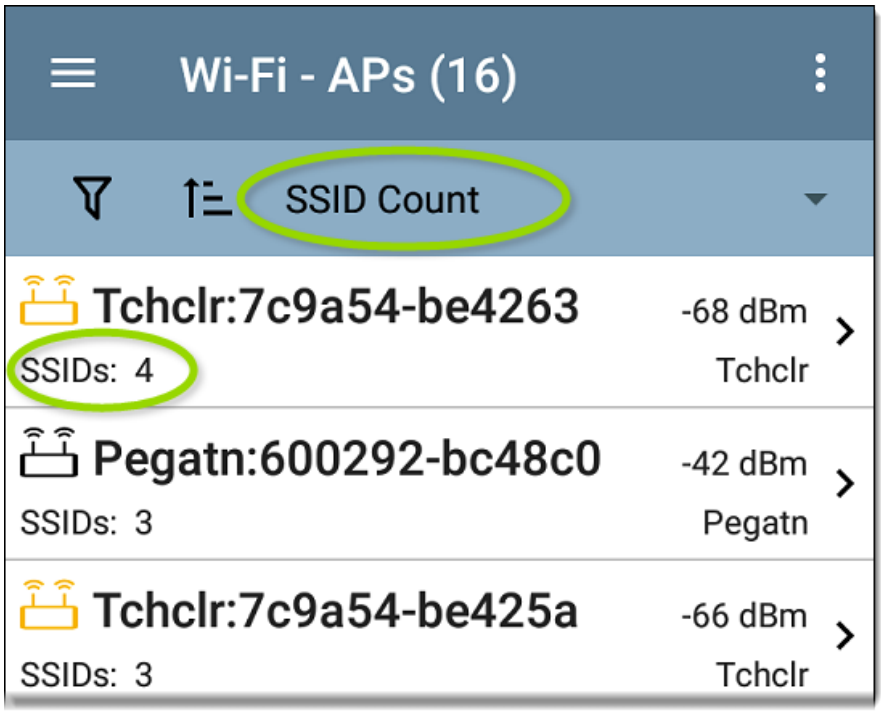


Sorting in the Wi-Fi App

Tap the Sort bar or down arrow to open the Sort drop-down menu. Each list screen supports relevant Sort options based on what you are viewing. The APs screen Sort options are shown below as an example.



Select a Sort option to order the list based on your selected characteristic.



The selected Sort option displays in the Sort bar above the list, and the sort characteristic for each item is shown under the type icon and name. In the image above, the discovered APs are sorted by SSID Count, which is shown below each AP icon.

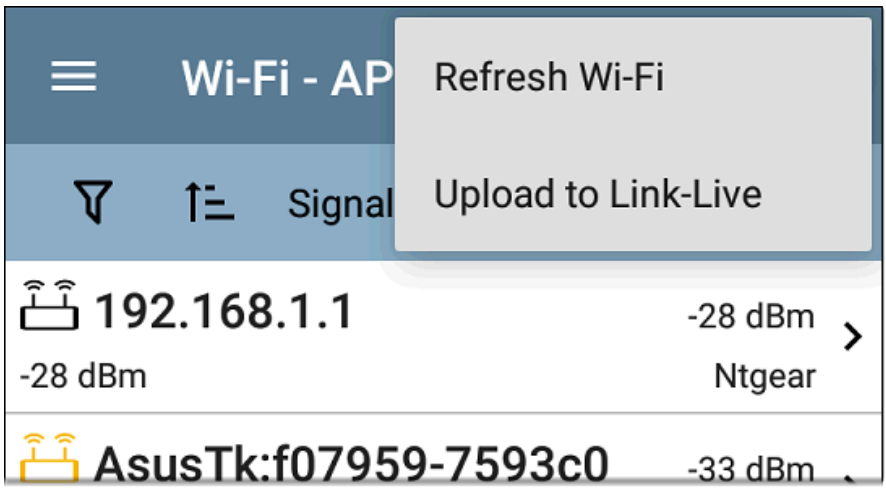
Tap the sort order icon to switch the sort order between normal and reverse order.

Wireless devices and IDs are sorted in groups. Those with resolved names appear at the top (in normal order), and then devices with only IPv4,

IPv6, and MAC addresses appear below, respectively. Reversing the normal sort order reverses the devices within the groups but does not change the order of the groups.

Refreshing Wi-Fi

Tap the action overflow icon ⋮ at the top right of the screen in any of the Wi-Fi screens (Channels Map, Channels, SSID, APs, BSSIDs, or Clients), and select **Refresh Wi-Fi** to clear and repopulate the Wi-Fi app screens with data.



Clearing All Problems

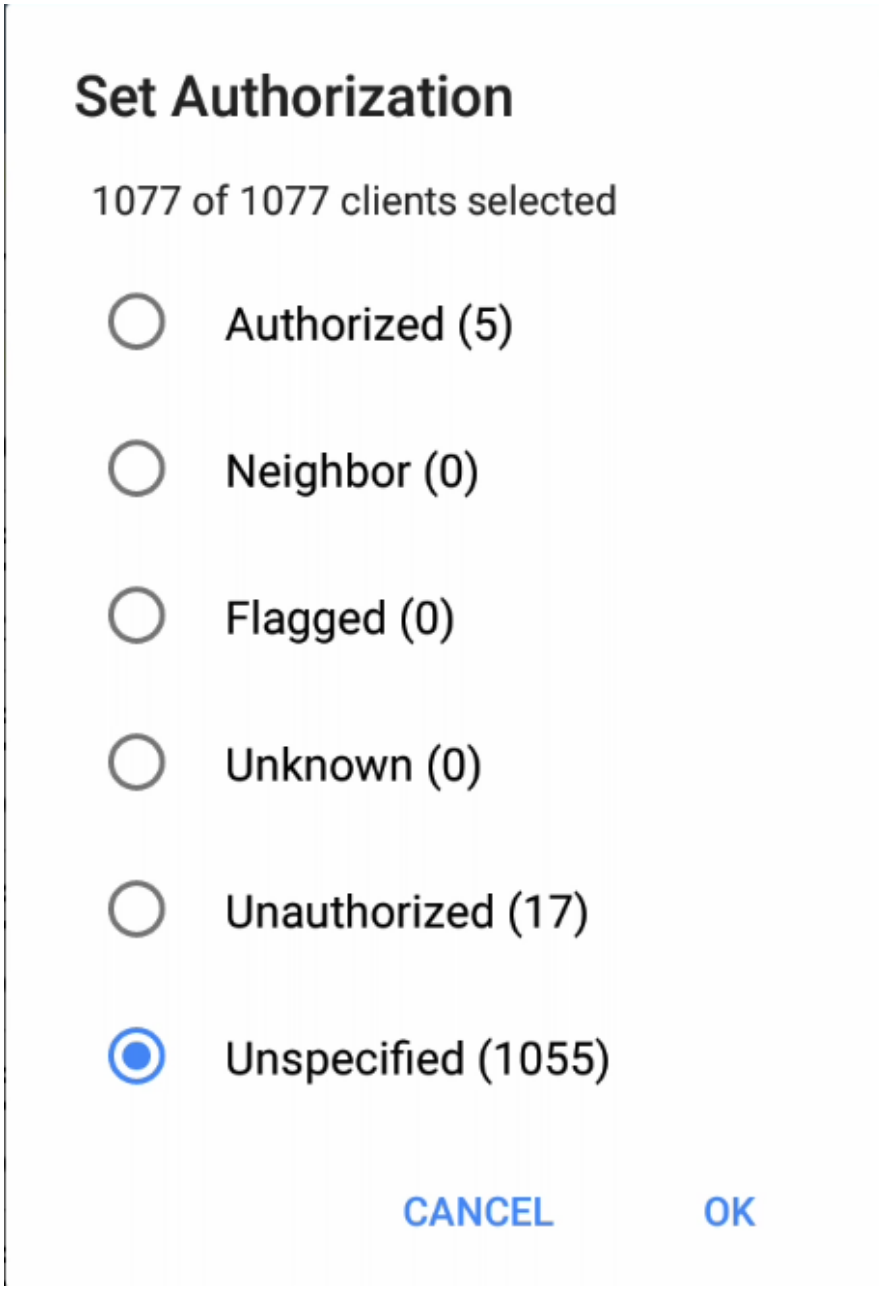
Tap the action overflow icon ⋮ at the top right of the screen in any of the Wi-Fi screens (Channels Map, Channels, SSID, APs, BSSIDs, or

Clients), and tap **Clear All Problems** to clear all detected problems on all Wi-Fi lists.

See Wi-Fi Problems Screen for more information.

Setting Authorization

You can also use the Authorization to sort the BSSID and Clients lists. From the BSSID or Clients list screen, tap the action overflow icon  at the top right and select **Set Authorization** to see how these devices are currently categorized and the number of devices in each category.



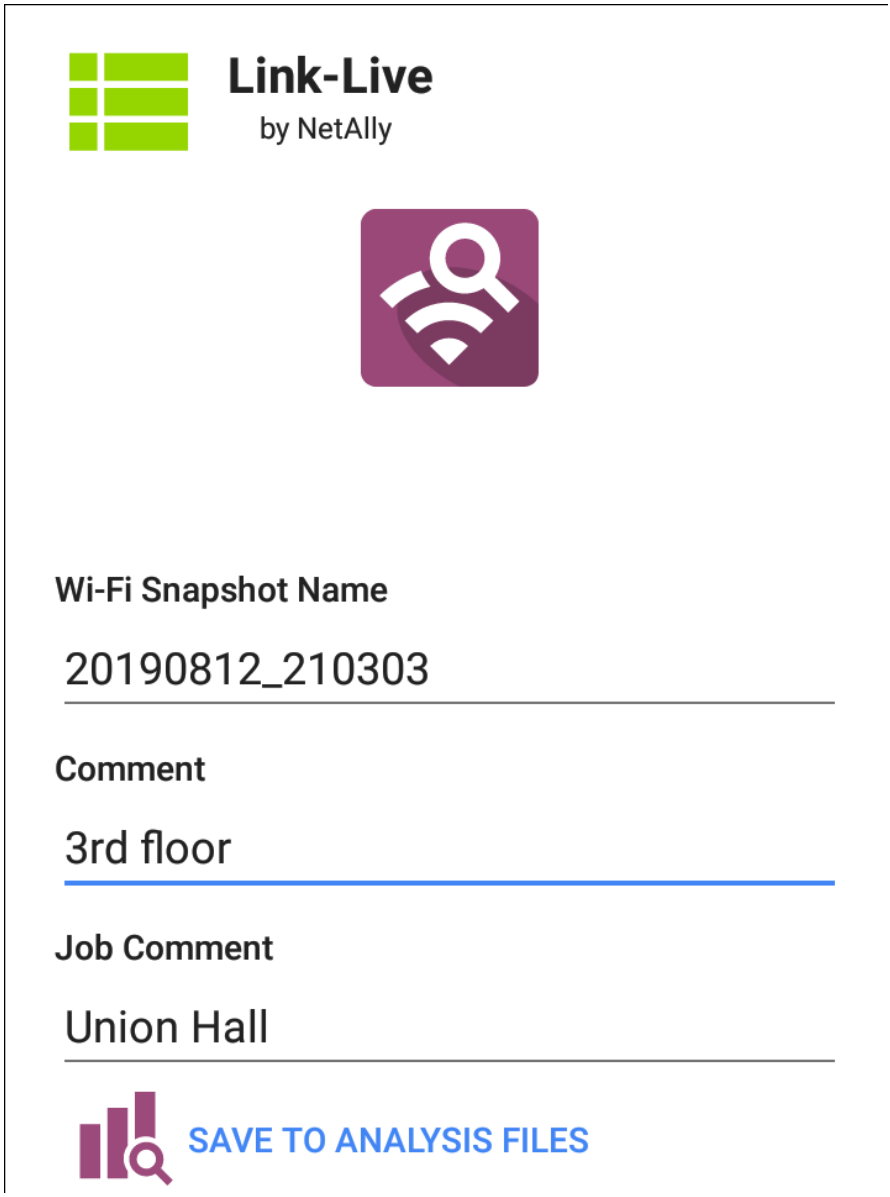
See "Wi-Fi Details Screens" on page 529 for more information.

Uploading Results to Link-Live

Tap the action overflow icon ⋮ at the top right of the screen in any of the Wi-Fi screens

(Channels Map, Channels, SSID, APs, BSSIDs, or Clients), and tap **Upload to Link-Live** to send the current Wi-Fi results to the Analysis page on Link-Live.com.

NOTE: Discovery app results automatically upload with the Wi-Fi results.



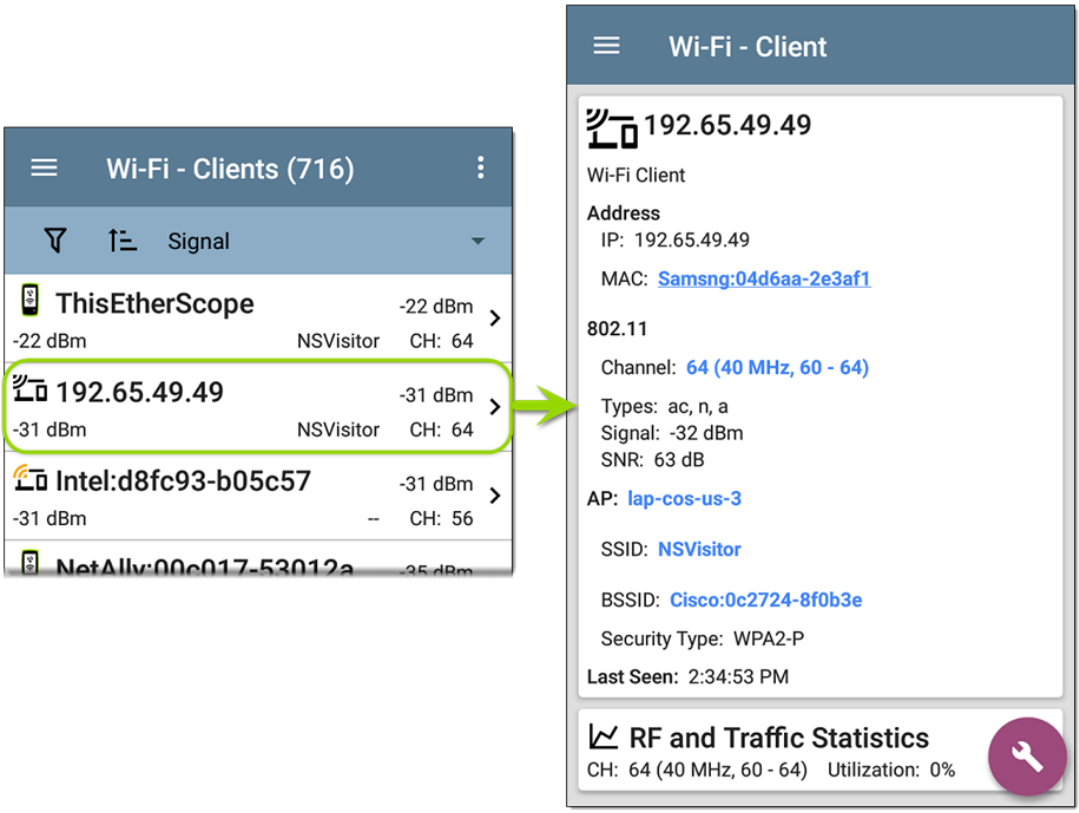
See the Link-Live chapter for more information.

Back to Title and Contents

Wi-Fi Details Screens

Tapping any card on a list screen—SSIDs, APs, BSSIDs, Clients, or Interferers (EXG-200 only) — opens the Details screen for that device or network ID.

The example below calls out a Client card and its Details screen.

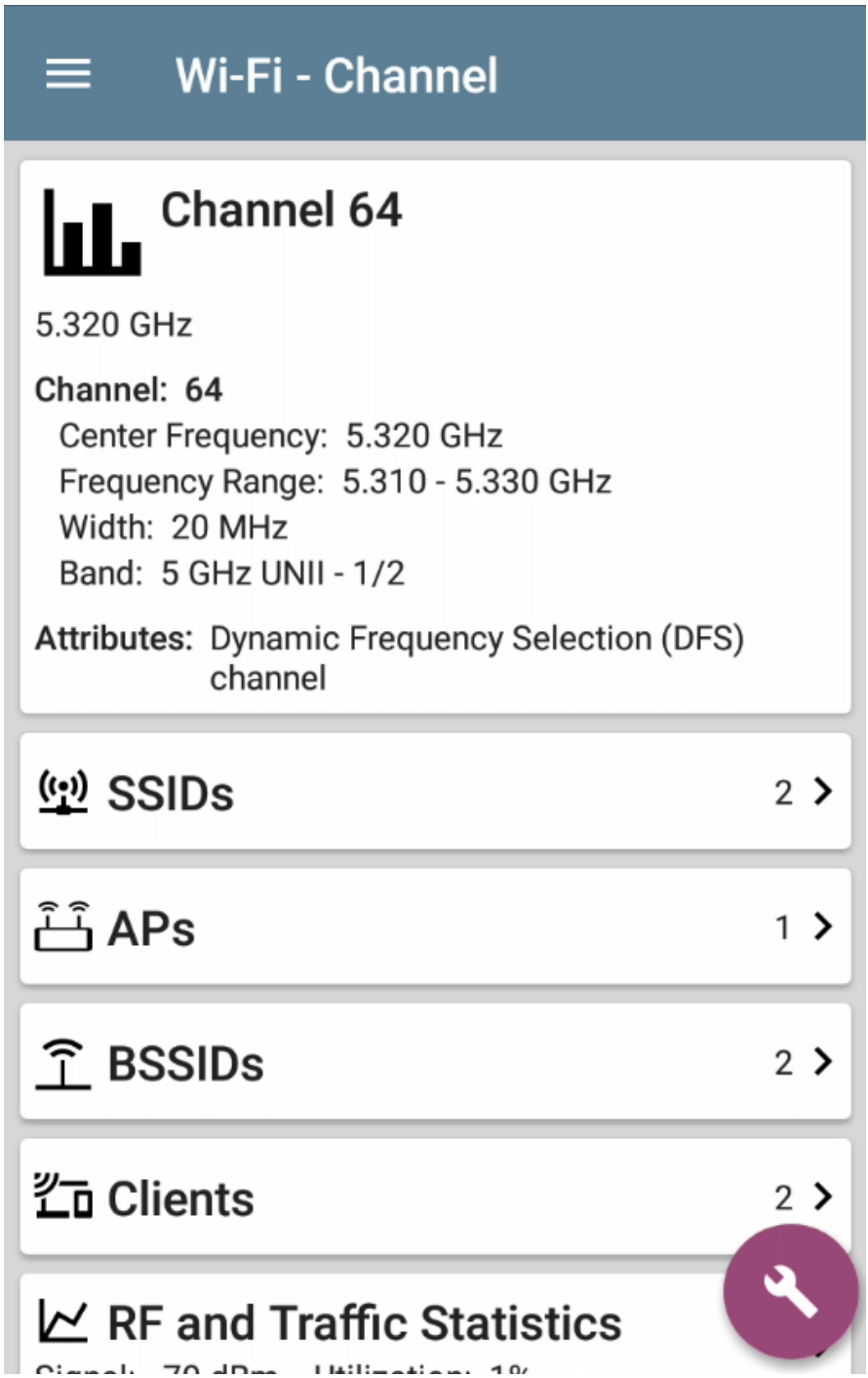


On the Wi-Fi Details screens, you can tap any **blue linked name or address** to open a Discovery or Wi-Fi app screen for the linked device.

NOTE: Non-underlined links open in the same app (in this case Wi-Fi), and **underlined links** open in a different app (in this case Discovery).

Each Details screen shows additional information about the selected item, any Problems detected by the EtherScope, and counts for other connected network devices or IDs.

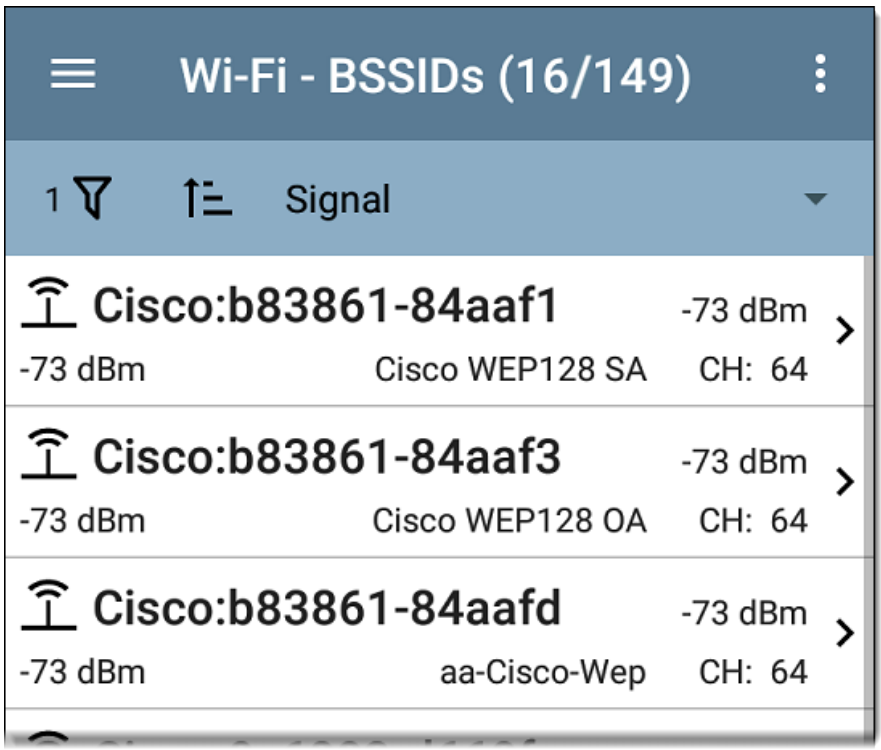
See also Data Fields on the Top Details Card in the Discovery chapter. Many of the Discovery data fields are the same as those shown in Wi-Fi Details.



The Channel Details screen above shows how many SSIDs, APs, BSSIDs, Clients, or Interferers (EXG-200 only) are detected on Channel 64. Tap the lower cards in Wi-Fi Details to open a list

screen that is filtered for the network component you are examining.

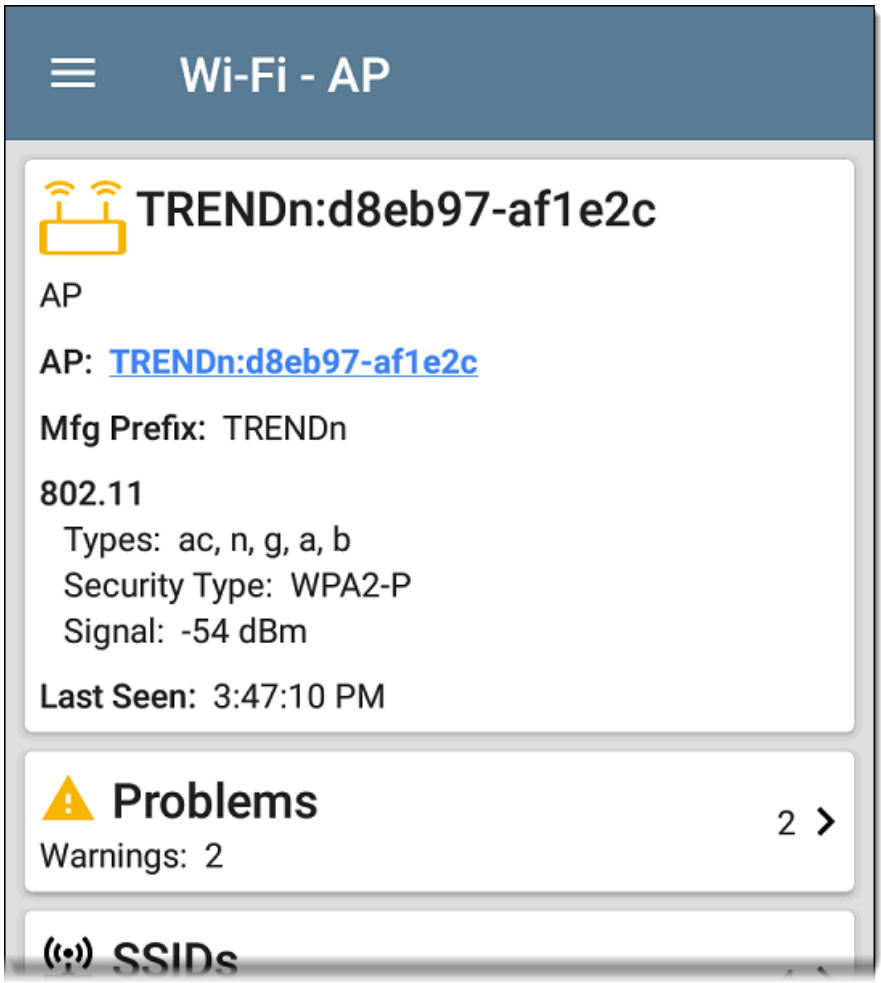
If you select BSSIDs on the Details screen for Channel 64, the BSSIDs screen opens and filters for BSSIDs found on Channel 64 only.



See the topics for each Wi-Fi app screen type (SSIDs, APs, etc.) for more discussion of the corresponding Details screen.

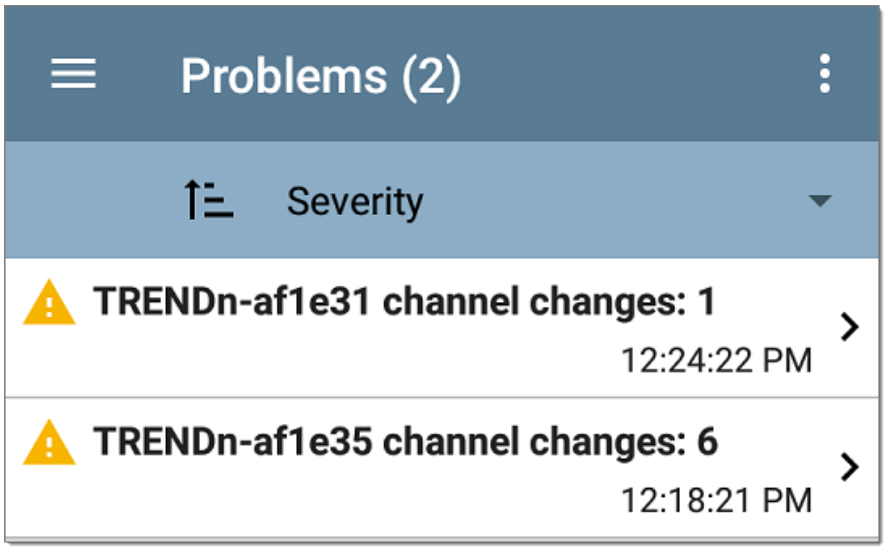
Wi-Fi Problems Screen

If any of the enabled Wi-Fi Problems are detected, the Problems card appears on the Wi-Fi Details screen.



The Problems card shows the icon color of the highest severity problem, and the number of detected **Warning**, **Failure**, **Information**, and **Resolved** conditions for the device or network component.

Tap the card to open the Problems screen.



On the Problems list screen, tap the Problem's row to read a detailed description.

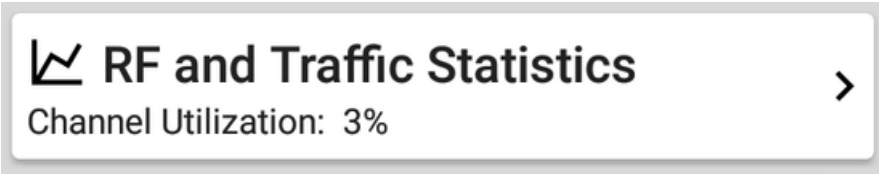
You can also tap the sort field to sort the list by **Severity** or by the time when the problem was **First Detected**. To clear a problem, tap the action overflow button ⋮ at the top right, and then tap **Clear Problem**.

See Problem Settings in the Discovery app to select which Wi-Fi Problems are detected and displayed by your EtherScope.

RF and Traffic Statistics Overview

The Channel, BSSID, and Client Details screens can display RF and Traffic Statistics if any traffic is detected.

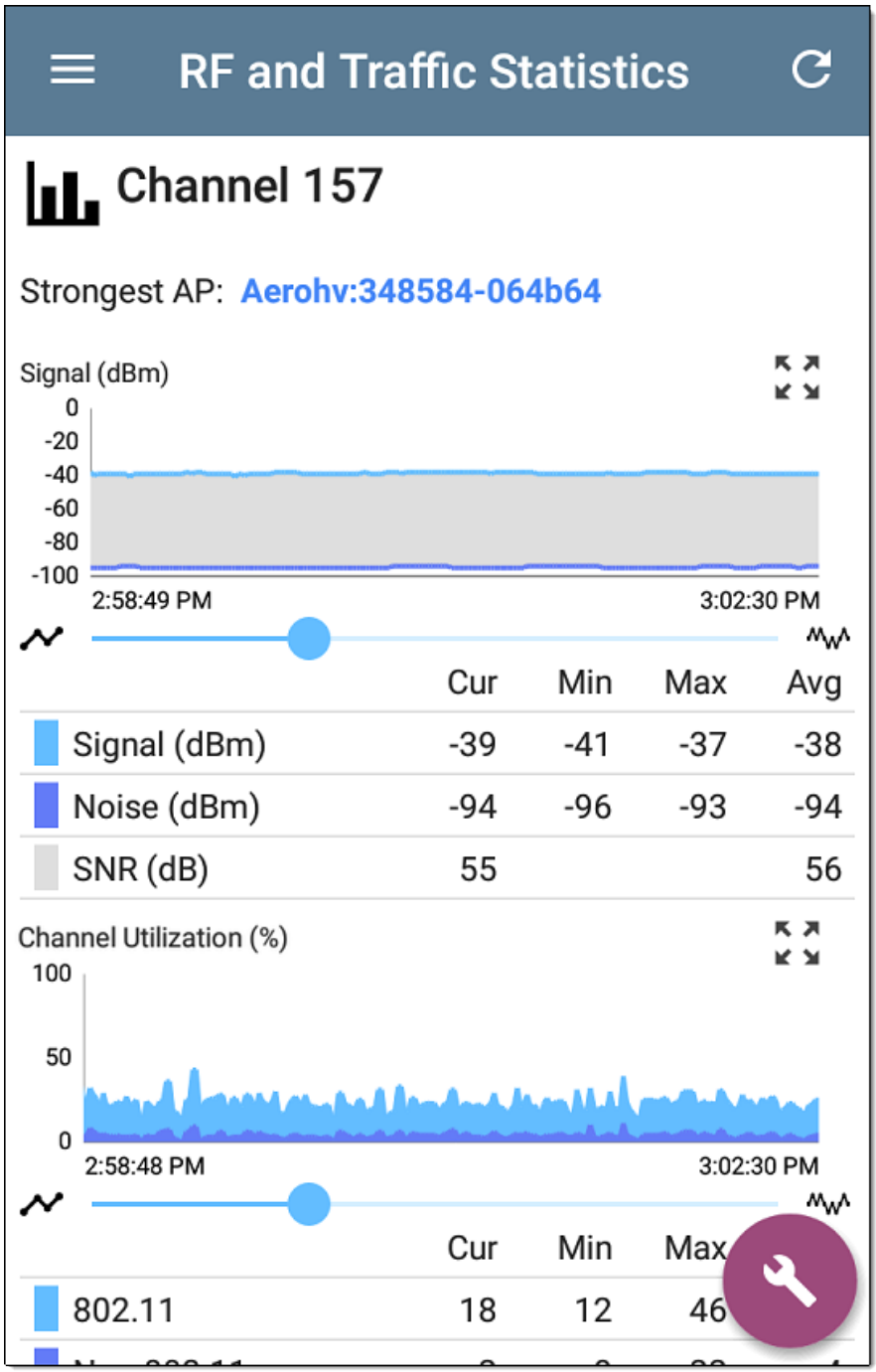
This section describes the common elements of the RF and Traffic Statistics screen. See the topic for each type of Details screen for differences.



The RF and Traffic Statistics card shows the Channel number or the Signal strength of the strongest AP on the channel and the channel's Utilization percentage.

Tap the card to view graphs of Signal, Noise, Utilization, and Retries.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.



Strongest AP: The AP on the channel with the strongest signal

Under each graph, a legend table displays the Current, Minimum, Maximum, and Average

measurements. The Current column contains measurements from the last second. Min, Max, and Avg columns show cumulative measurements gathered during the time the RF and Traffic screen has been open.

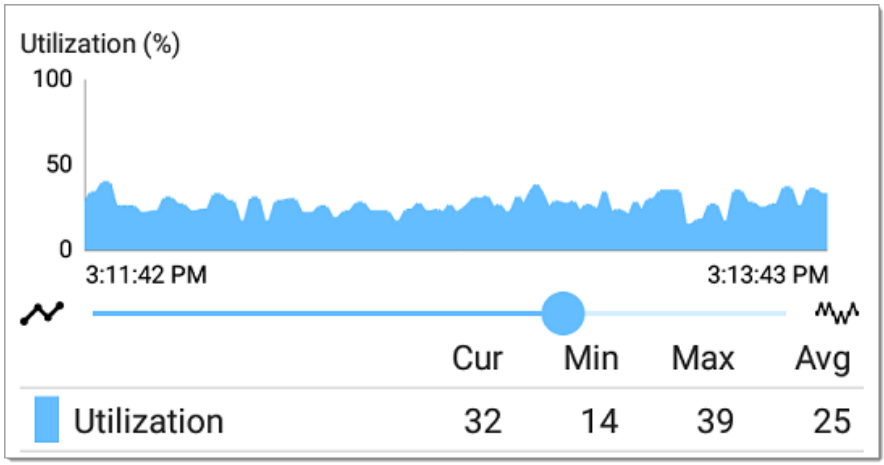
Tap the refresh button  at the top of the screen to clear and restart the measurements.

Signal (dBm) graph: Plots the signal strength in dBm of the selected AP or AP with the strongest signal on a channel

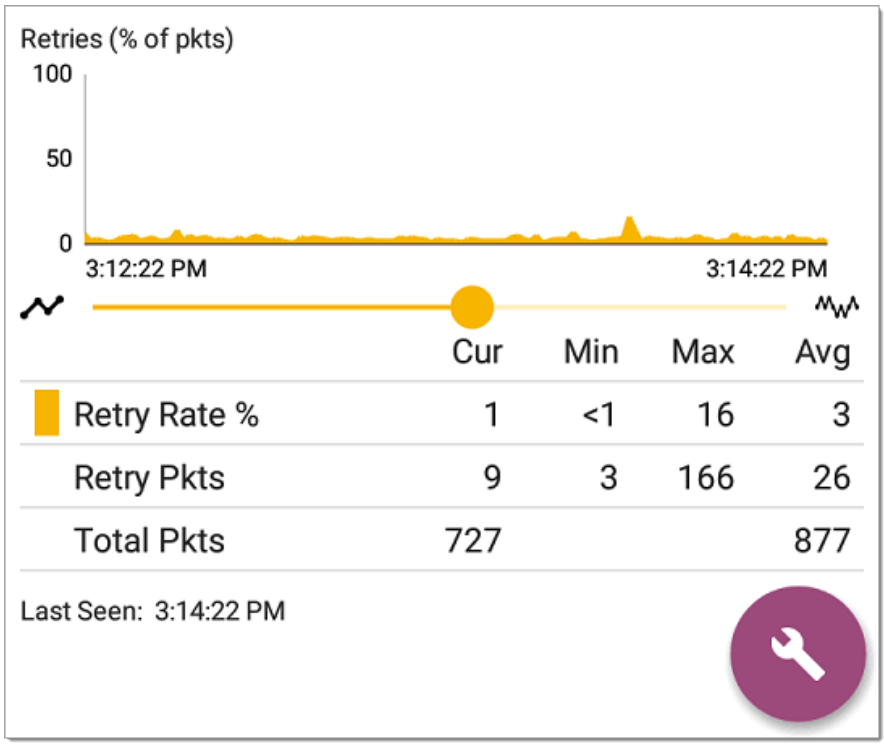
- Y-axis scales to the max Tx Rate supported by the Access Point, not the Wi-Fi Client.
- Signal - The AP's signal strength in dBm
- Noise - The noise level in dBm on the channel used
- SNR - The network's signal-to-noise ratio, a measure of signal strength relative to noise, measured in decibels (dB)

Channel Utilization (%) graph: Plots percentage of the channel capacity being used by 802.11 devices and by non-802.11 interference.

(EXG-200 only) If the **Combine Utilization** setting is enabled in General Settings, the Utilization graph shows combined channel utilization and 802.11 utilization only for BSSIDs and Clients.



Retries (% of packets) graph: Plots percentage of transmitted packets that are retry packets.



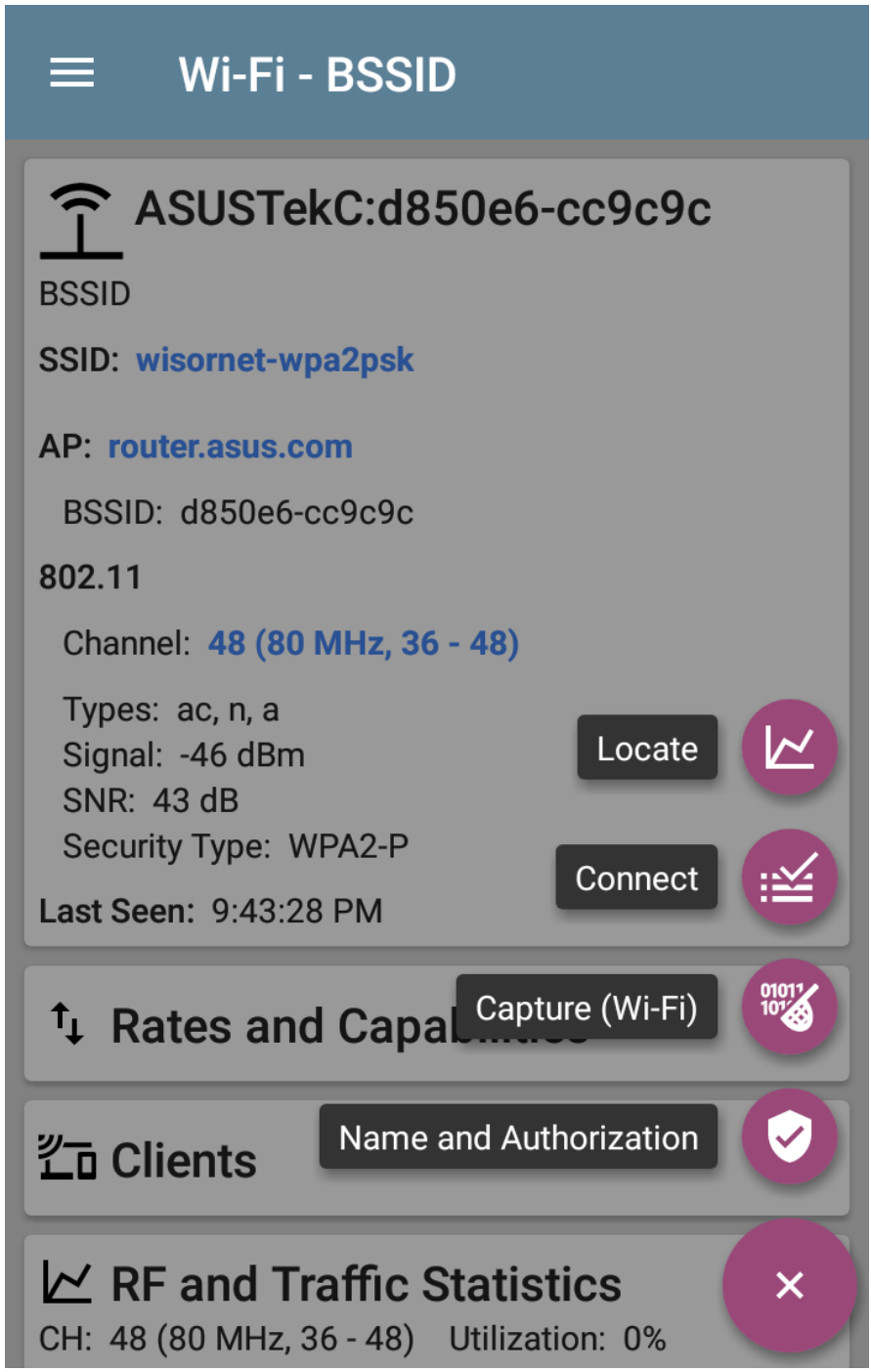
- Retry Rate % - The percentage of total packets that are retry packets
- Retry Pkts - The number of retry packets
- Total Pkts - The total number of transmitted packets

Locating Wi-Fi Devices

You can use your EtherScope to locate APs and Wi-Fi clients from the Channels Map screen for BSSIDs and Clients.

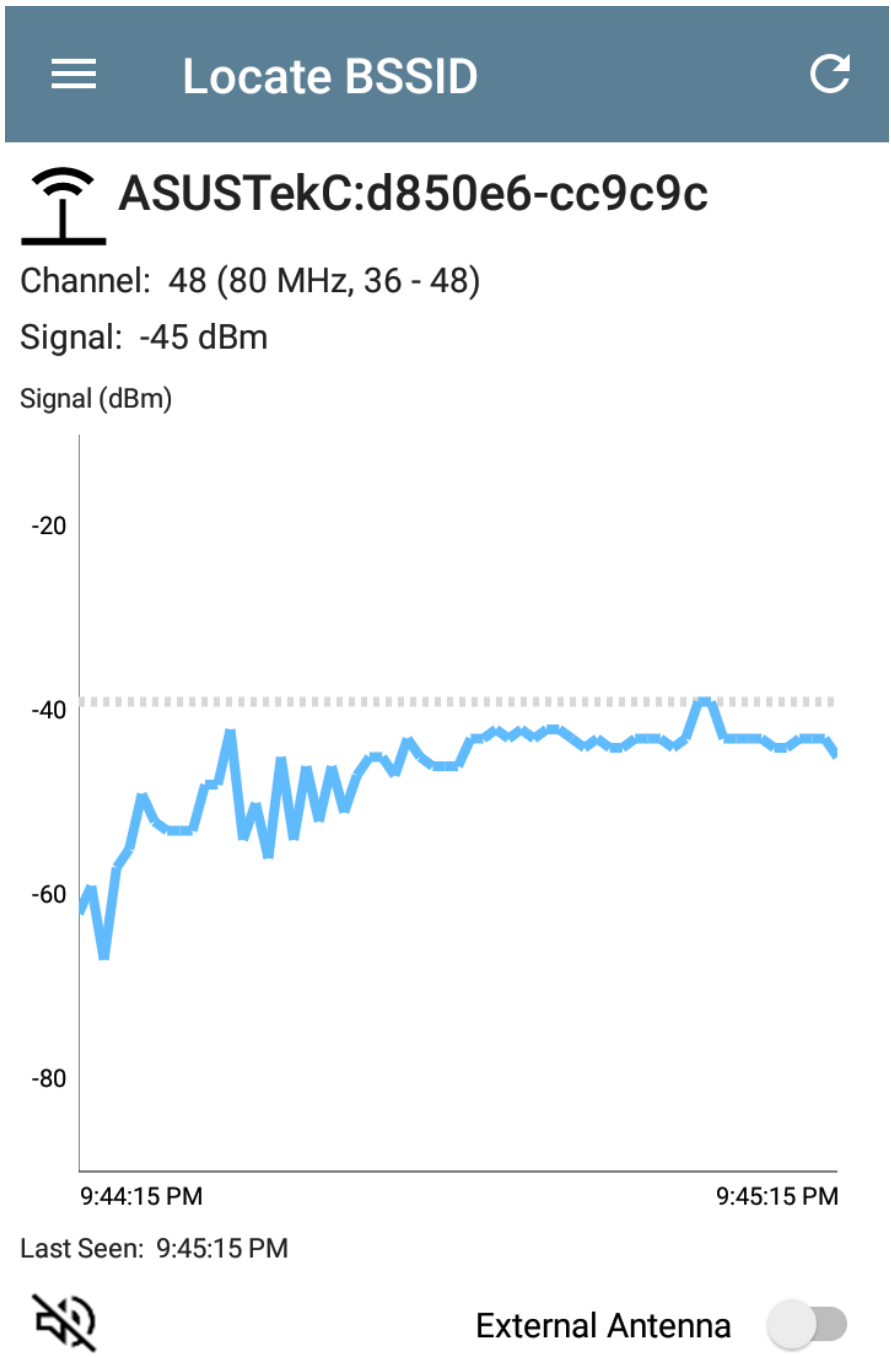
To begin a location action:

1. Start the Wi-Fi app.
2. From the menu icon  , select **BSSIDs** or **Clients**.
3. Select the BSSID or Client that you want to locate.
4. Tap the FAB menu icon  in the lower right corner of the screen. This displays the FAB pop-up options.



5. Tap **Locate**. This opens the Locate screen and causes your EtherScope to "listen" for the BSSID or Client wireless devices you

want to find using either the internal antennas or the optional external antenna (sold separately or in kits).

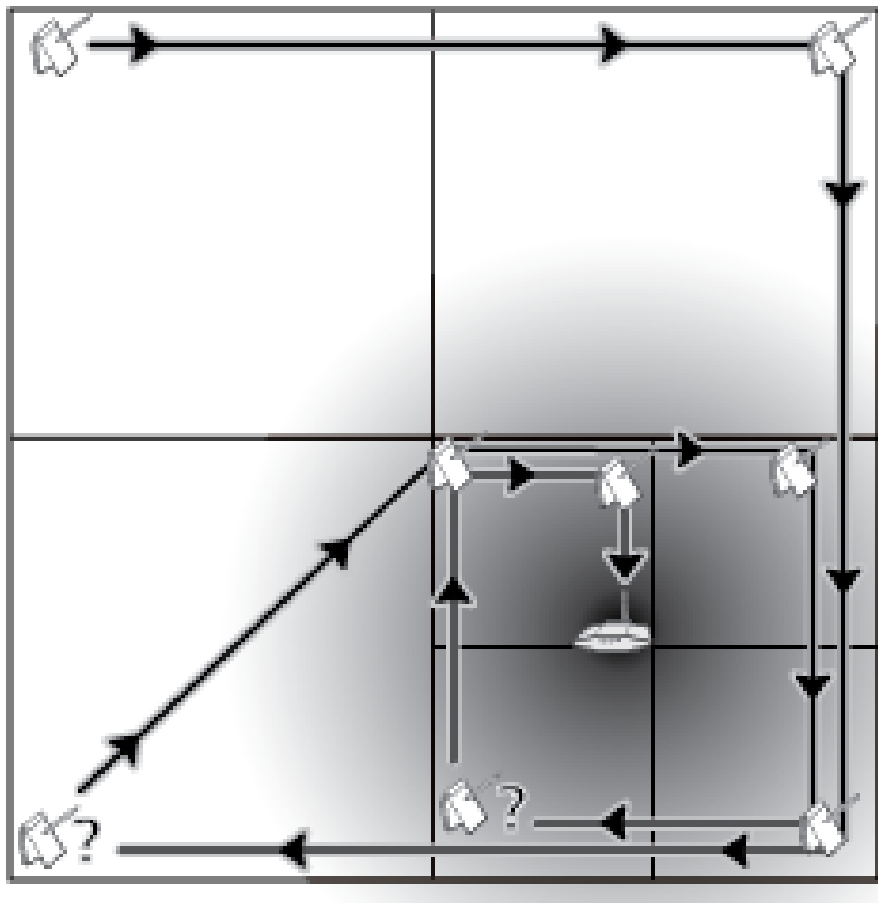


- The test unit can emit an audible tone that increases in pitch as the signal strength of the device increases (as you get closer to it).
  - Tap the speaker icon to turn sound on or off.
- The **External Antenna** toggle enables the optional external antenna for BSSID or Client location.
  - In areas with many rooms, like a hospital or school, the internal antennas are more effective. See Using the Internal Antennas to Locate below.
  - In large, open areas, the external antenna can help locate devices more quickly. See Using the Optional External Antenna below.

Locating with the Internal Antennas

EtherScope uses the internal antennas by default.

1. Navigate to the RF and Traffic Statistics screen for the BSSID (AP) or client you need to locate.
2. (Optional) Tap the speaker icon to toggle the audible tone on or off.
3. Divide the area you want to search into four sections.



4. Go to one corner of your search area, and note the device's signal strength on the Signal graph.

5. Go to the other three corners of the area, and note the signal strength at each corner.
6. Go to the section with the strongest signal.
7. Repeat steps 3 through 6 until you find the device.

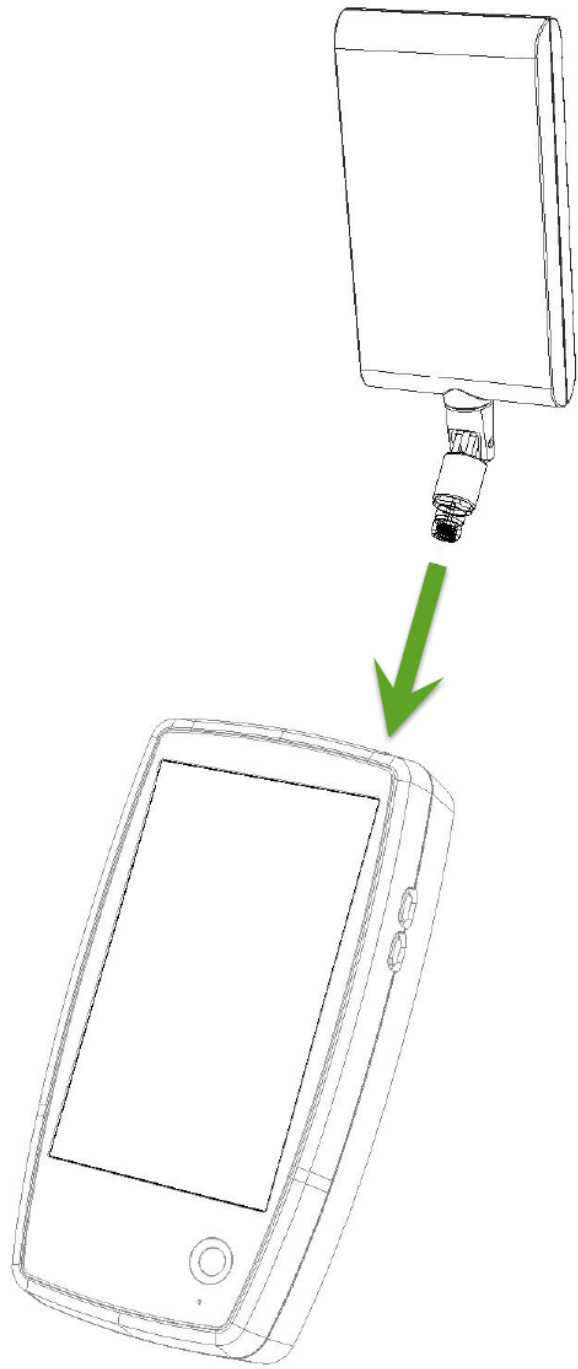
If you still cannot find the device, try looking on the floors above or below you. If you cannot find a client, try locating the AP to which the client is connected first.

Locating with the Directional External Antenna

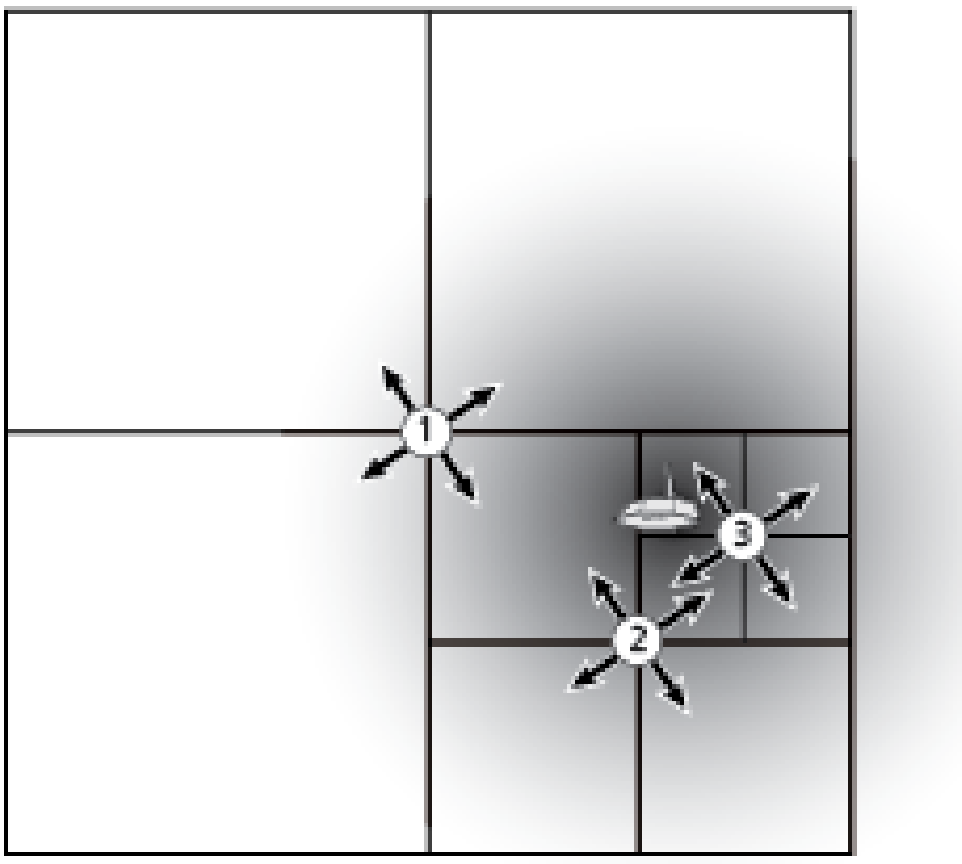
In large, open areas, the directional external antenna can help determine the direction of a signal source more precisely than the internal antennas. Visit NetAlly.com for purchasing information.

1. If using the Directional Tri-band (2.4, 5, and 6 GHz) external antenna, screw the antenna's RP-SMA connector into the antenna port on the top of the EtherScope (shown below). If using the Dual-band (2.4

and 5 GHz) Flag antenna, screw the external antenna cord into the antenna port.

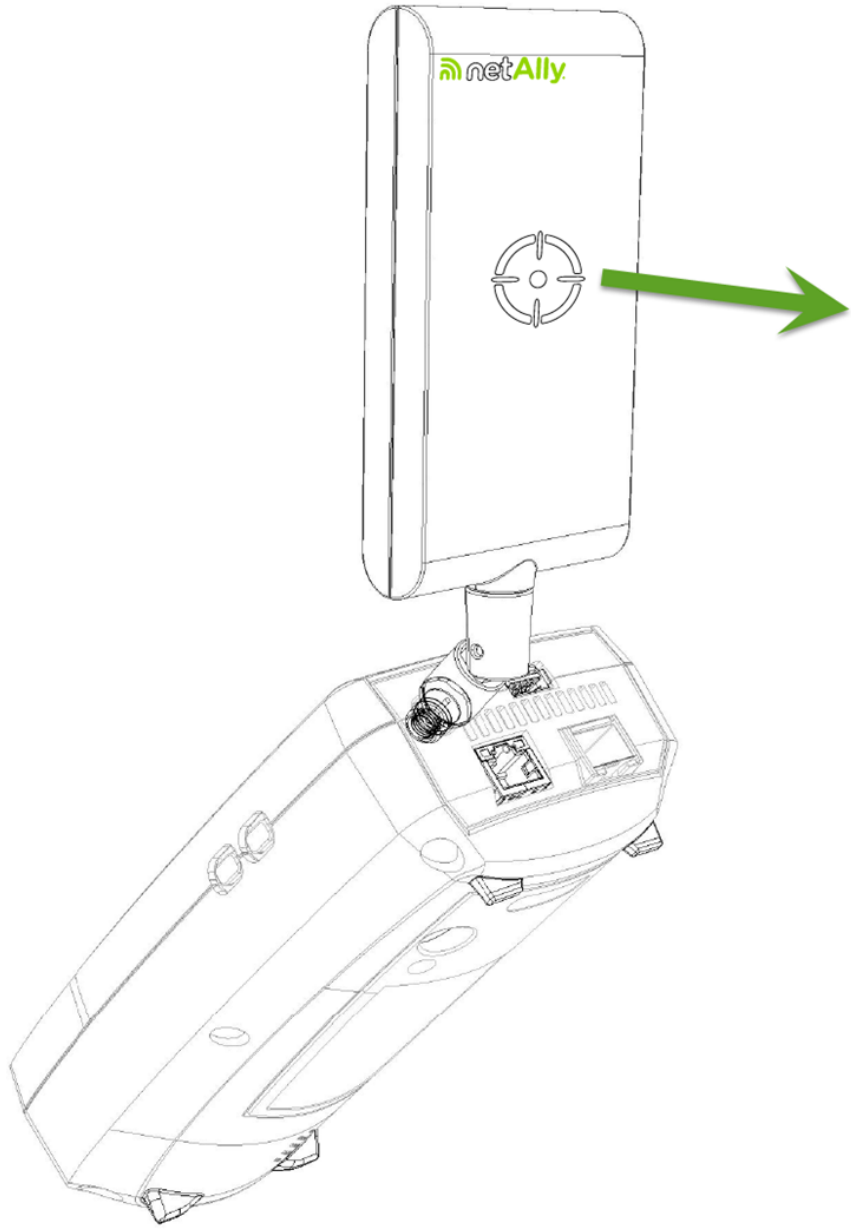


2. On the RF and Traffic Statistics screen, tap the **External Antenna** toggle to enable the external antenna.
3. (Optional) Tap the speaker icon to toggle the audible tone on or off.
4. Divide the area you want to search into four sections.



5. Go to the center of your search area.
6. For the Directional Tri-band external antenna, use the swivel joint on the RP-SMA

connector to angle the antenna so that the "target" silkscreen on the antenna points toward your search area, as shown below. Point the antenna towards each corner of the area. To get the best measurements, hold it at a constant height and above barriers such as cubicle walls.



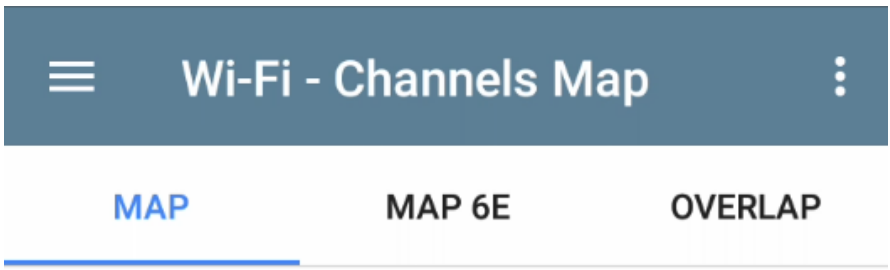
7. For the Dual-band Flag antenna, point the front edge of the antenna toward your search area, as shown below.

8. Go to the middle of the section with the strongest signal.
9. Repeat steps 4 through 7 until you find the device.

Back to Title and Contents

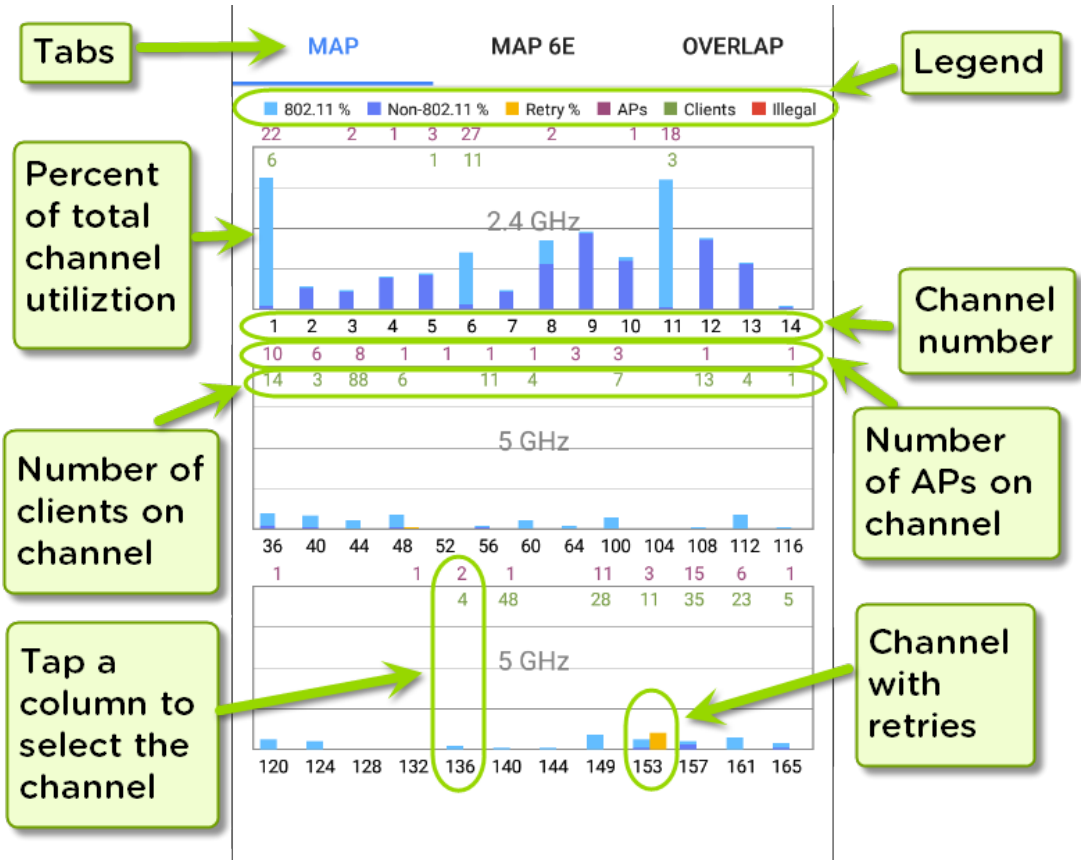
Channels Map

The Channels Map screens provide charts of channel utilization with AP coverage and overlap. Swipe right or left or tap the tab names to switch between the chart types: **Map**, **Map 6E**, or **Overlap**.



Map and Map 6E Tabs

The Map and Map 6E tabs display a bar graph of 802.11 and non-802.11 utilization, retry percentage, APs for each channel, clients for each channel, and illegal channels. (The Map 6E tab is for 6 GHz channels only.)

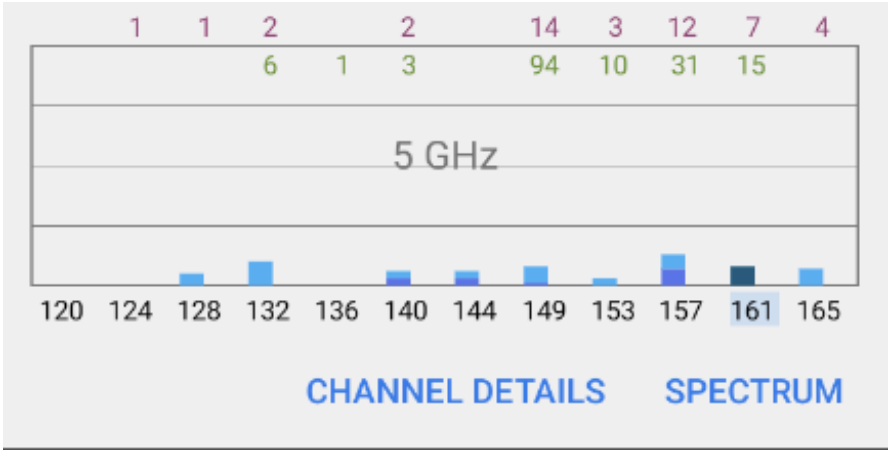


- Blue vertical bars show the percentage of each channel's capacity used by 802.11 devices (light blue) and non-802.11 interference (dark blue). (EXG-200 only) If the

Combine Utilization setting is enabled in General Settings, the graph shows only combined 802.11 and non-802.11 Utilization.

- Yellow bars next to the blue bars show the percentage of retries.
- Channel numbers are listed on the x-axis and utilization percentage on the y-axis.
- AP counts for the APs' primary channel are shown in dark red at the top of the column for each channel. In the example below, Channel 161 has 7 APs. (Channels that do not have APs can still show 802.11 utilization because of overlap from adjacent channels.)
- Client counts for the channel are shownnear the top of the column for each channel. In the example below, Channel 161 has 15 clients.
- Tap a Channel's column on the Map or Map 6E graph to select and highlight the channel. This displays the CHANNEL DETAILS and SPECTRUM links at the bottom of the screen. In the example below, Channel 161 is

highlighted.

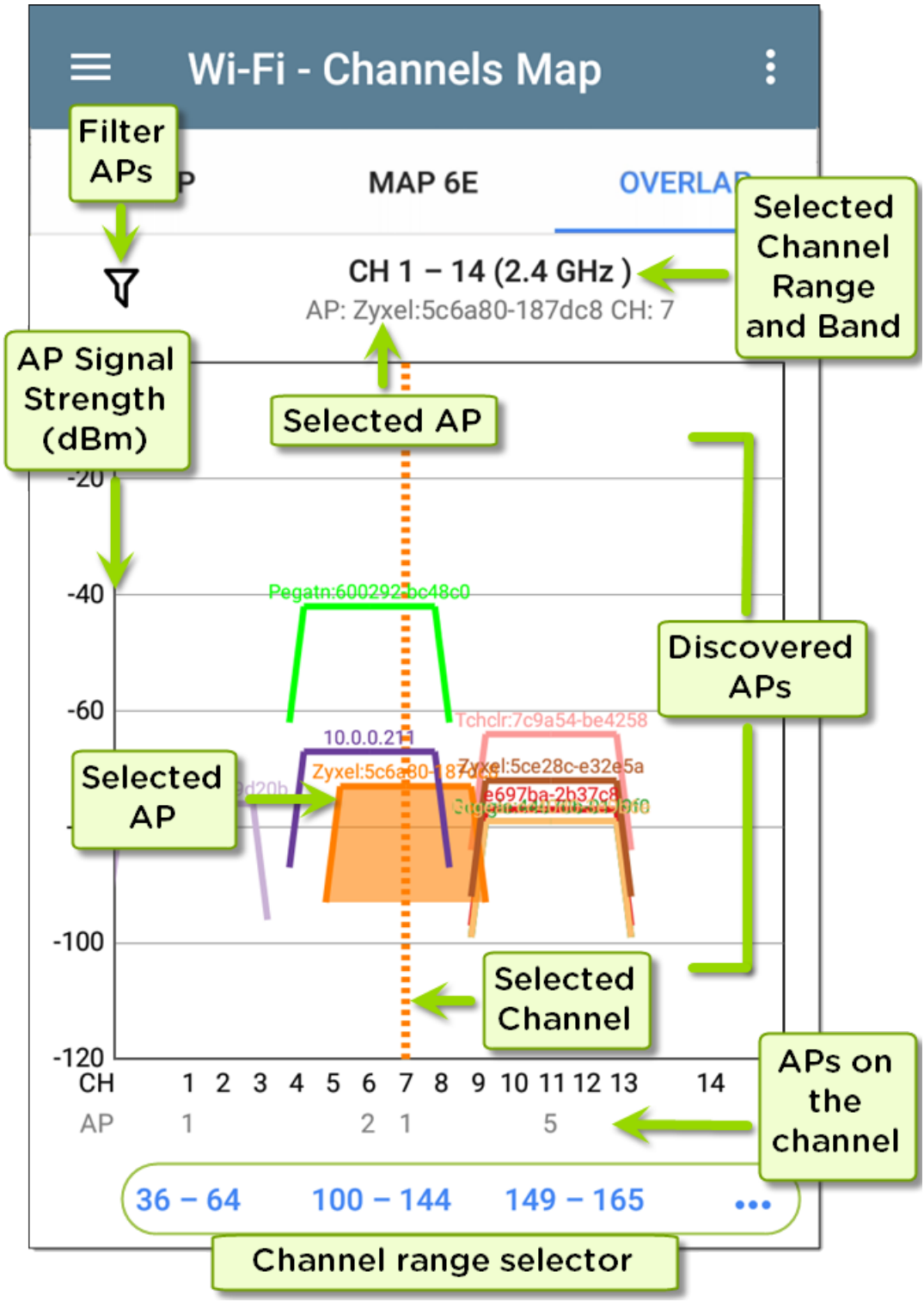


The Channel Details screen lets you examine the addresses and devices operating on the channel and perform a deeper analysis.

The Spectrum link opens the Spectrum app, a Wi-Fi spectrum analyzer that provides data about signal strength and noise.

Overlap Tab

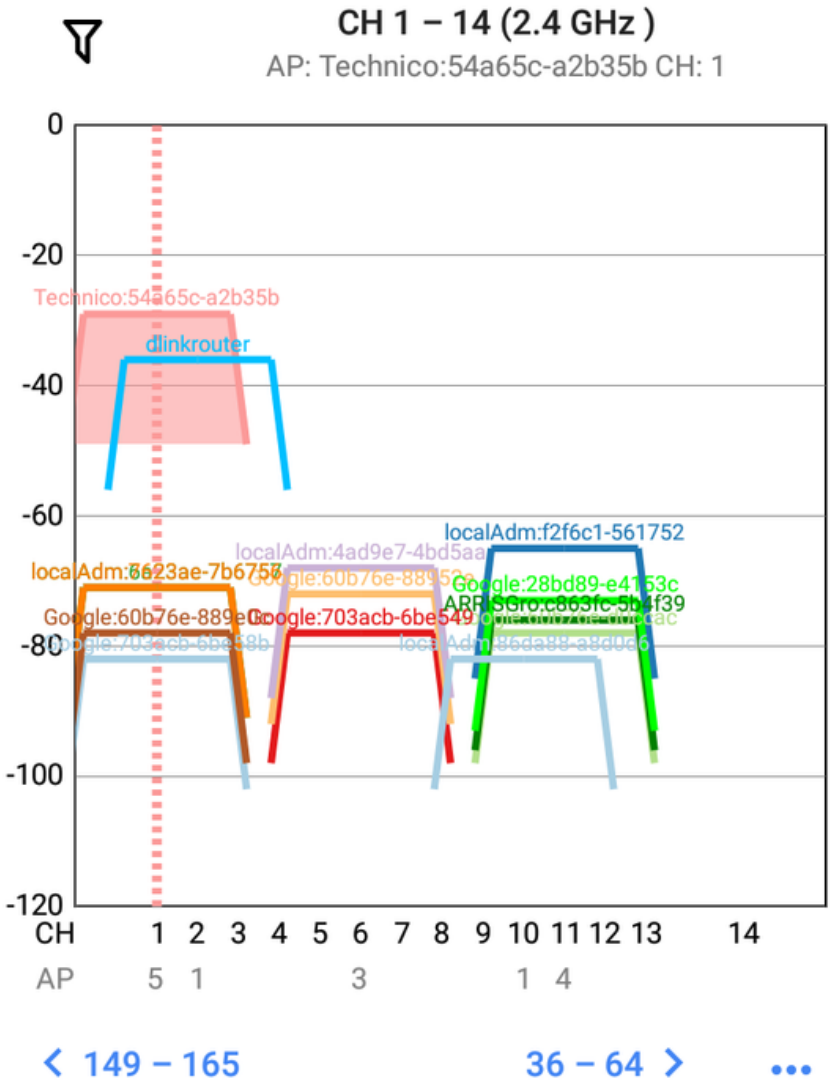
Tap **Overlap** to view access point channel, coverage, and overlap. This can help you spot potential coverage issues. Each discovered AP is shown as a colored bracket on a graph based on channel coverage (on the x-axis) and signal strength in dBm (on the y-axis).



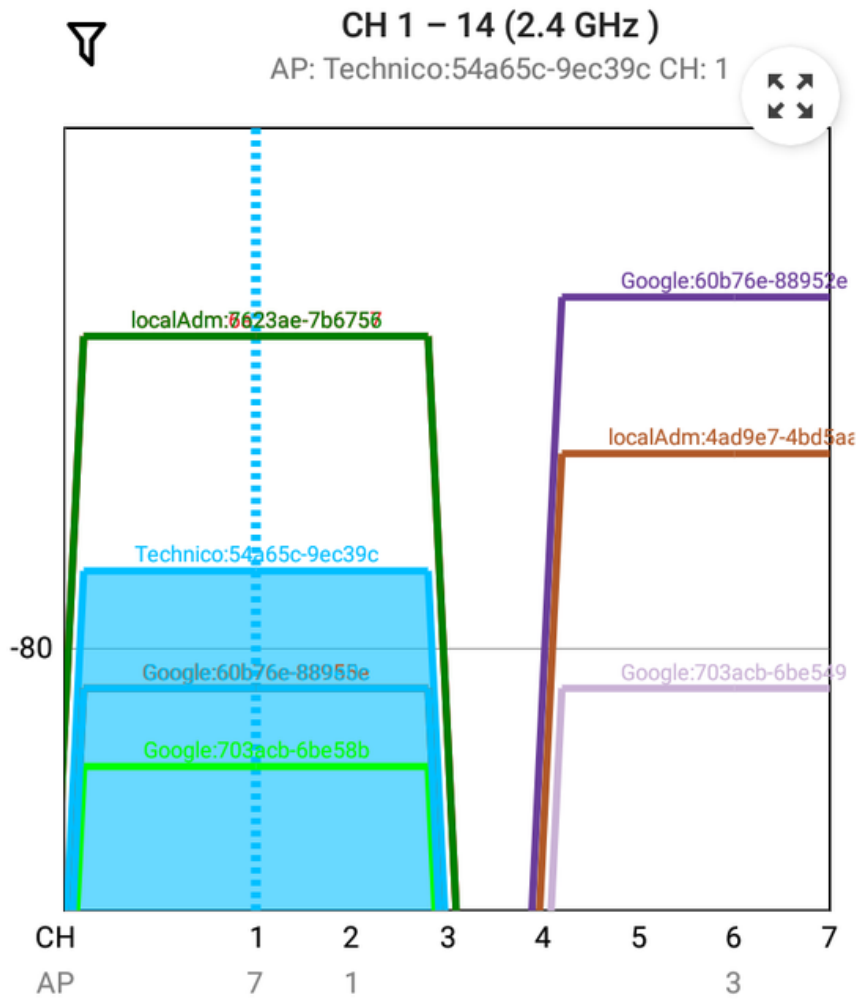
- Tap the Filter icon near the top left to open the Overlap Filters screen to control

what APs are displayed. You can select filters for channels, SSIDs, Signal, SNR, 802.11 type, or Security.

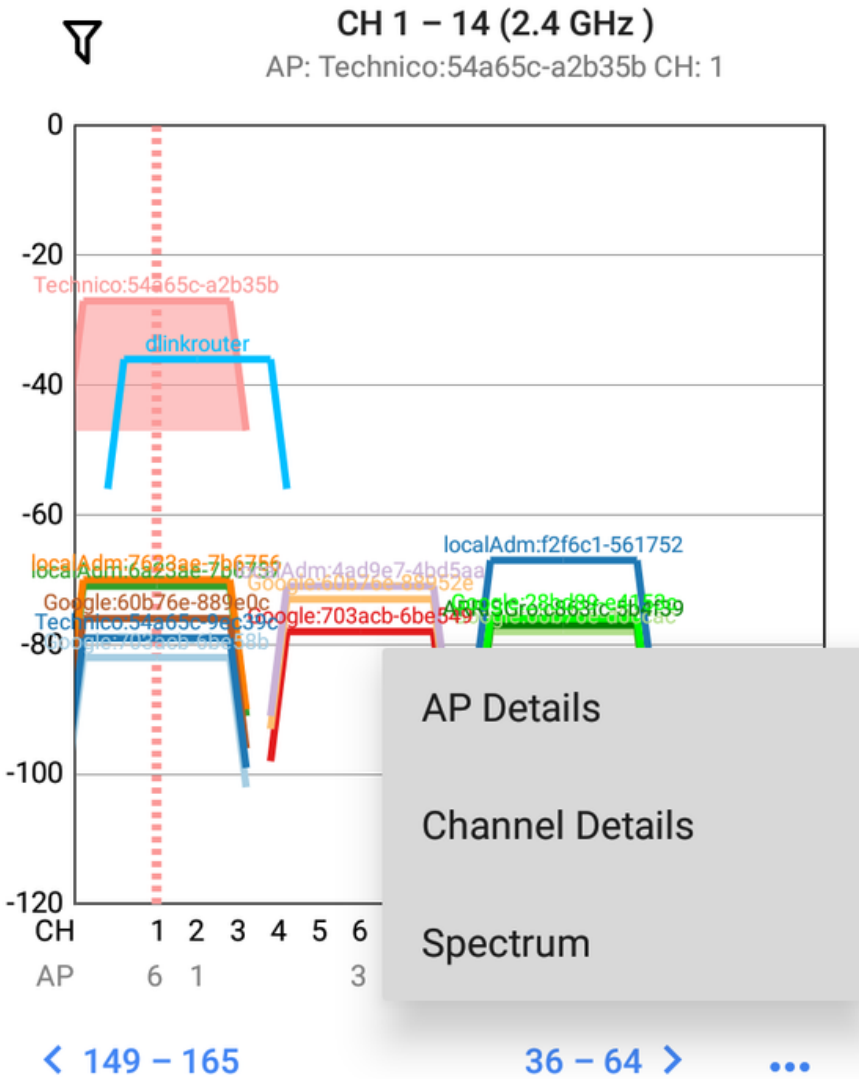
- Tap an AP on the graph to select it and its primary channel. This highlights the area covered by the channel and lists the channel information above the graph. In the image below, the AP named "Technico:54a65c-a2b35b" on channel 1 is selected.



- Double-tap the graph to zoom in or use "pinch" gestures with your thumb and forefinger. Tap the Restore icon or reverse the pinch gesture to return to the full graph. The image below shows a zoomed-in view with the AP named "Technico:54a65c-a2b35b" on channel 1 selected.



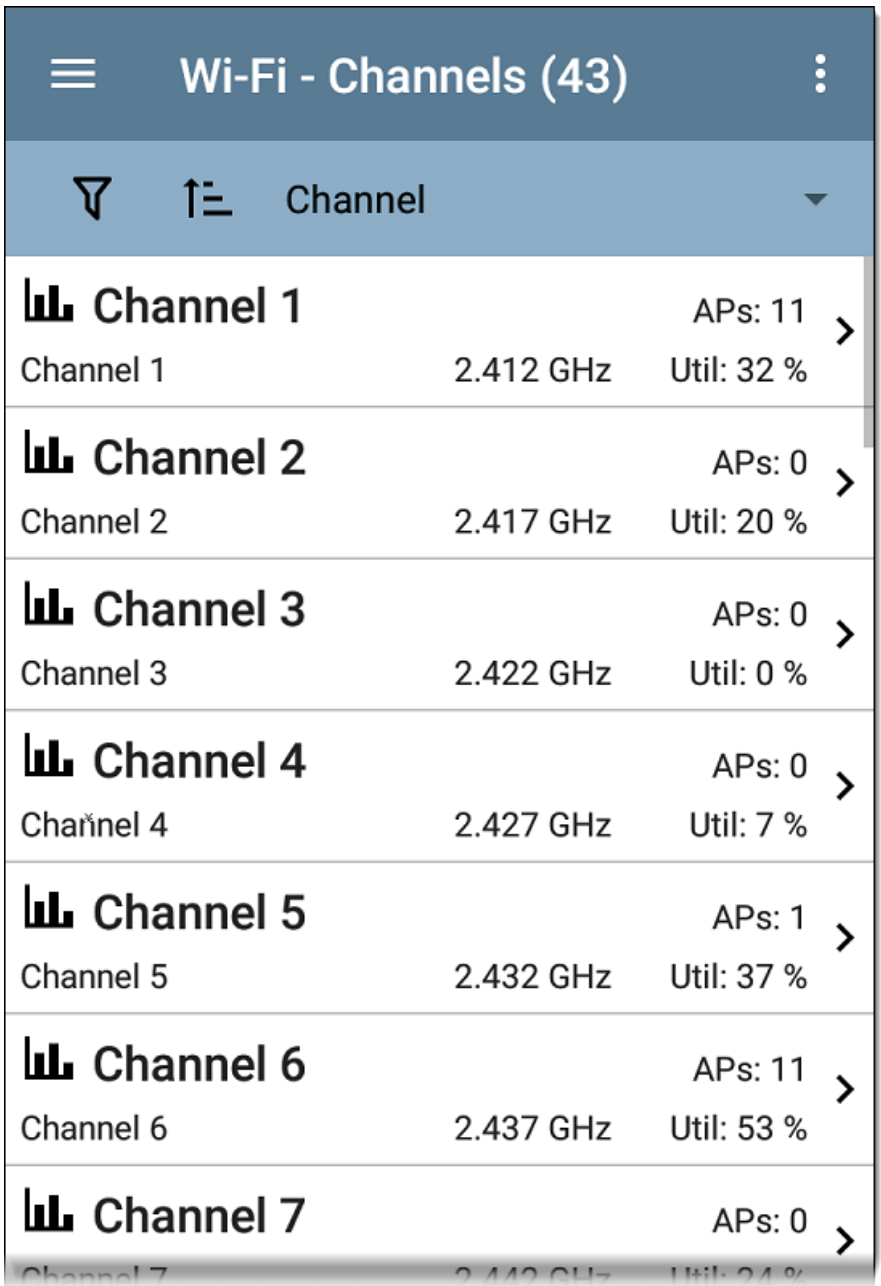
- Tap the **blue channel** selectors at the bottom to view a different Wi-Fi band (2.4, 5 and 6 GHz) and channel range on the graph.
- Tap the action overflow button ••• to open the AP Details or Channel Details screens for the selected AP or Channel or to open the Spectrum Test App.



See Filtering in the Wi-Fi App for an explanation of the Overlap screen's filtering options.

Channels

The Channels list screen displays the characteristics of the wireless Channels as they are scanned in your location.

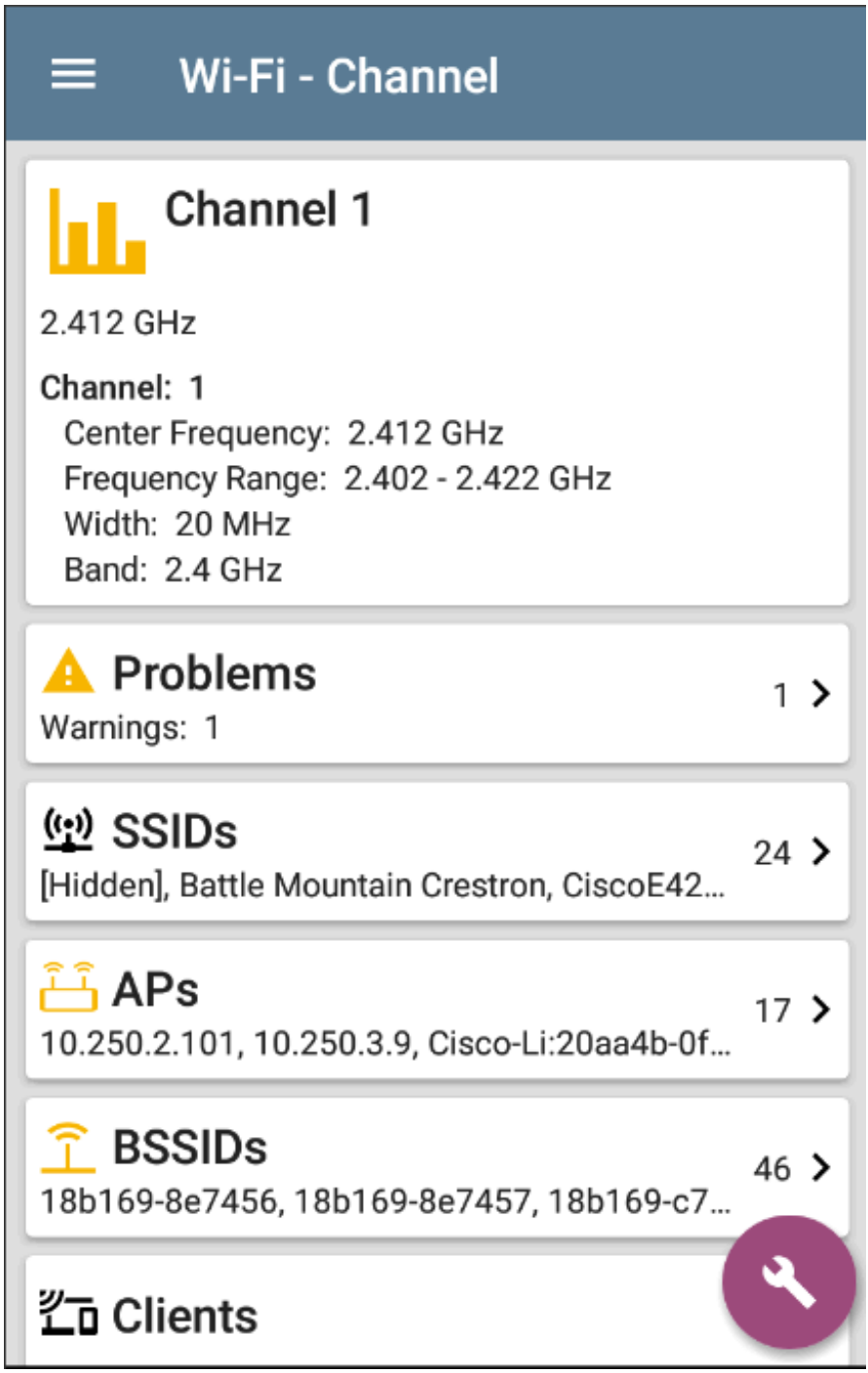


You can Filter  and Sort  the list to determine which Channels are shown and their order. Refer to the Wi-Fi App List Screens topic if needed.

By default, Channels are ordered by channel number, and each card shows the channel frequency, number of APs, and total Utilization percent.

Tap a Channel card to open the Channel Details screen.

Channel Details



The Channel Details screen displays the channel's Center Frequency under the icon,

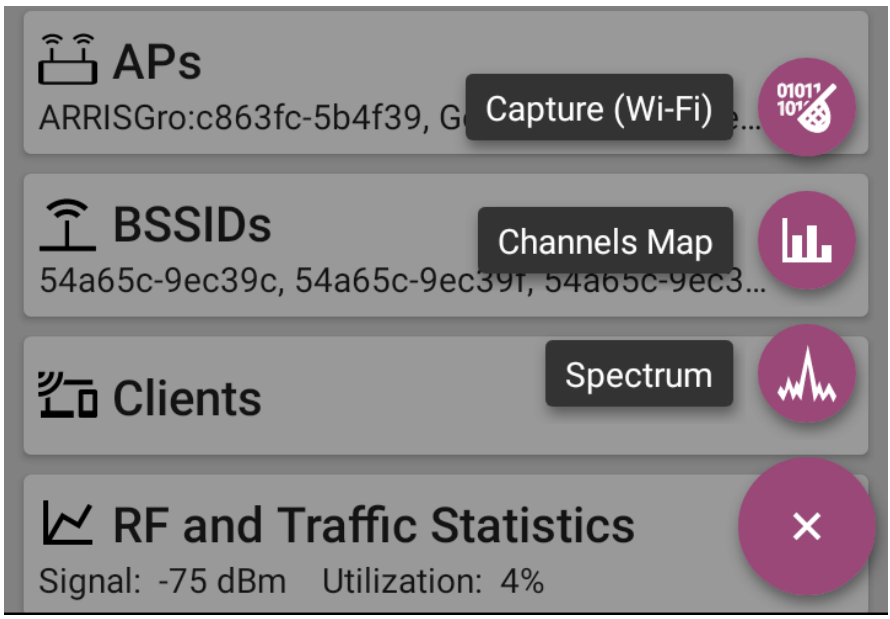
along with the Frequency Range, Width, and Band.

Dynamic Frequency Selection (DFS) channels also display an Attributes field that indicates DFS.

Channel RF and Traffic Statistics

The RF and Traffic Statistics card appears when there is an active AP and Utilization on the channel. See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic.

Channel FAB

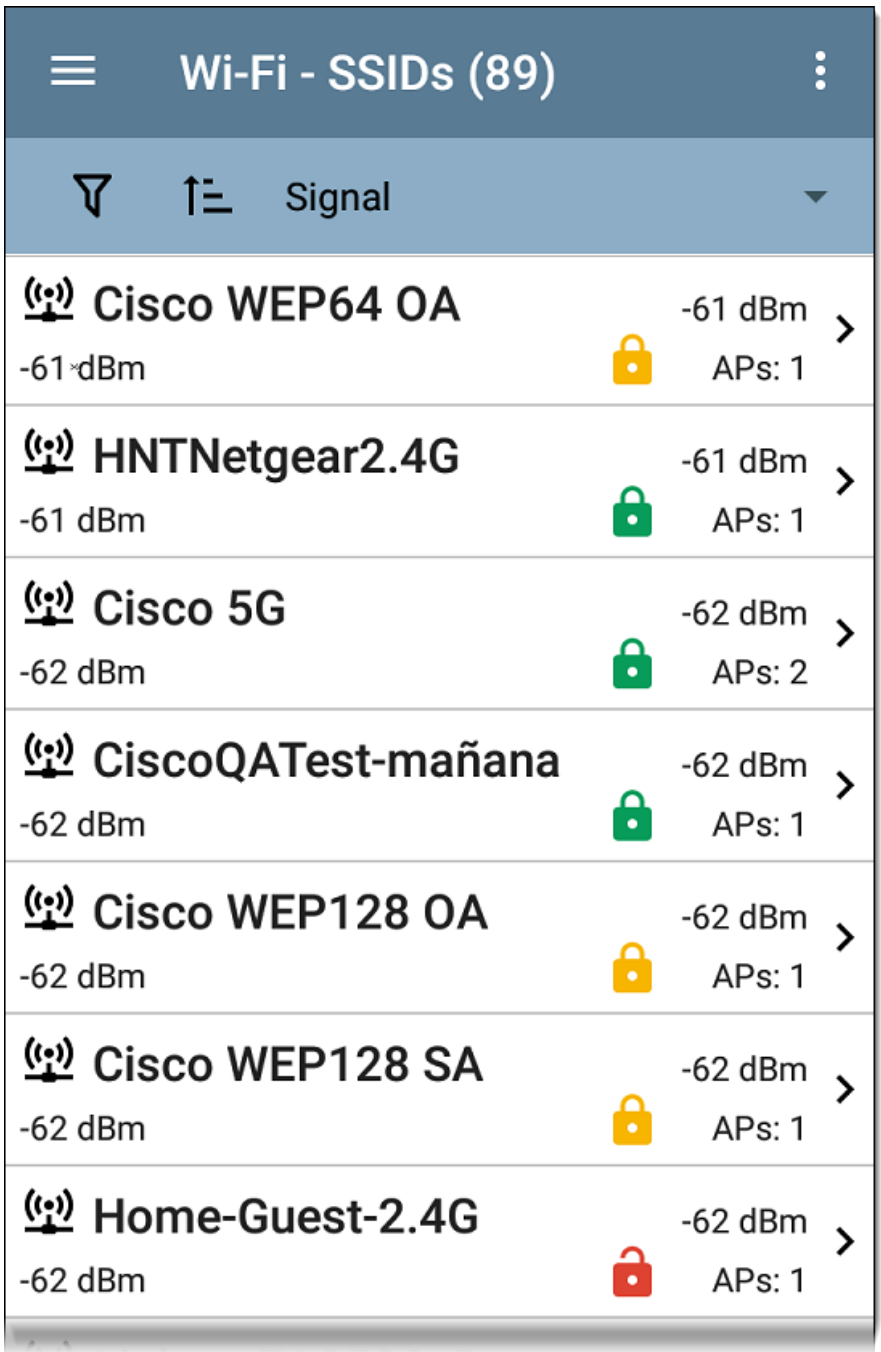


Tap the FAB on the Channel Details screen to:

- Open the Capture app to record a packet capture on the channel.
- Open the Channels Map screen with the current channel selected.
- Open the Spectrum app to view signal measurements for the channel.

SSIDs

The SSIDs list screen shows all the network SSIDs the EtherScope has discovered.



You can Filter  and Sort  the list to determine which SSIDs are shown and their order. Refer to the Wi-Fi App List Screens topic if needed.

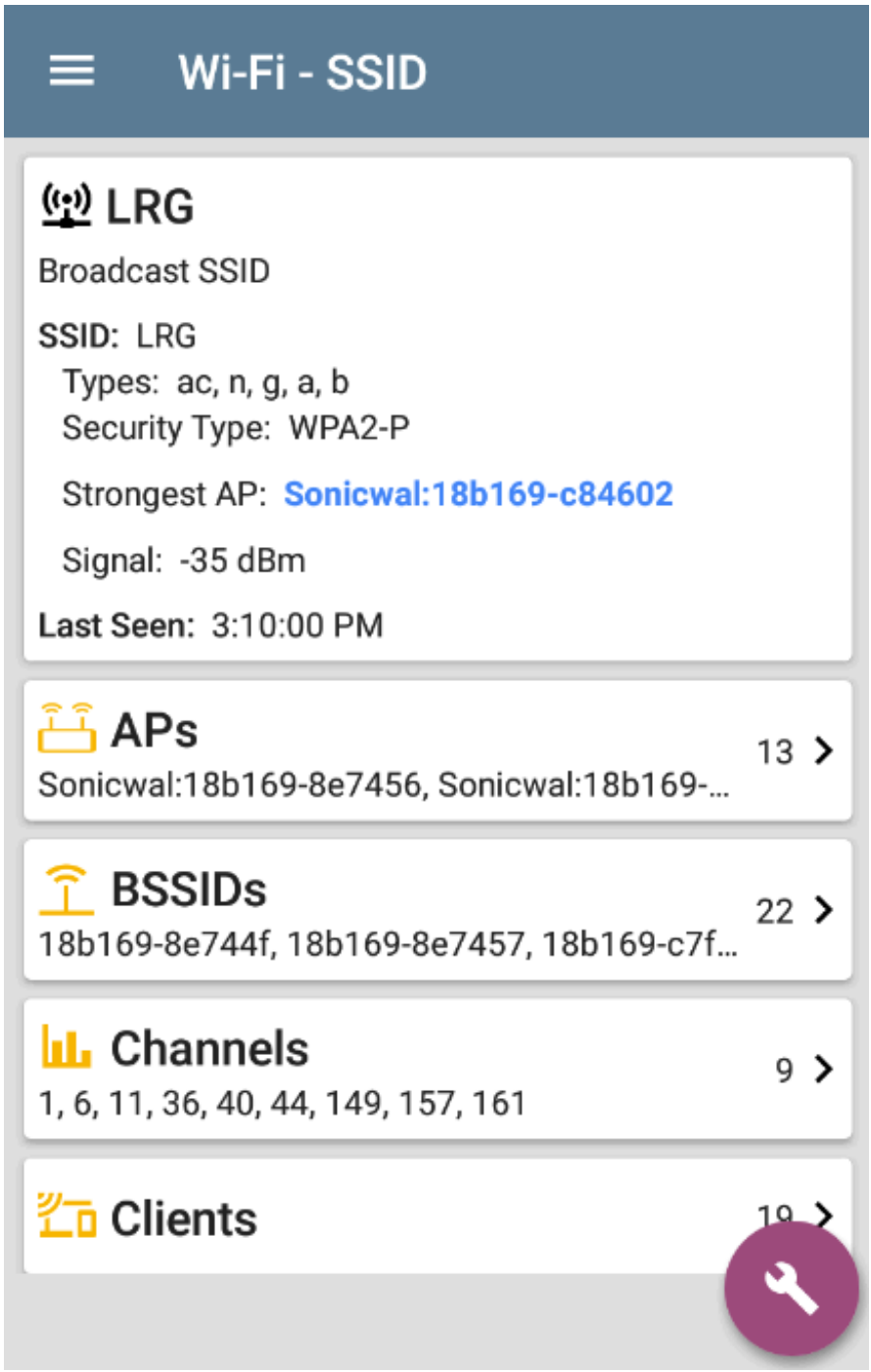
By default, SSIDs are ordered by Signal strength, and each card shows the network security status and number of APs on the network.

The security status icons have the following meanings:

- Green closed lock: All APs on the network use secure protocols, like WPA2 or WPA3.
- Yellow closed lock: One or more APs use WEP or Cisco LEAP protocols, which are less secure.
- Red open lock: The network does not have security enabled.

Tap a SSID card to open the SSID Details screen.

SSID Details



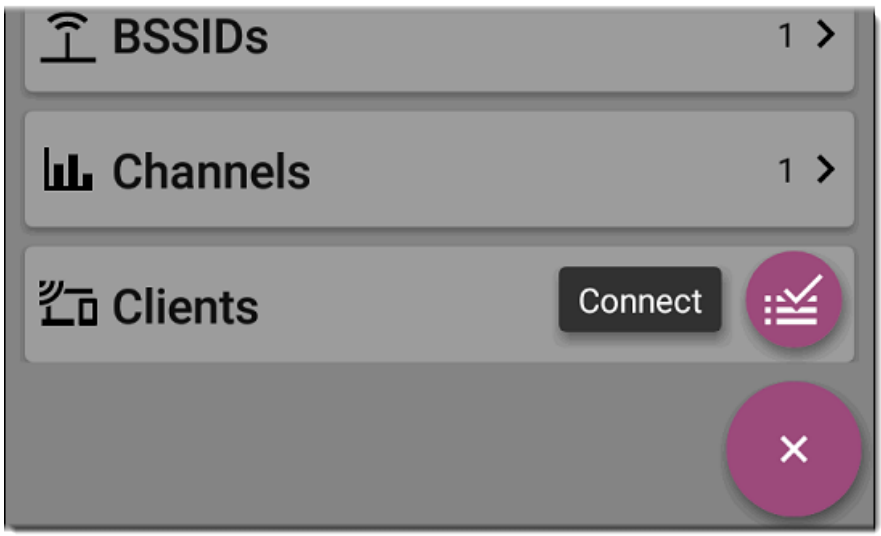
In addition to the Signal and Security Type, the SSID Details displays the AP on the network with the strongest signal, 802.11 Types that the APs in

the network support, and the time the EtherScope last detected activity on the network (Last Seen).

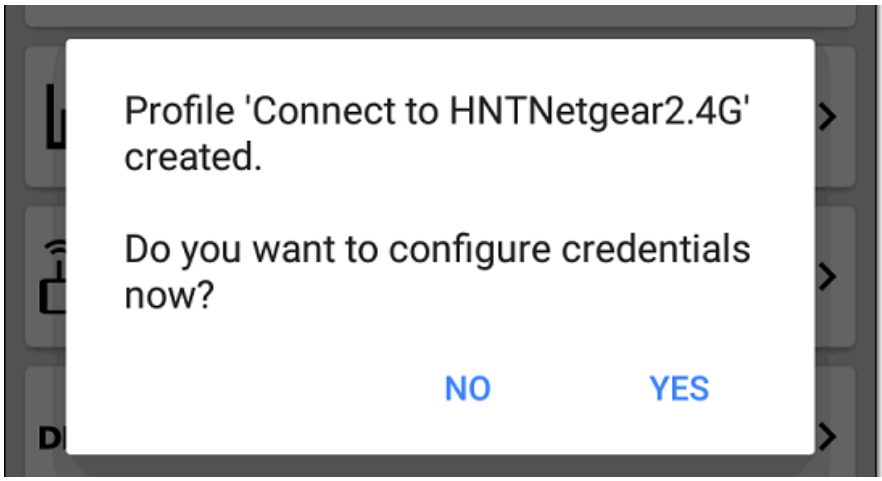
EtherScope nXG can detect and display 802.11 types a/b/g/n/ac/ax.

SSID FAB

Tap the FAB on the SSID Details screen to **Connect** to the network.



This action opens the AutoTest app and creates a new Wi-Fi profile called "Connect to [SSID]."

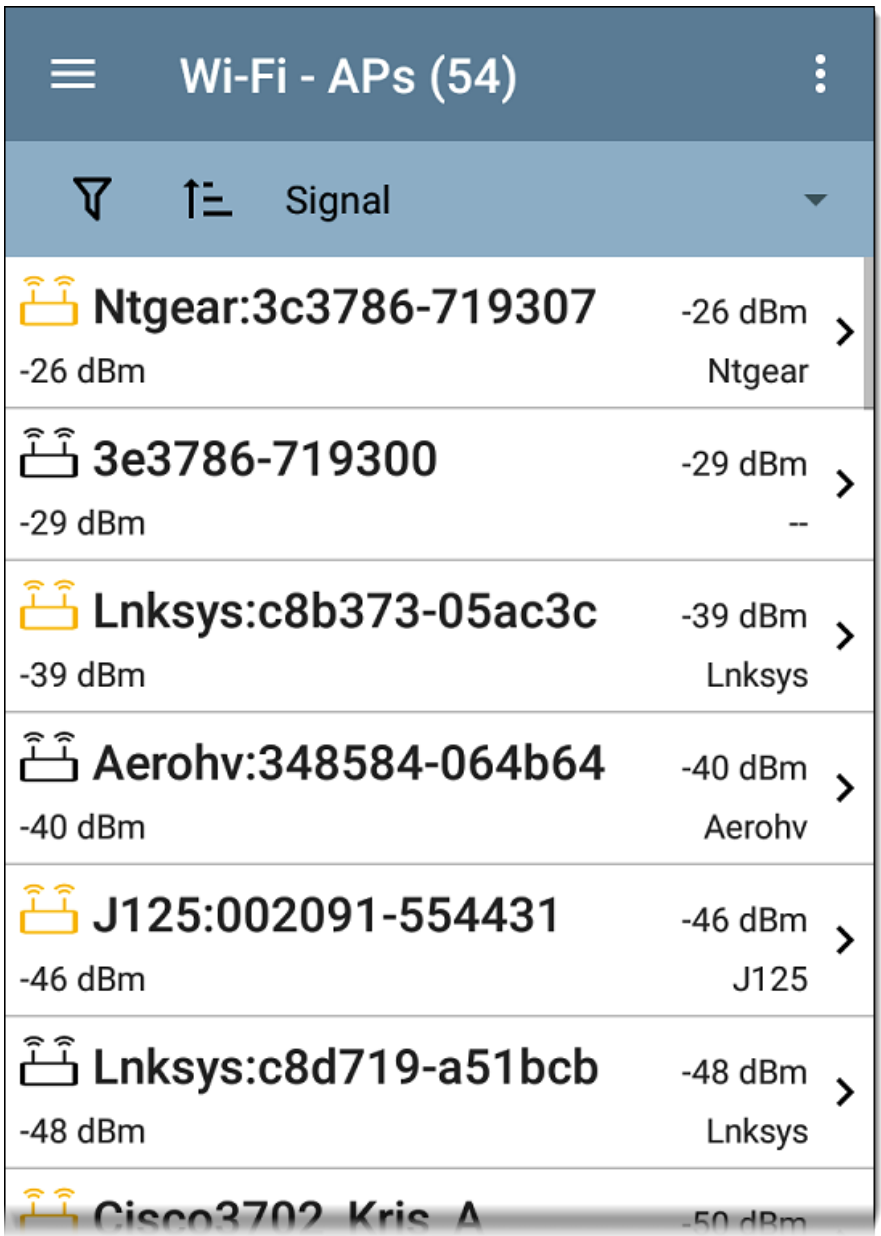


See Creating a Wi-Fi Profile from the Wi-Fi Analysis App in the AutoTest chapter for a more detailed description of this process.

Back to Title and Contents

APs

The APs list screen displays all the Access Points discovered operating on your wireless networks.



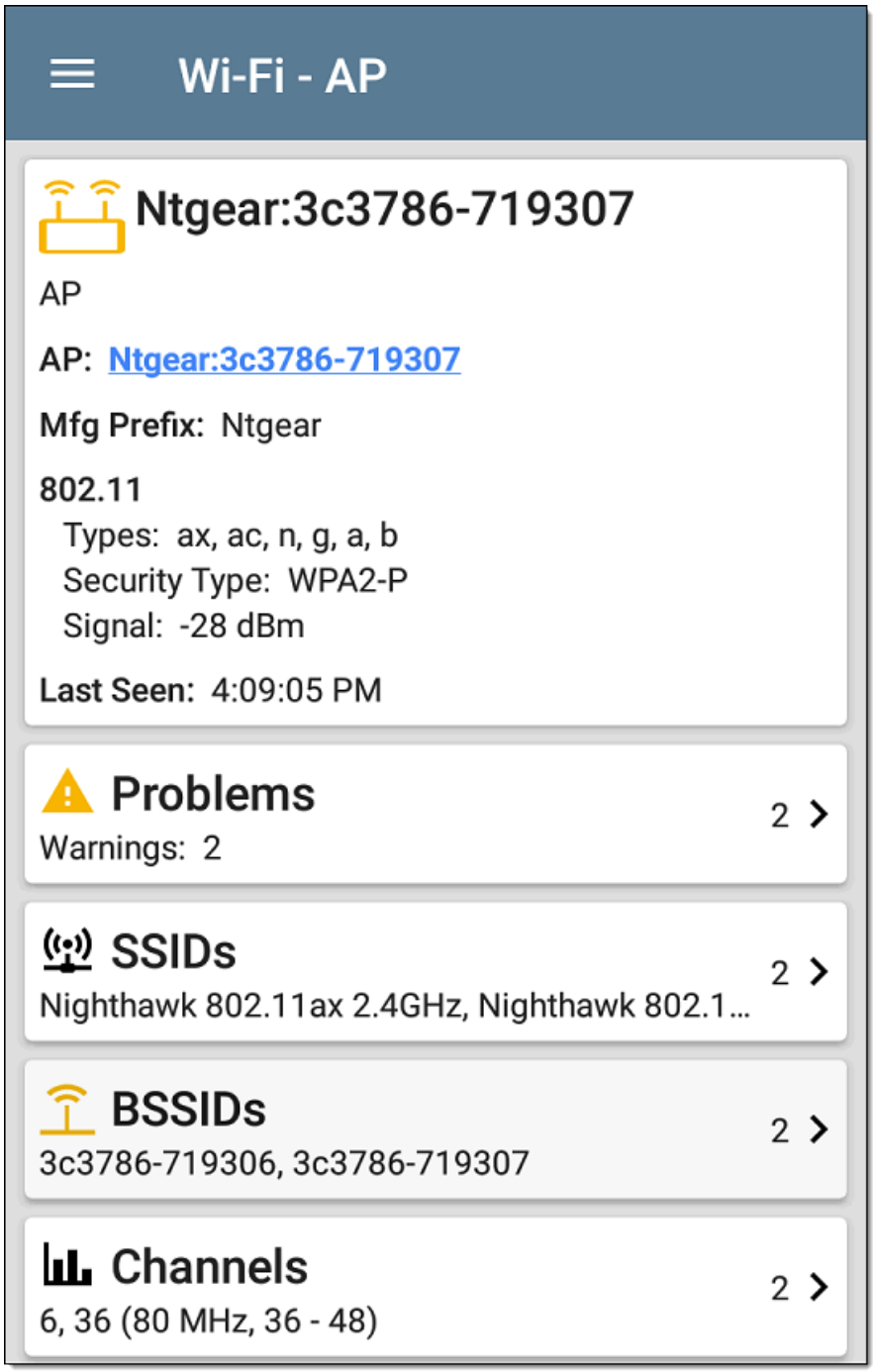
You can Filter and Sort the list to determine which APs are shown and their order.

Refer to the Wi-Fi App List Screens topic if needed.

By default, APs are ordered by Signal strength, and each card shows the Signal strength in dBm and the AP's manufacturer prefix.

Tap an individual AP's card to open the AP Details screen.

AP Details



The AP Details screen shows the 802.11 Types the AP supports, the AP's Security Type, and the

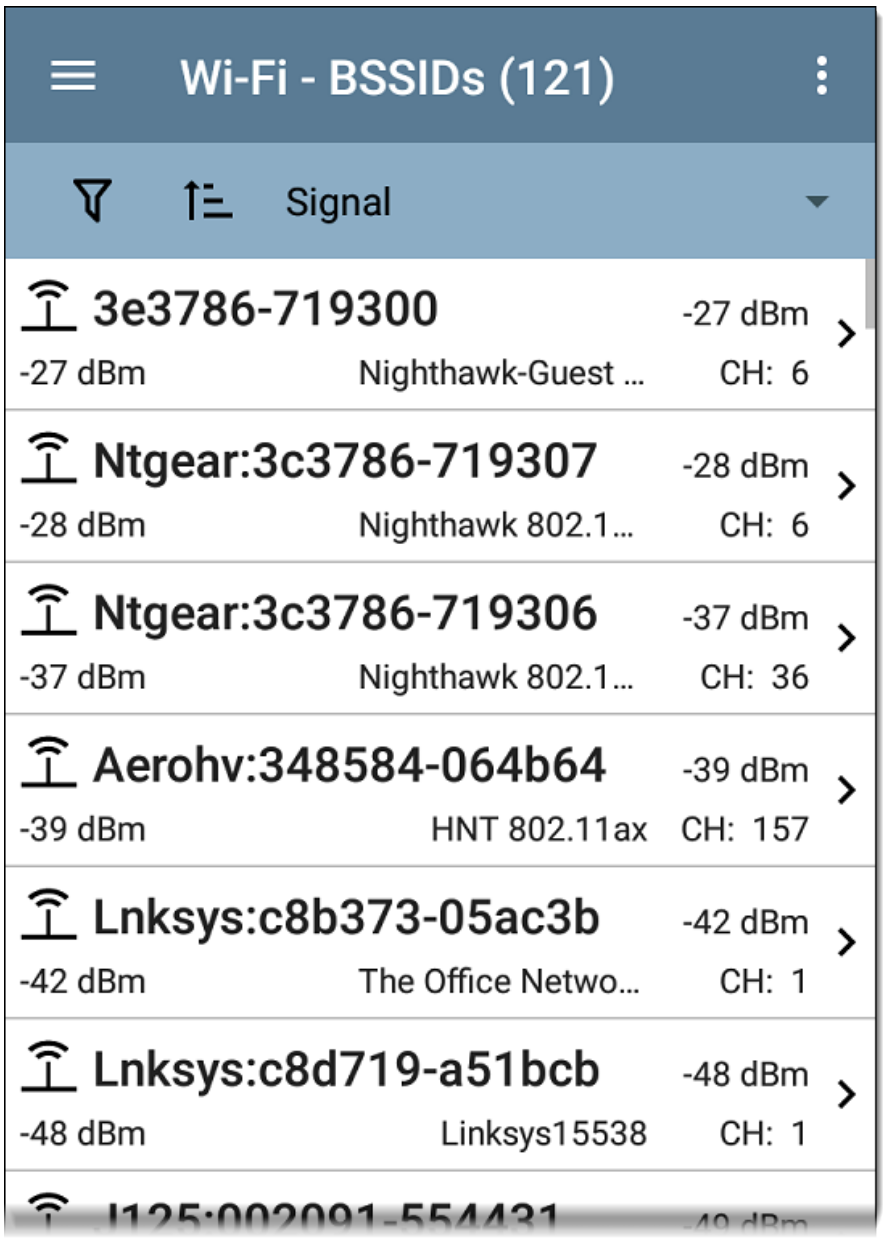
time the AP was last detected (Last Seen) by the EtherScope.

Tap the lower cards to view the network IDs, Channels, and Clients associated with the AP.

See Wi-Fi Problems for more information about the Problems card.

BSSIDs

The BSSIDs list screen shows the BSSID addresses discovered in your wireless environment.



You can Filter and Sort the list to determine which BSSIDs are shown and their order. Refer to the Wi-Fi App List Screens topic if needed.

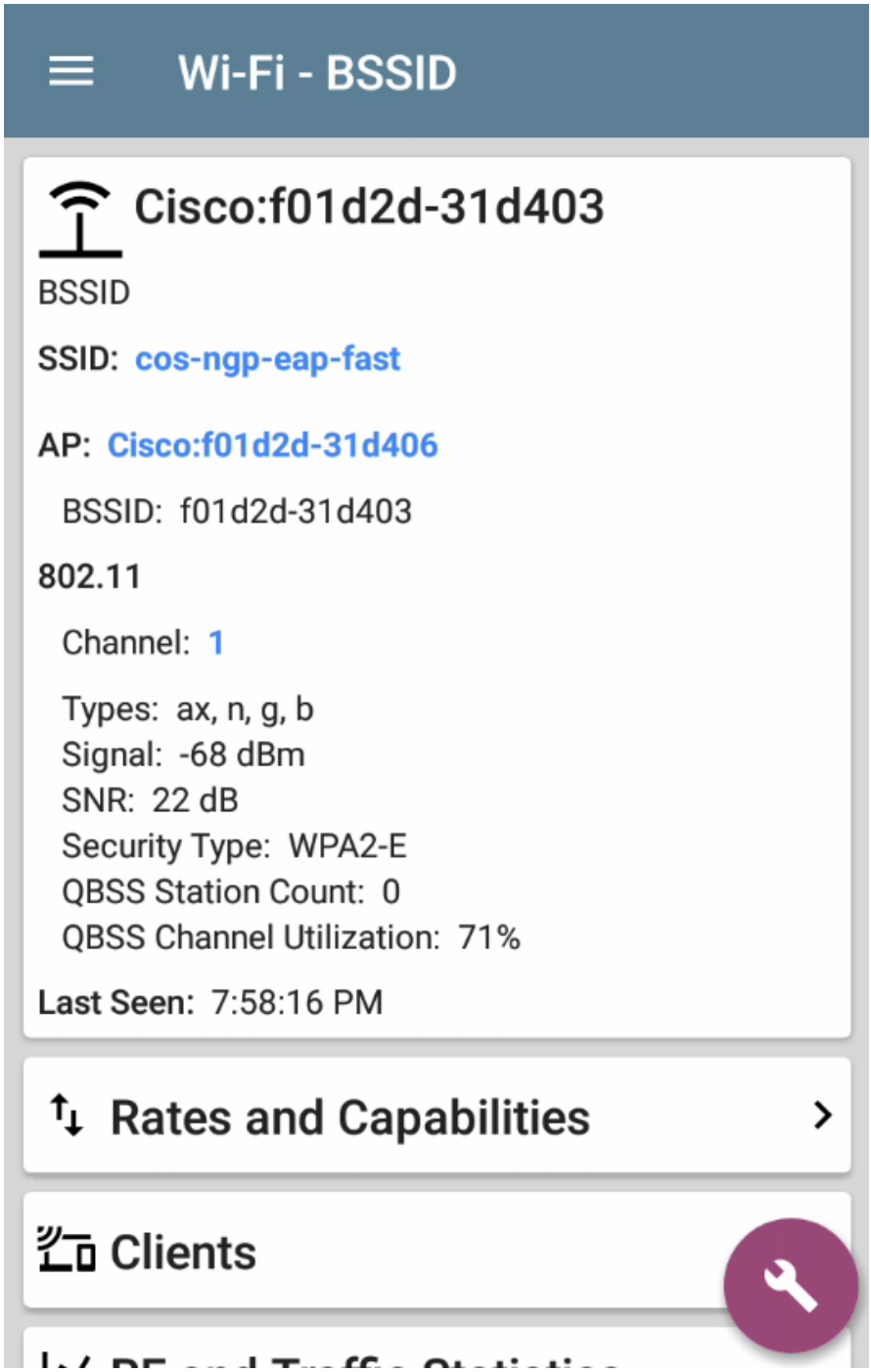
By default, BSSIDs are ordered by signal strength, and each card shows the signal strength, SSID, and channel number on which the BSSID operates. The icons indicate different types of BSSID:

	Single, transmitted
	Reduced neighbor report, transmitted
	Reduced neighbor report, non-transmitted
	Multiple, transmitted (6 GHz)
	Multiple, non-transmitted (6 GHz)

Colors show the BSSID's status: black indicates normal status, **yellow** indicates a warning-level problem, and **red** indicates an error-level problem.

Tap a BSSID's card to open the Details screen.

BSSID Details



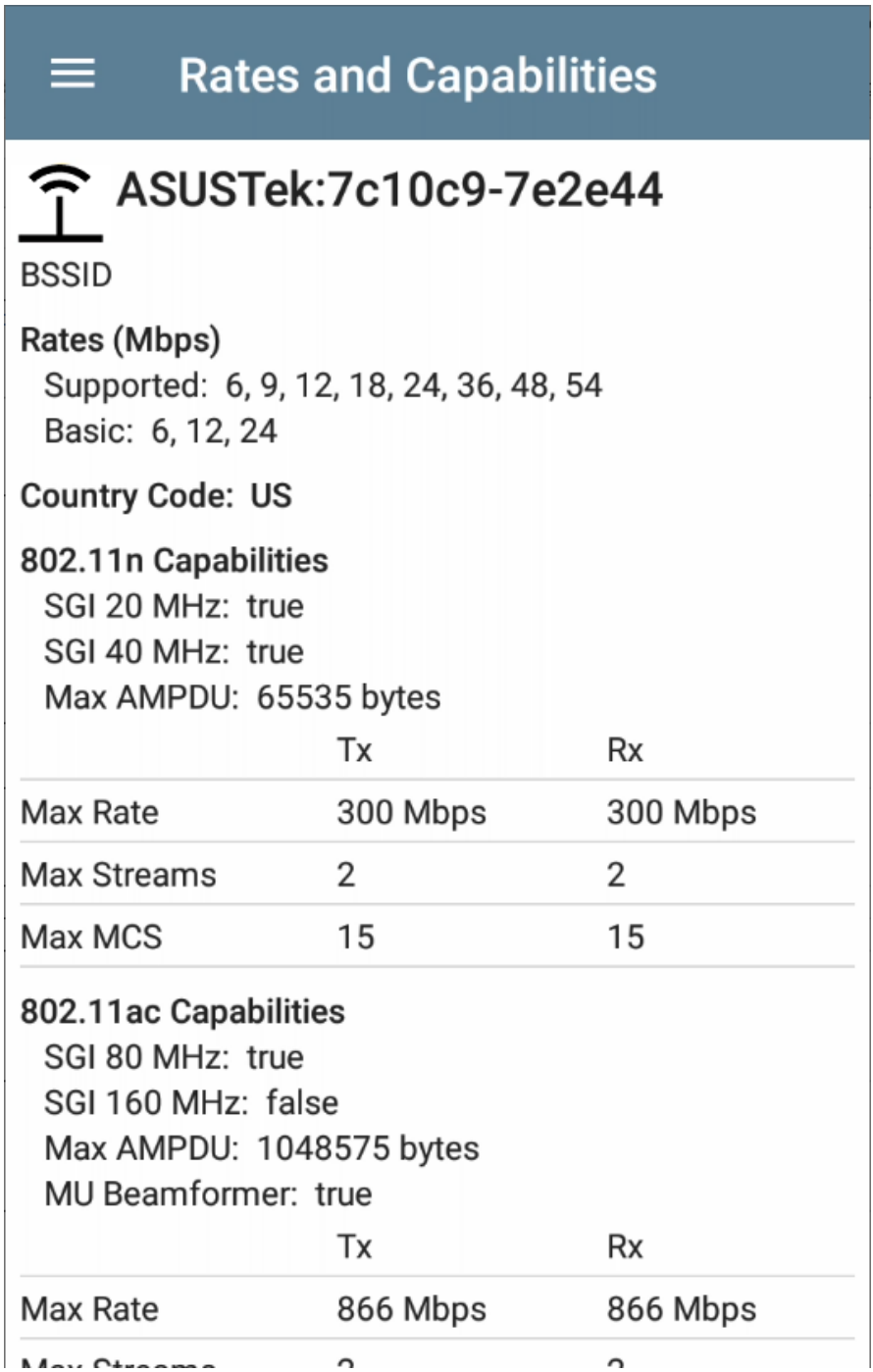
In addition to the characteristics on the BSSID cards, the Details screen displays the following information:

- User-assigned Authorization status (if set)
- Supported **802.11 Types**
- Signal-to-Noise ratio (**SNR**) measurement
- Network **Security** type
- QBSS station count and channel utilization
- Time activity was **Last Seen** on the BSSID

BSSID Details also includes cards that link to Rates and Capabilities details, the Wi-Fi Clients list, and BSSID RF and Traffic Statistics details.

Rates and Capabilities

Tap the Rates and Capabilities card to open the full screen.



This screen shows advanced information about the transmit and receive rates and 802.11 capabilities reported by the beacon.

Rates (Mbps)

Supported: The extended physical (PHY) rates that the AP is configured to support

Basic: The basic physical (PHY) rates that the AP is configured to support

Country Code

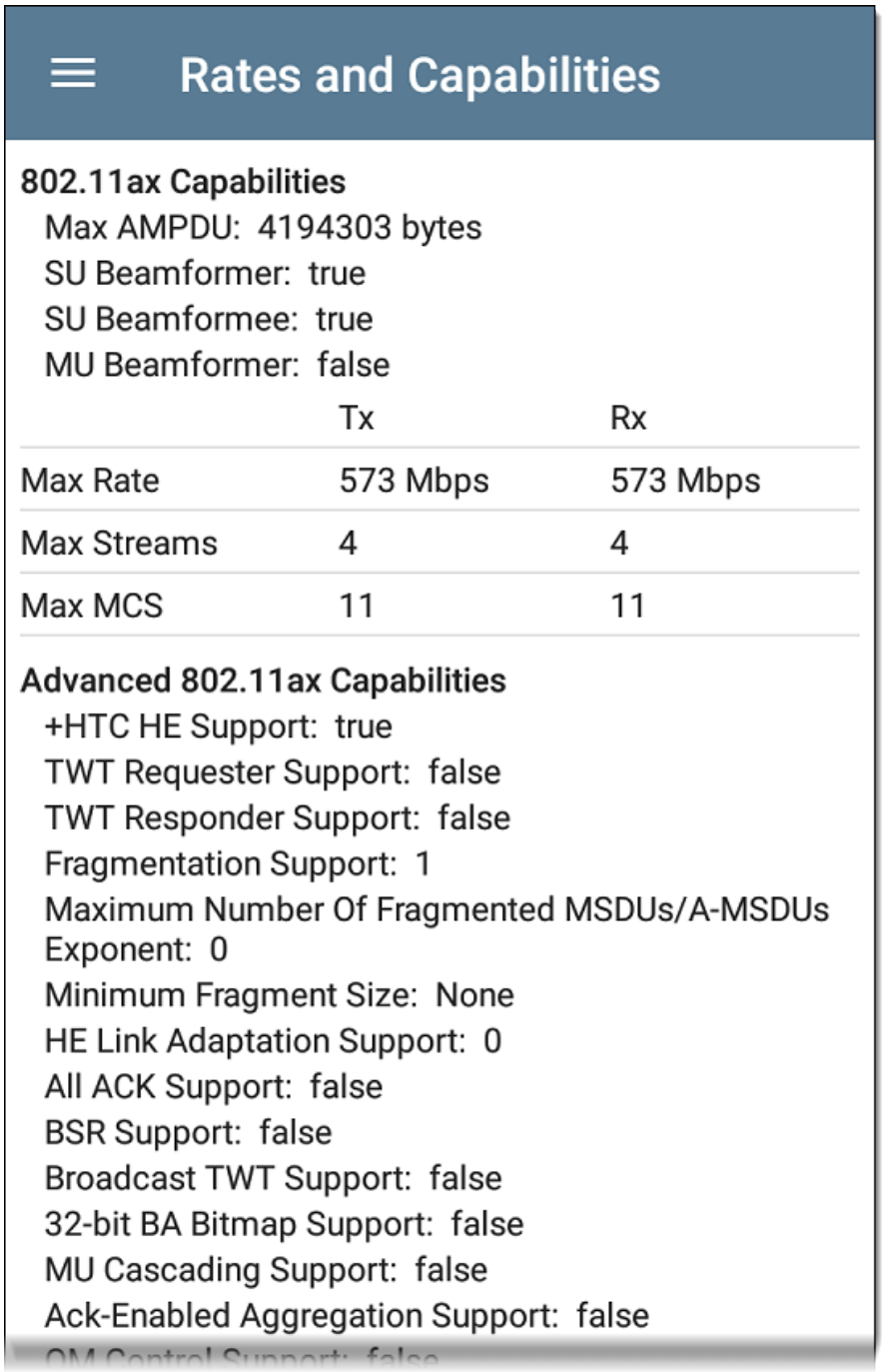
The 802.11d country code as detected for the country in which you use your device.

802.11 Capabilities

- 802.11n capabilities are gathered from HT capabilities in the beacon.
- 802.11ac capabilities are gathered from VHT capabilities in the beacon.
- 802.11ax capabilities are gathered from HE capabilities in the beacon.

802.11ax Rates and Capabilities

EtherScope nXG can also report Advanced 802.11ax (Wi-Fi 6) capabilities it sees in the beacon.



Clients

Tap the **Clients** card to open the Wi-Fi Clients list screen.

BSSID RF and Traffic Statistics

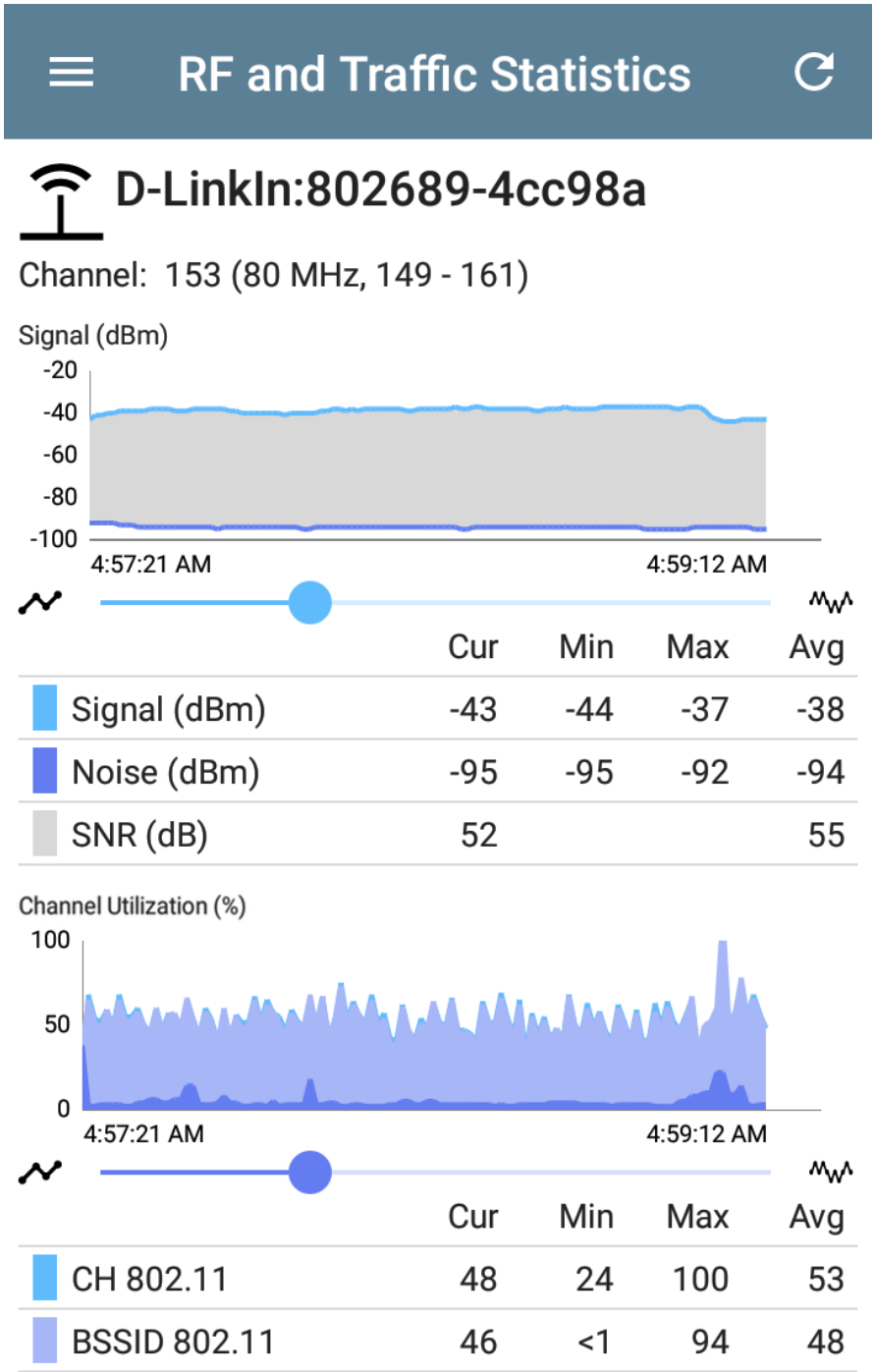
Tap the **RF and Traffic Statistics** card to open the RF and Traffic Statistics screen. This screen displays the BSSID and channel number at the top of the screen as well as informational graphs.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider under each graph. Tap the Restore icon to return to the full graph. (See the Trending Graphs topic for an overview of the graph controls.)

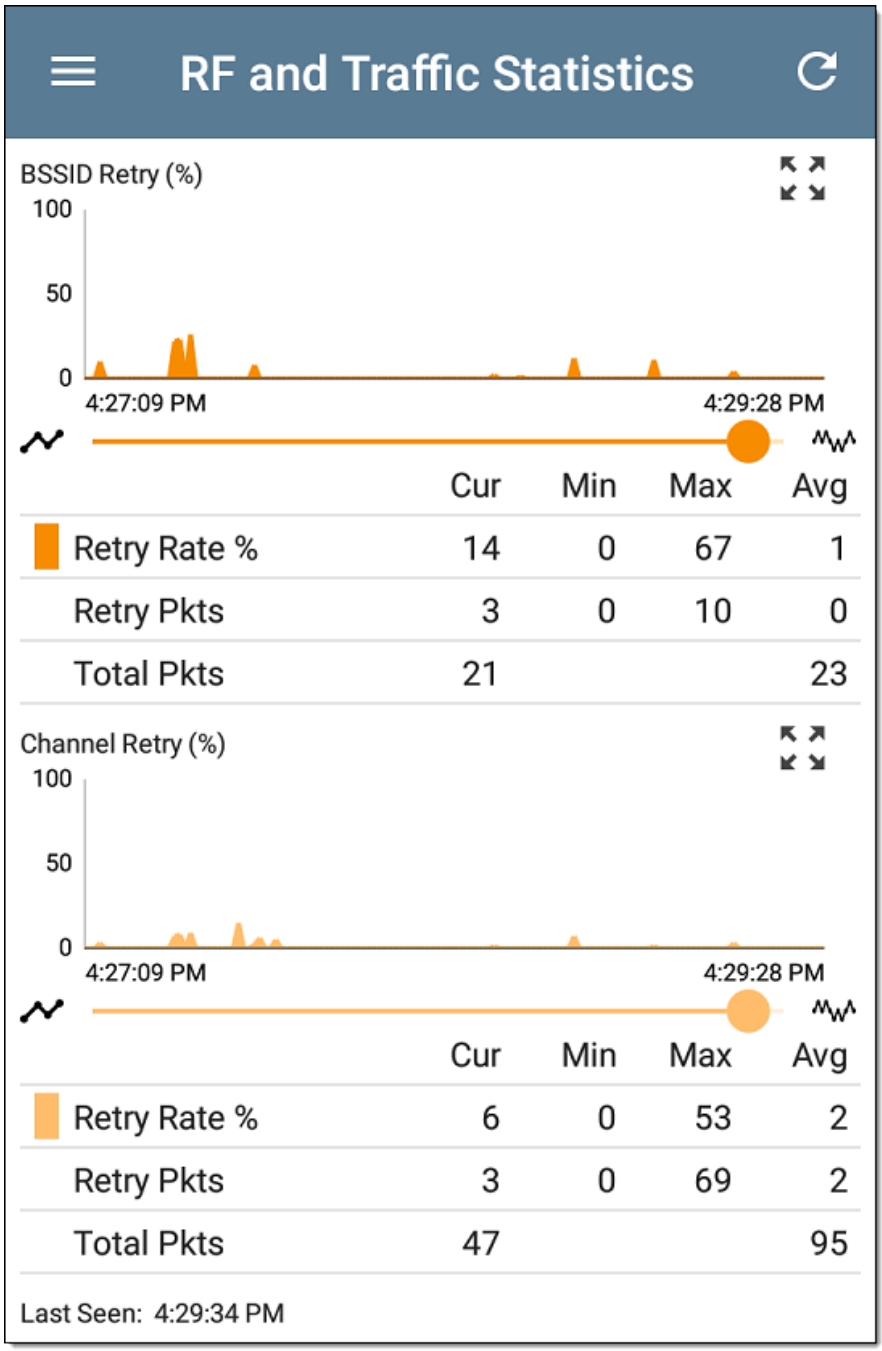
See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.

The Signal graph shows the signal in light blue, noise in dark blue, and a calculated SNR.

The Channel Utilization graph uses light blue to show 802.11 channel utilization and dark blue to show non-802.11 utilization:



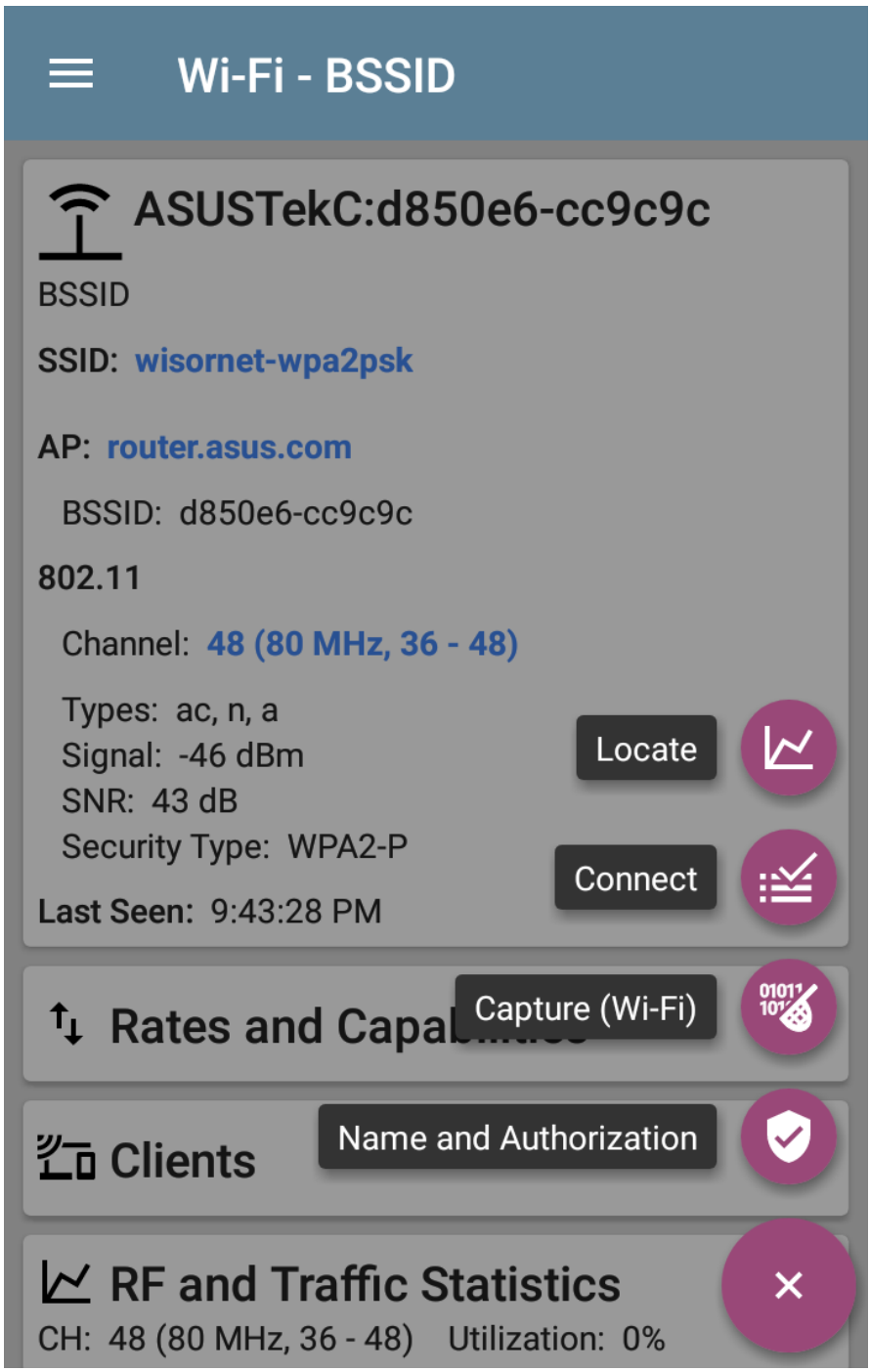
The screen also displays separate graphs for BSSID Retries and Channel Retries:



BSSID FAB

The floating action button on the BSSID screen lets you **Locate** the wireless device, **Connect** to the BSSID, record a packet **Capture** of the

network traffic with the current BSSID on the connected channel, and assign or change its **Name and Authorization**.

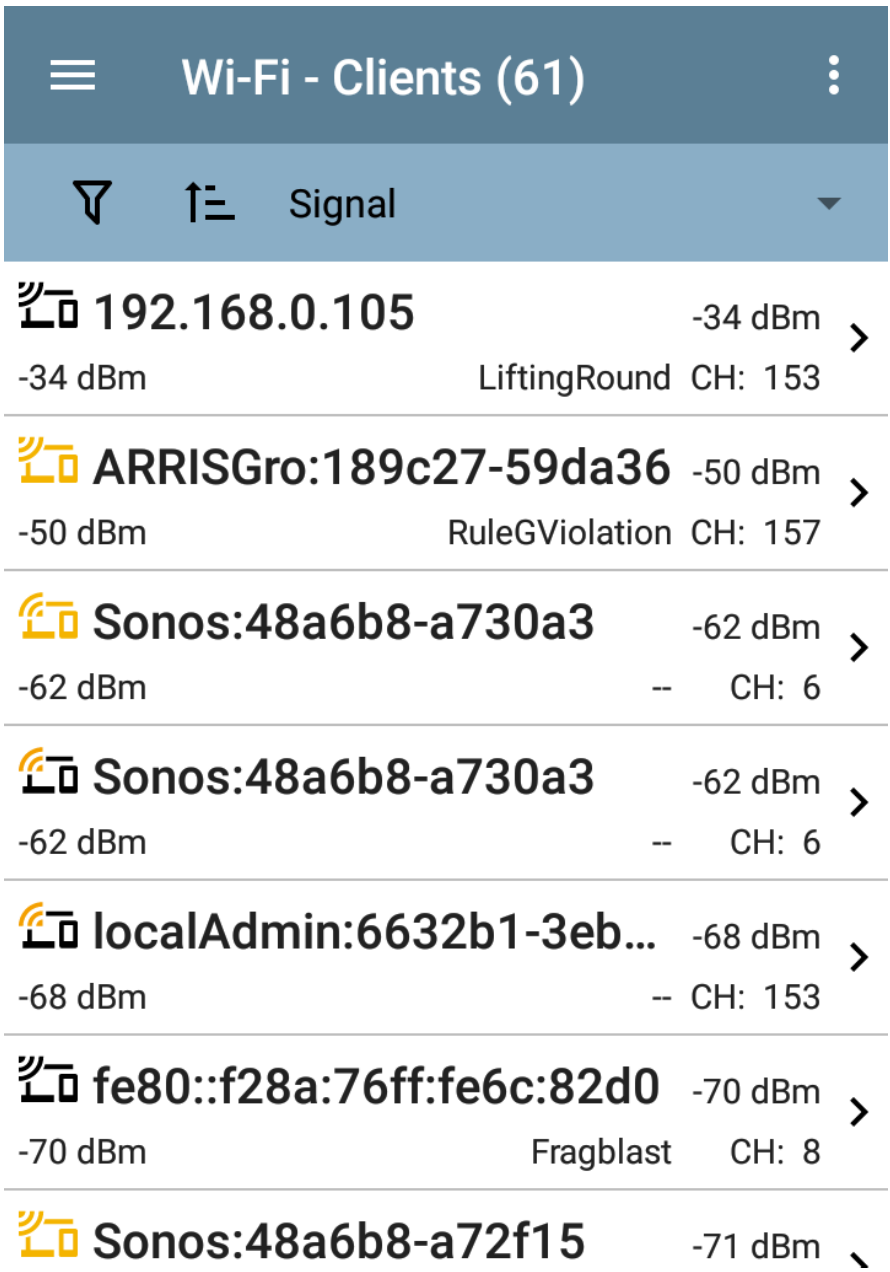


- Selecting **Locate** opens the Locate BSSID screen. See Locating Wi-Fi Devices.
- Tapping **Connect** opens the AutoTest app and creates a new Wi-Fi profile called "Connect to [BSSID]." See Creating a Wi-Fi Profile from the Wi-Fi Analysis App in the AutoTest chapter for a more detailed description of this process.
- Selecting **Capture** opens the Capture app populated with the Channel and BSSID. See the Capture app chapter.
- Selecting **Name and Authorization** opens the Name and Authorization dialog. See Assigning a Name and Authorization to a Device.

Back to Title and Contents

Clients

The Clients list screen displays the wireless clients the EtherScope has discovered connected to your wireless networks.



You can Filter and Sort the list to determine which Clients are shown and their order. Refer to the Wi-Fi App List Screens topic if needed.

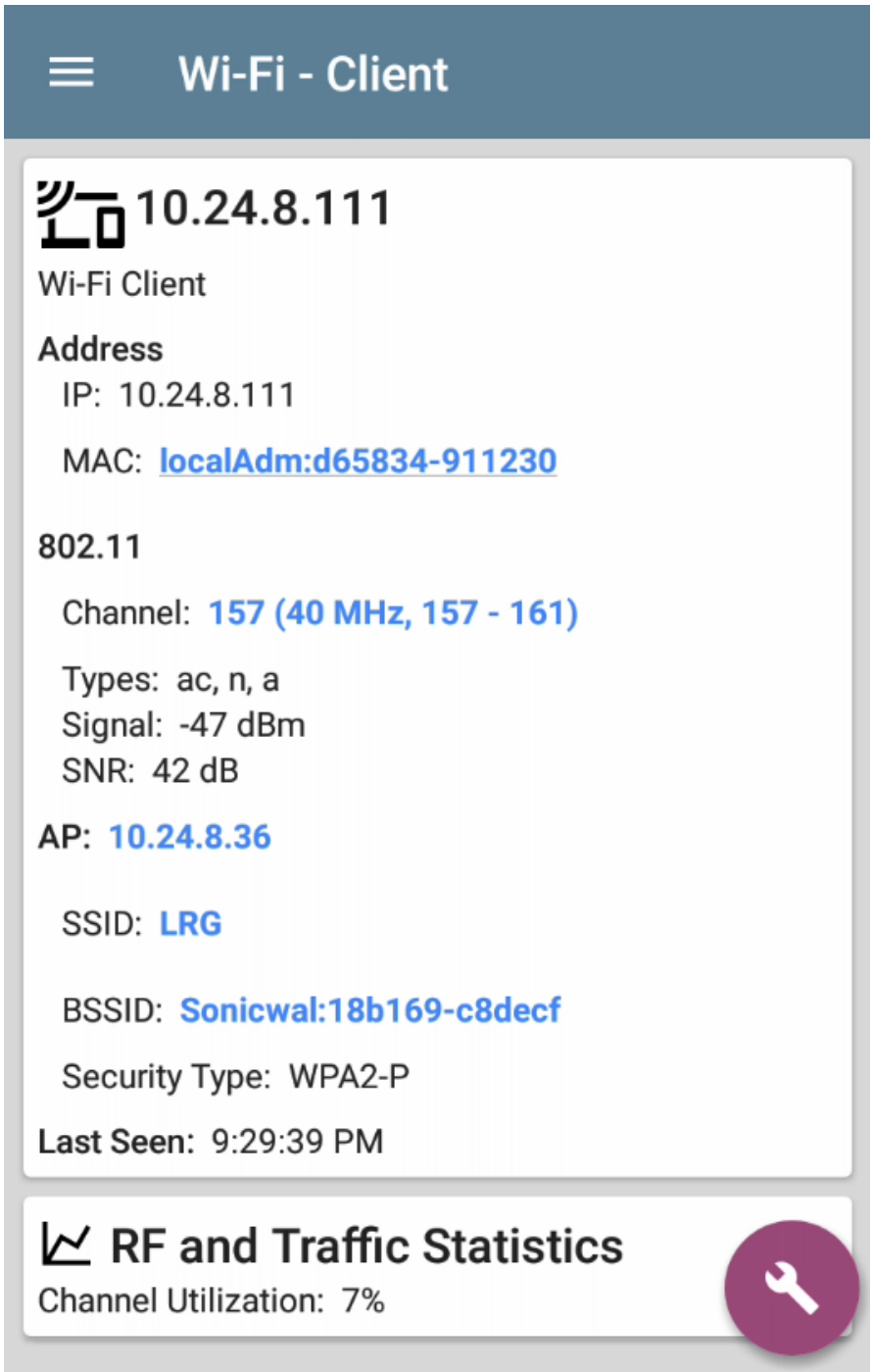
By default, the Clients are ordered by Signal strength, and each card shows the client's Signal strength in dBm, the SSID of the network to which the client is connected, and the channel number on which the Client is operating.

The general Client icons indicate whether the device is Probing or Connected to a network and able to receive data. If a Client is probing, two dashes -- display where the SSID would appear.

The Clients screen also shows specific icons for NetAlly testers, like the EtherScope icon shown in the image above.

Tap a Client's card to open the Details screen.

Client Details



The top Client Details card for a connected Client displays the following information:

- Client's **IP** and **MAC** addresses.
- User-assigned **Authorization** status (if set)
- Supported **802.11** media **Types**
- Signal-to-Noise ratio (**SNR**) measurement
- Name of the **AP** to which the Client is connected
- **SSID** of the network to which the Client is connected
- **BSSID** on which the Client is operating
- Network **Security** type
- Time the Client was **Last Seen** by the Ether-Scope

Probing Clients

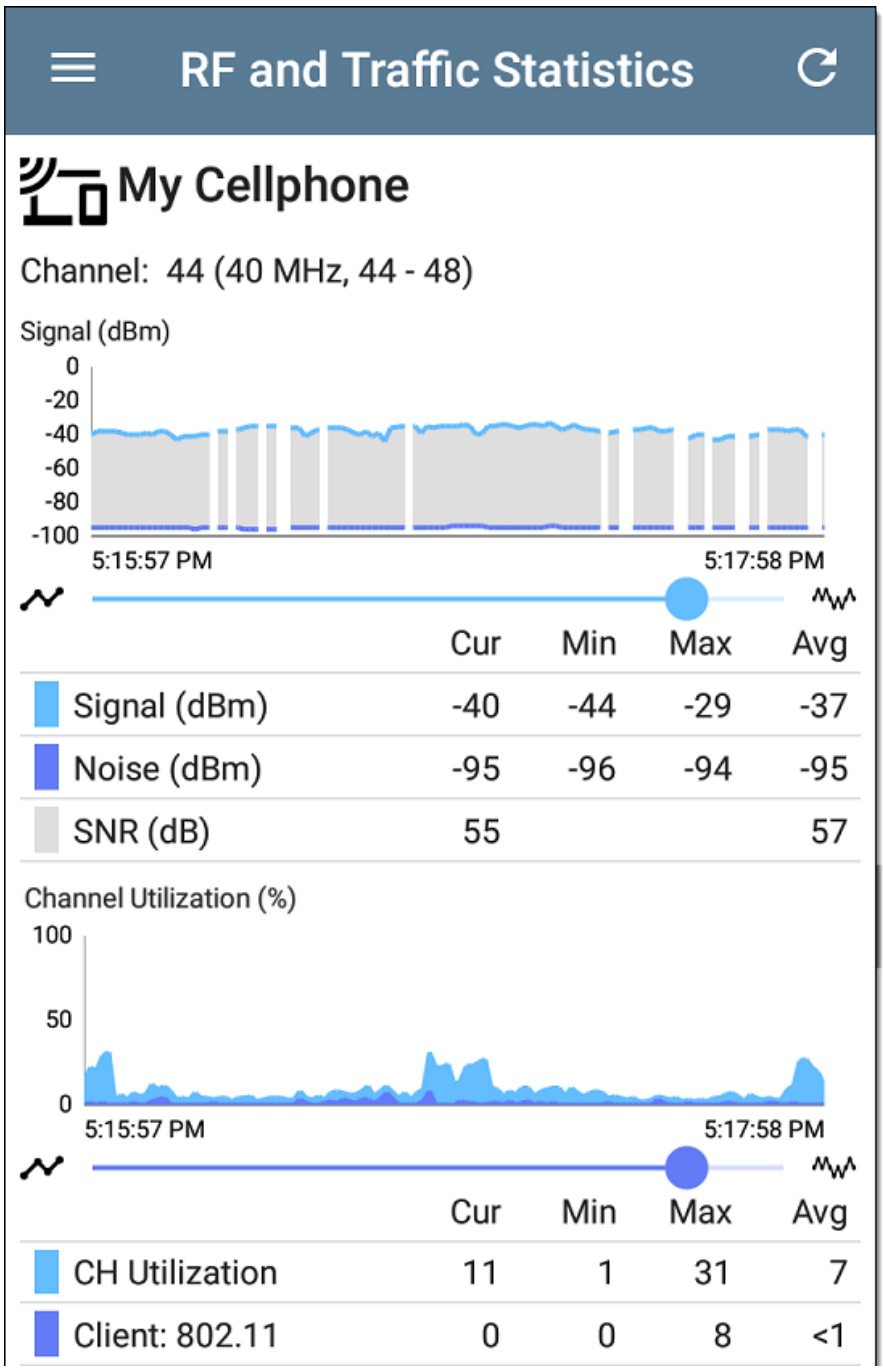
If the client is a Wi-Fi probing client, the details screen replaces AP details with a list of the SSIDs for which the client is probing in the **Probes For** field:

Client RF and Traffic Statistics

Tap the **RF and Traffic Statistics** card to open the RF and Traffic Statistics screen. This screen displays the client's ID or address and channel number at the top of the screen as well as informational graphs.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider under each graph. Tap the Restore icon to return to the full graph. (See the Trending Graphs topic for an overview of the graph controls.)

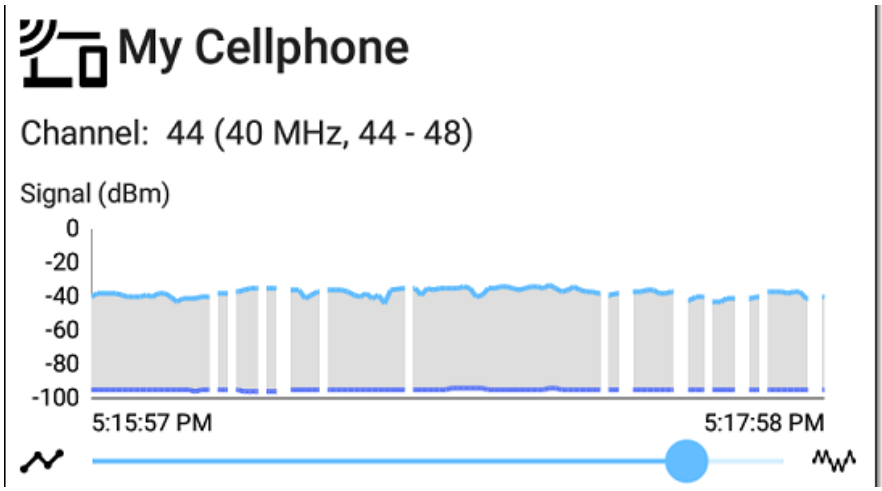
See RF and Traffic Statistics Overview in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.



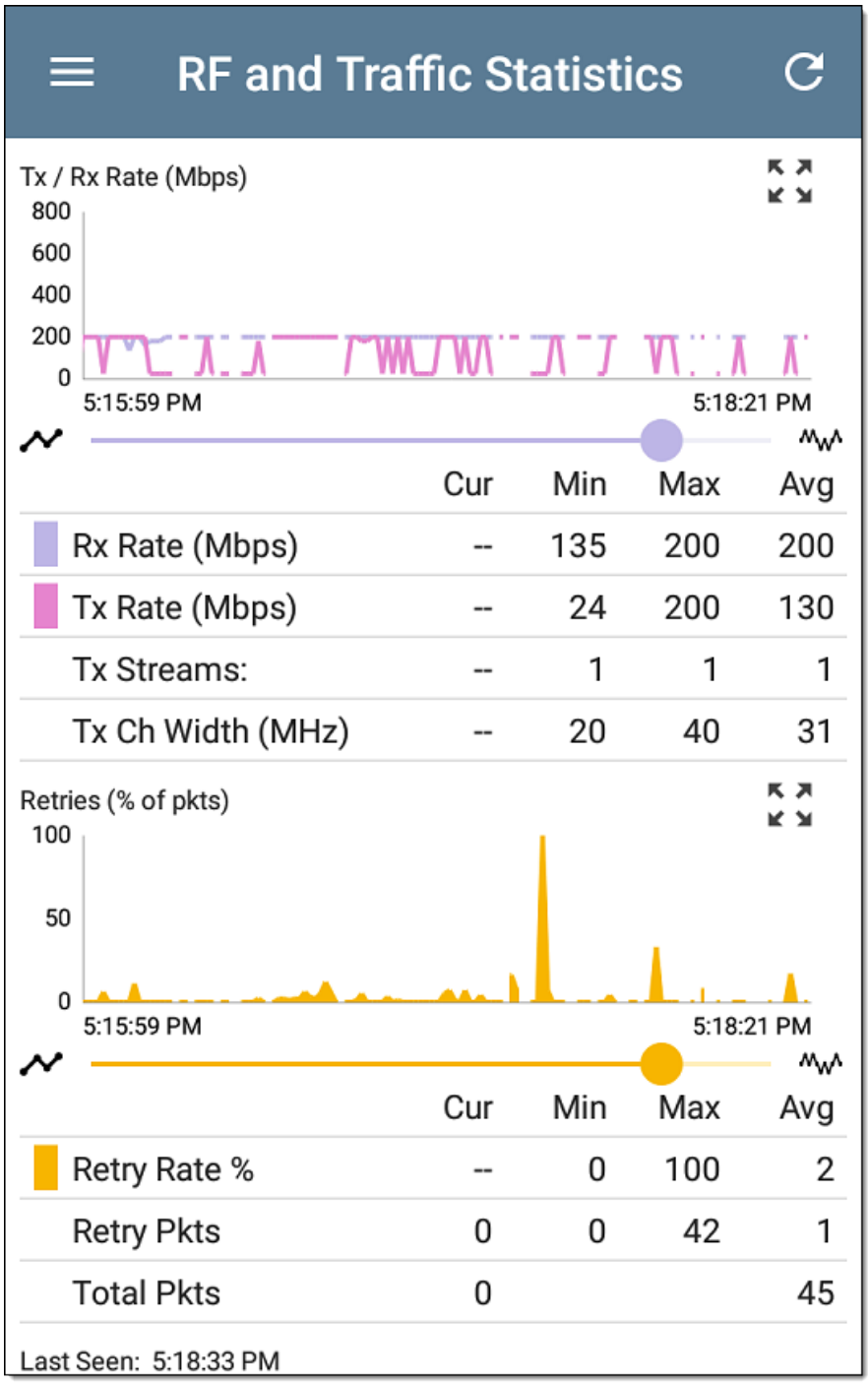
The Signal graph shows the signal in light blue, noise in dark blue, and a calculated SNR.

The Channel Utilization graph uses light blue to show 802.11 channel utilization and dark blue to show non-802.11 utilization:

Breaks in the Client RF and Traffic graphs may occur if the Client is not consistently transmitting, so there is no data for EtherScope to display during those times.



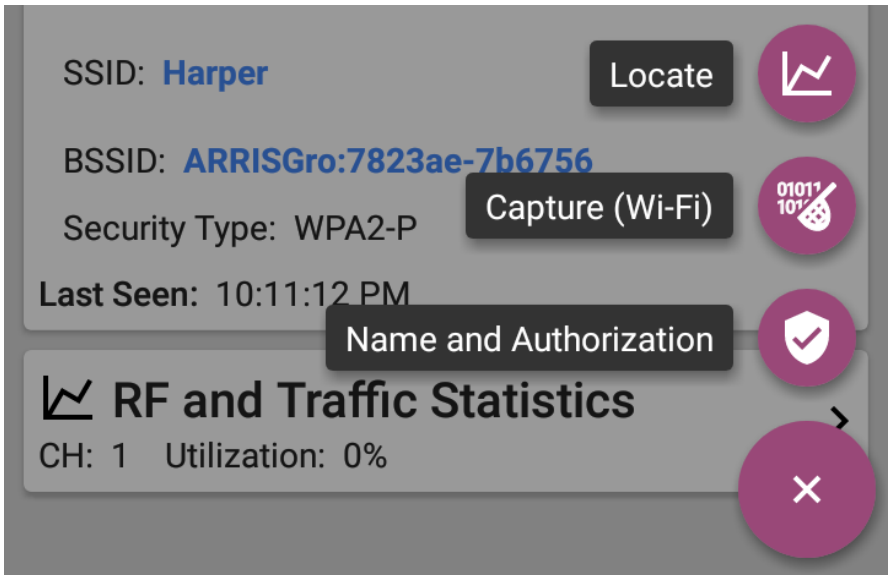
The Clients RF and Traffic Statistics screen also displays a graph of Transmit (Tx) and Receive (Rx) Rates in Mbps, number of Tx Streams, and Tx Channel Width in MHz.



Clients FAB

Tap the FAB on the Client Details screen to **Locate** the client device, to open the **Capture** app to record a packet capture of traffic going to

and from the client, or to assign or change its **Name and Authorization**.



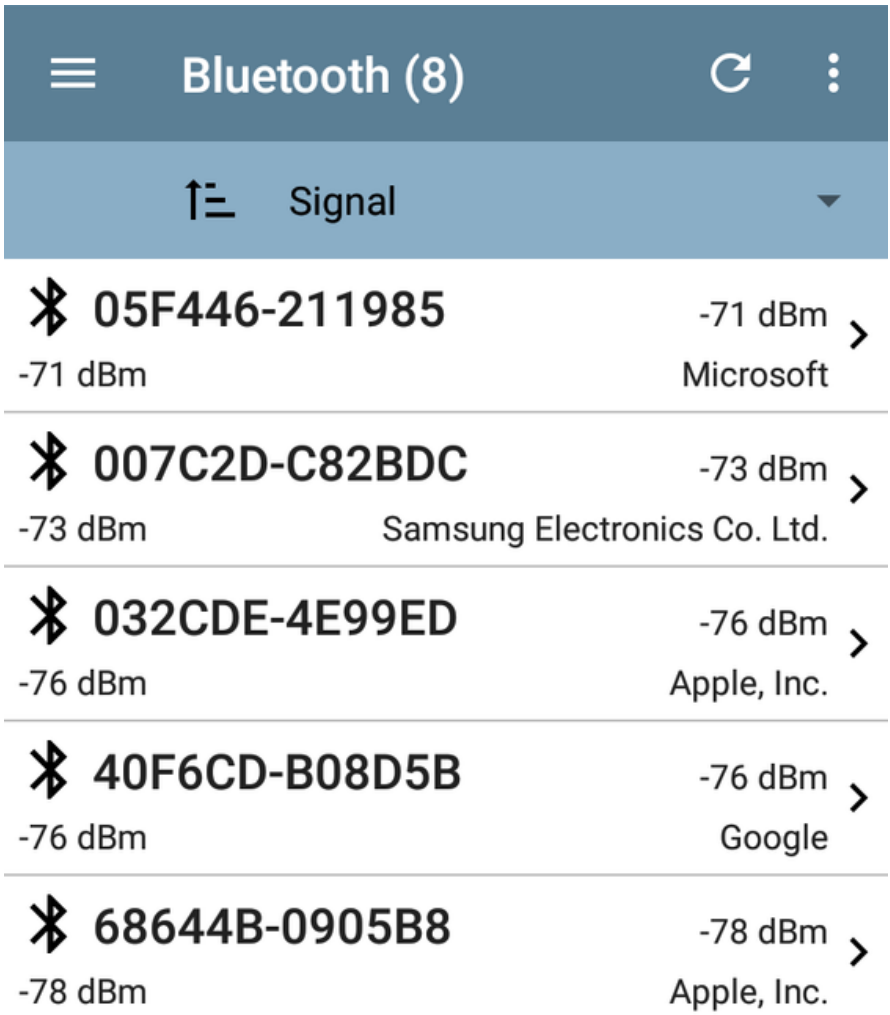
- Select **Locate** to open the Locate Client screen. See Locating Wi-Fi Devices.
- Select **Capture** to open the Capture app populated with the Channel and MAC address of the client. See the Capture app chapter.
- Select **Name and Authorization** to open the Name and Authorization dialog. See Assigning a Name and Authorization to a Device.

Back to Title and Contents

Bluetooth

The Bluetooth list screen displays all the Bluetooth devices discovered operating on your wireless networks.

> NOTE: This list requires that Bluetooth is enabled in your EtherScope nXG system settings. To verify, swipe down from the Status Bar at very top of the screen to open the system Notification Panel to see if the Bluetooth disabled icon is displayed. If so, tap the icon to turn on Bluetooth and display the Bluetooth enabled icon .



You can Sort the list to determine the order in which Bluetooth devices are shown. See Sorting in the Wi-Fi App for more details.

By default, Bluetooth devices are ordered by Signal strength. Each card shows the device address, signal strength in dBm (top right), and company name (bottom right).

> NOTE: Your EtherScope nXG considers a device *inactive* if it is not seen in over 1

minute. These devices are displayed with a grey title text and signal strength value and grey title text on the Wi-Fi - Bluetooth Device details screen. If the device continues to be inactive, EtherScope nXG considers the device *obsolete* and removes it removed from the list.

Tap an individual Bluetooth device card to open the Wi-Fi - Bluetooth Device screen.

Bluetooth Device Details

The Wi-Fi - Bluetooth Device screen shows the following:

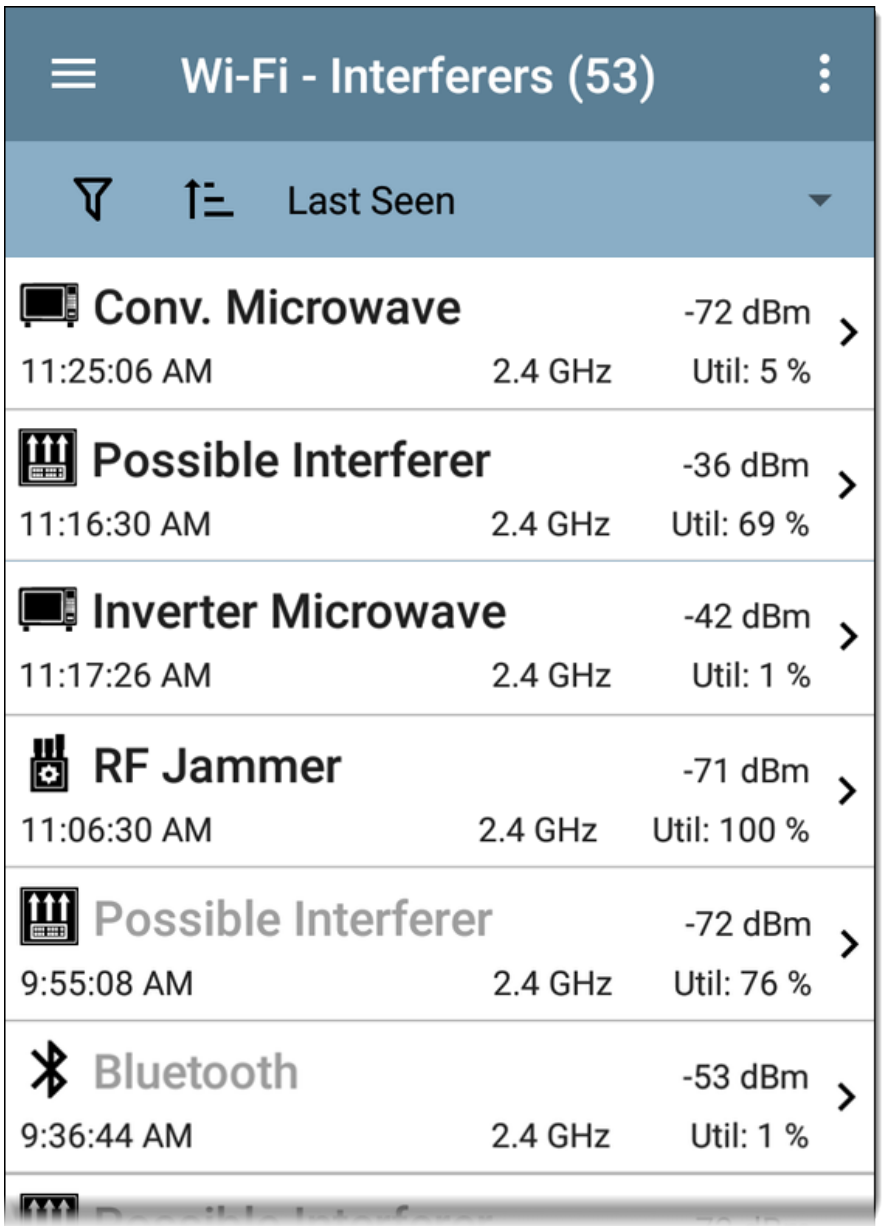
- Address
- RSSI

- Manufacturer company name and ID
- Beacon type (Eddystone-UID, Eddystone-URL, iBeacon, or None), beacon-specific information (depending on the beacon type), and transmit power (if applicable)
- Any advertised flags or data
- Last seen date/time.

Back to Title and Contents

Interferers

(EXG-200 only) The Interferers screen displays devices detected by the EtherScope that may be interfering on your networks.



You can Filter and Sort the list to determine which Interferers are shown and their

order. Refer to the Wi-Fi App List Screens topic if needed.

By default, Interferers are ordered by the time they were most recently detected by the EtherScope. Each card shows the Last Seen time, the device's Power measurement in dBm, the frequency band on which it was detected, and its Utilization.

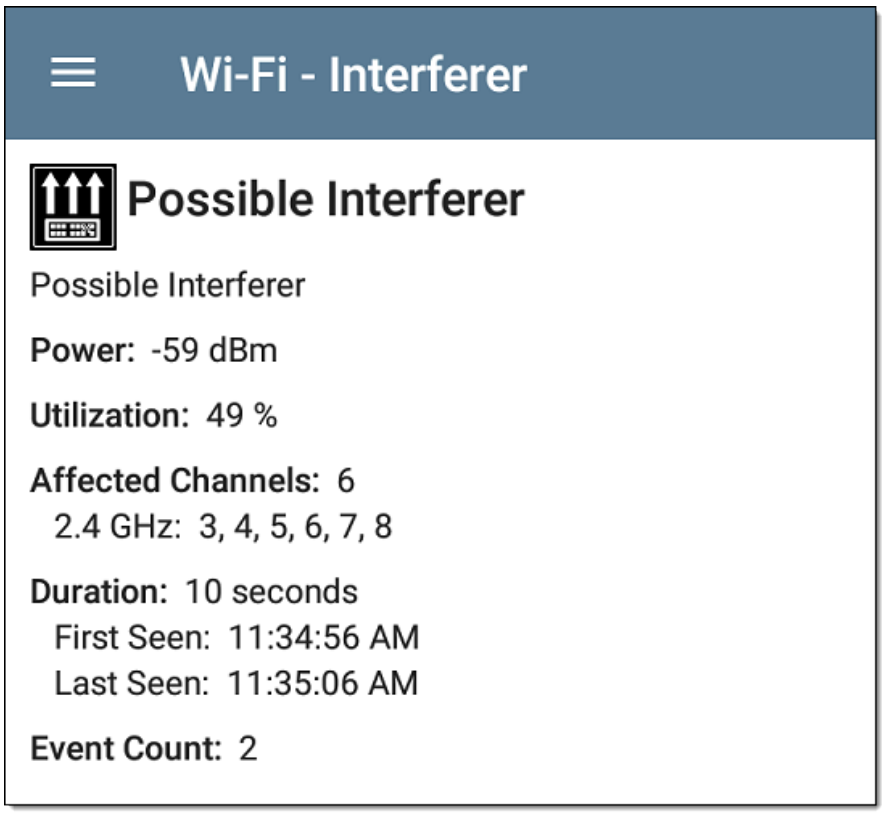
EtherScope can detect and display the following potential Interfering devices types:

- Baby Monitor
- Bluetooth
- DS Cordless Phone
- FH Cordless Phone
- Game Controller
- Possible Interferer
- Unknown Interferer
- RF Jammer
- YDI Narrowband Jammer
- Conventional Microwave
- Inverter Microwave

- Motion Detector
- Narrowband CW Signal
- Video camera

Tap an Interferer card to open the Details screen.

Interferer Details



Power: The most recently observed power output from the device

Utilization: The percentage of time, during the most recent sample, for which the interferer was detected

Affected Channels: The bands and channels on which EtherScope detects the interfering device

Duration: Amount of time EtherScope detected the device and when it was first and last detected

Event Count: Number of separate instances of detected transmission from the interferer

Back to Title and Contents

Path Analysis App

Path Analysis traces the connection points, including intermediate routers and switches, between the EtherScope nXG and a destination URL or IP address. You can use Path Analysis to identify issues such as overloaded interfaces, overloaded device resources, and interface errors. It also shows how devices within your network (and off-net devices) are connected to each other along a path.

All switches are pre-discovered through SNMP queries. When the measurement is complete, EtherScope shows the number of hops to the destination device. A maximum of 30 hops can be reported.

Introduction to Path Analysis

Path Analysis combines Layer 3 and Layer 2 measurements.

The Layer 3 measurement combines the classic Layer 3 IP (UDP, ICMP, or TCP) traceroute measurement with a view of the path through the Layer 2 switches.

The Layer 2 measurement discovers switches between the router hops by looking for the routers' MAC addresses in the switch forwarding tables by sending SNMP queries to all discovered switches. The switches found in the path are displayed between the router hops when the measurement finishes.

Path Analysis is most effective when you have configured the Discovery app with SNMP credentials. See SNMP Configuration in the Discovery Settings topic to learn how.

Path Analysis Settings

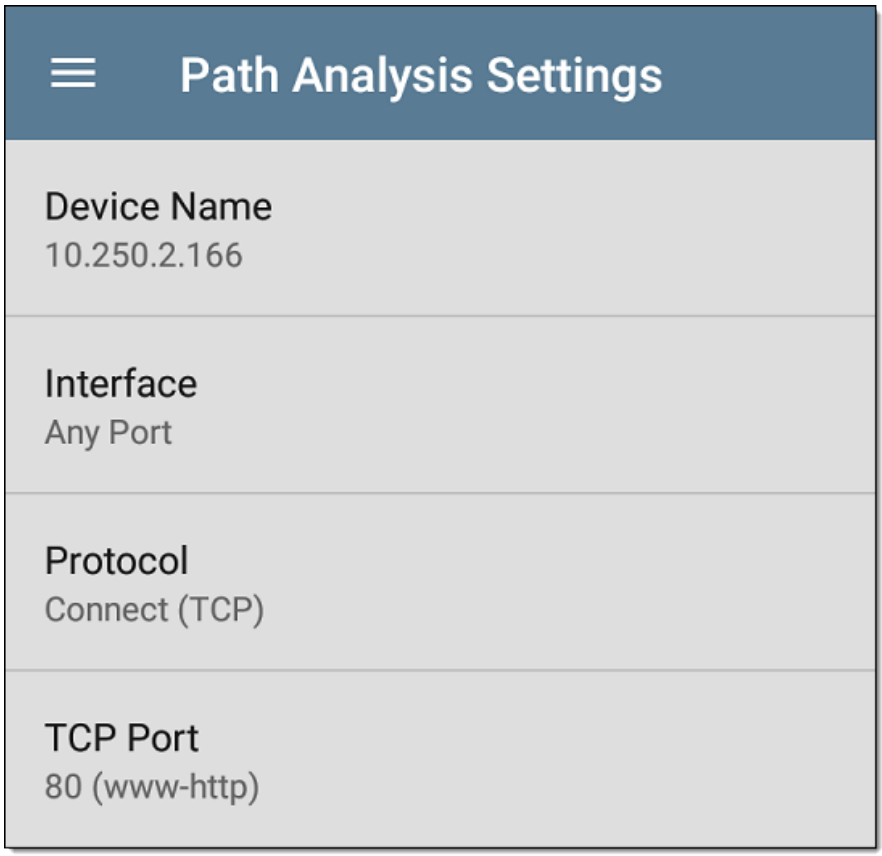
The Path Analysis source device is always your EtherScope nXG. The default destination is www.google.com.

Populating Path Analysis from Another App

Like other EtherScope testing apps, when you open Path Analysis from another app, like Discovery, the address of the network component you were viewing in the previous app is pre-populated as the Path Analysis Destination.

Configuring Path Analysis Manually

Open the app settings to configure a custom destination and select an Interface and Protocol. To open, from the Path Analysis app screen, tap the settings  icon, or open the left-side navigation drawer and select **Path Analysis Settings**.



On the Path Analysis Settings screen, tap each field as needed to configure your target:

Device Name: Tap to enter the IP address or DNS name of the Path destination. The default is www.google.com.

Interface: This setting determines the EtherScope port from which the port scan runs. Tap the field to select a port. (See Selecting Ports for explanations of the different ports.)

EtherScope must have an active network link on the selected port to run a Path Analysis. If **Any**

Port is selected, available links are used in the order shown in the Interface dialog above.

See Test and Management Ports for explanations of the different ports and how to link.

Protocol: Tap to select the Connect (TCP), Ping (ICMP), or Echo (UDP/7) protocol for your Path Analysis.

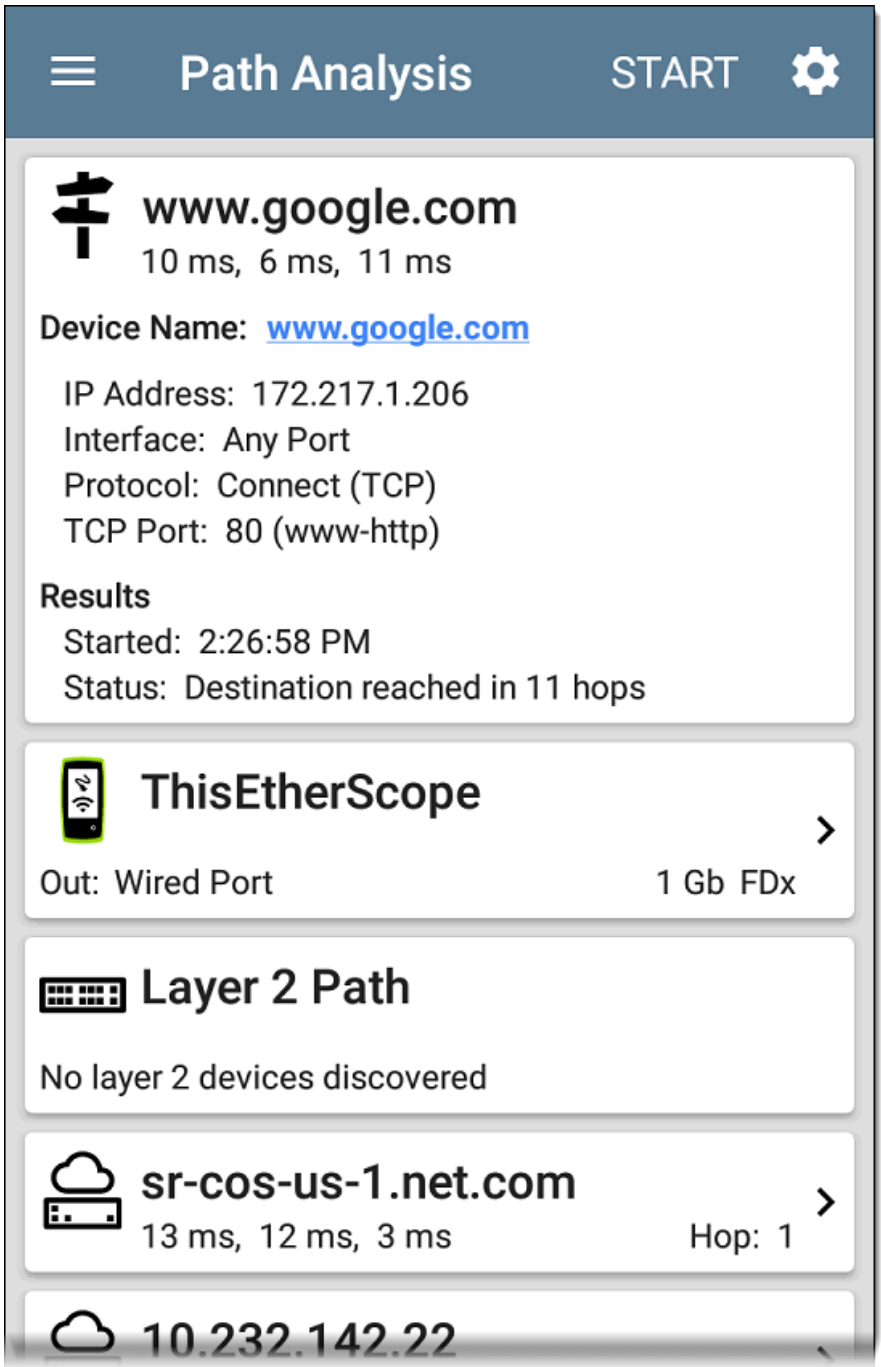
TCP Port: This field only appears if you have selected the Connect (TCP) Protocol. Tap to enter the port number over which you want to run Path Analysis. (You may need to enter a specific port number because routes can vary based on the port number and/or may be blocked by firewalls.)

Back to Title and Contents

Running Path Analysis

Tap the **START** button at the top of the app screen to begin a Path Analysis.

> NOTE: EtherScope must be linked on the Interface (Port) selected in the app's settings. See Test and Management Ports for help.

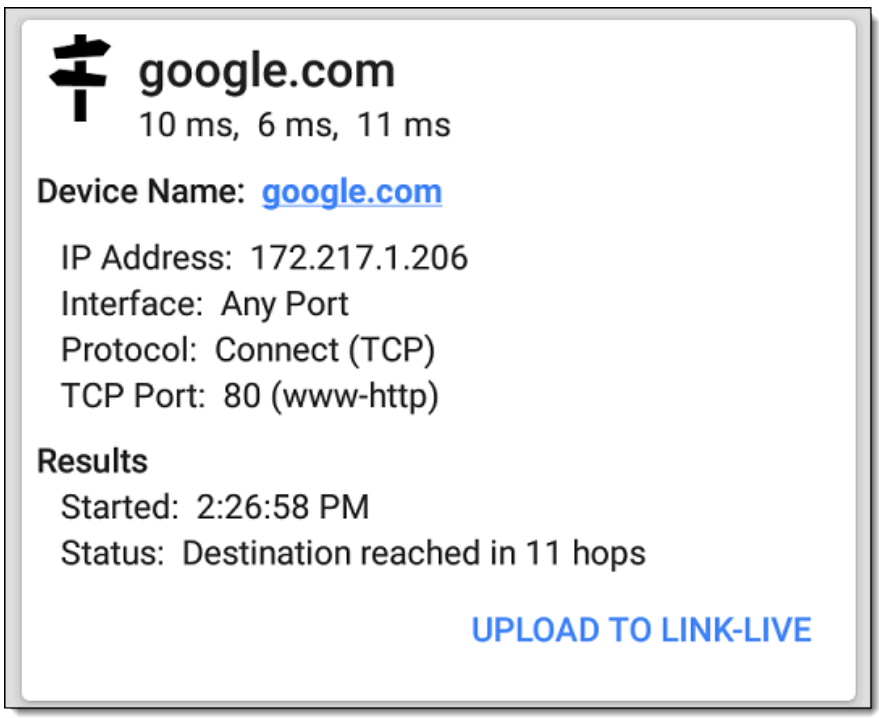


Like AutoTest, Path Analysis results are presented on cards. The top card shows the main test details, the second card shows information for the source device (your EtherScope nXG), and the following cards show

the Layer 2 and Layer 3 Hops in the path, which are sequentially ordered.

Tap any **blue linked name or address** in the Path Analysis results screens to open the Discovery or Wi-Fi app and further examine the linked element.

Path Analysis Results and Source EtherScope Cards



The top Path Analysis results card shows the path's Destination address at the top, followed by the three response times from the TCP Connect, Ping, or Echo tests.

Device Name: Resolved DNS name or IP address of the destination entered in the settings

IP Address: IPv4 address of the target destination

Interface: The Interface option selected in the settings

Protocol: The Protocol selected in the settings (TCP, Ping, or Echo)

TCP Port: The port number used for a TCP Connect Protocol. This field does not appear for Ping or Echo Protocol results.

Results

Started: Time at which the Path Analysis began

Status: Current status of the Path Analysis test, including any error messages

UPLOAD TO LINK-LIVE: Tap this link to upload your results to a Link-Live account. See Uploading Results to Link-Live later in this topic.

Source EtherScope Card

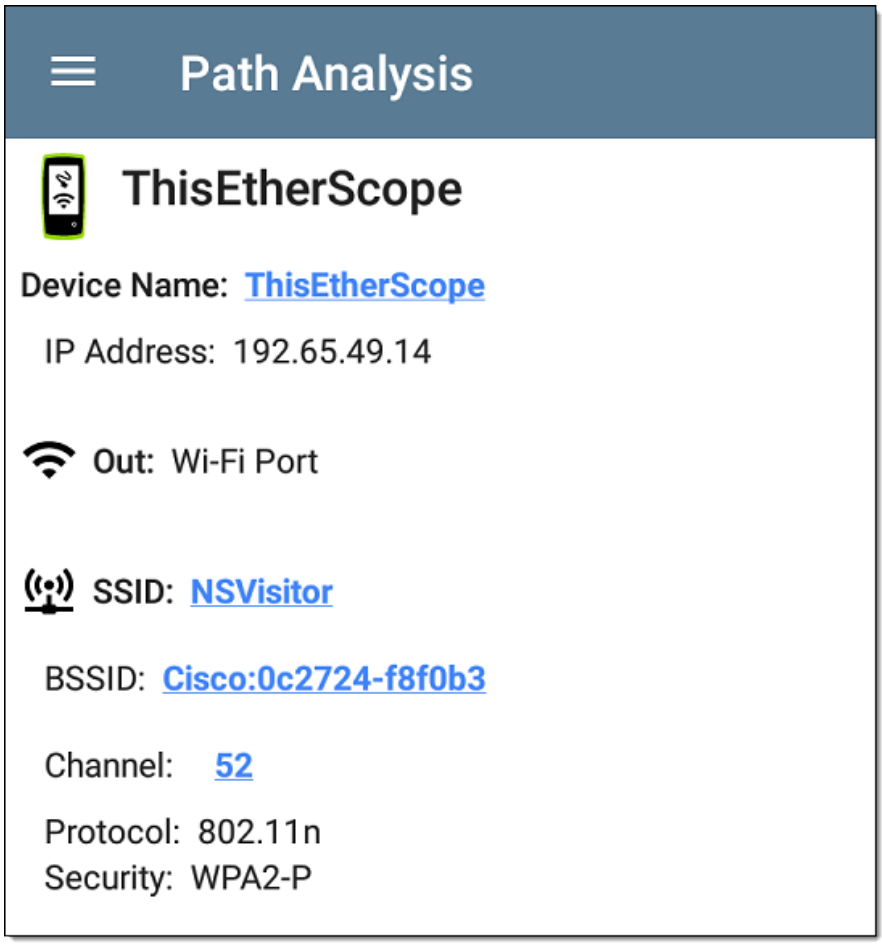
This EtherScope card displays the port from which the Path Analysis ran.

For Wired Test or Management port analyses (shown above), this card displays connection speed and duplex.

For Wi-Fi port analyses, the card displays the SSID and channel number.

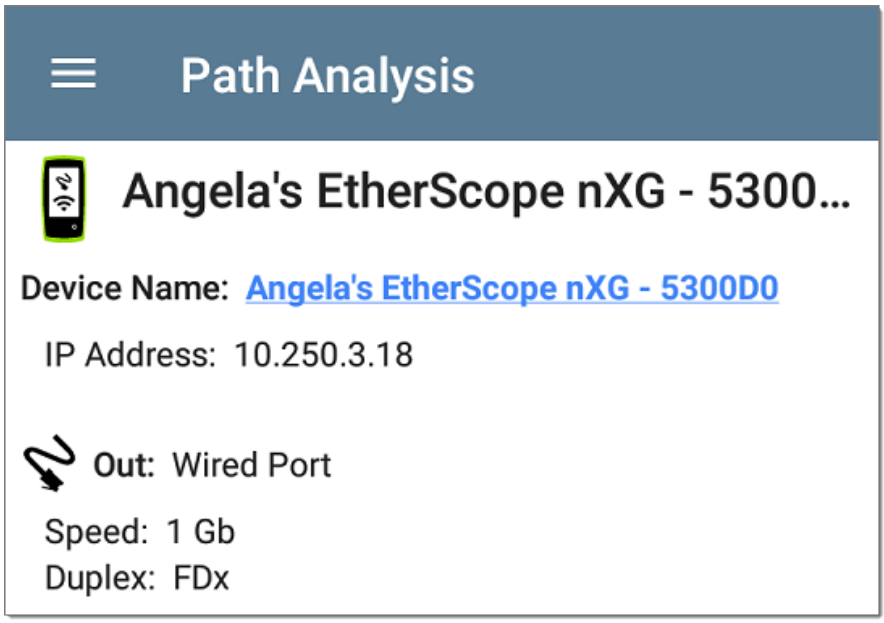
> NOTE: This card and screen only display a custom name for your EtherScope if you have claimed it to Link-Live.

Tap the card to view more details.



The example image above shows the SSID, Channel, and other Wi-Fi information the EtherScope can display after running a Path Analysis over Wi-Fi.

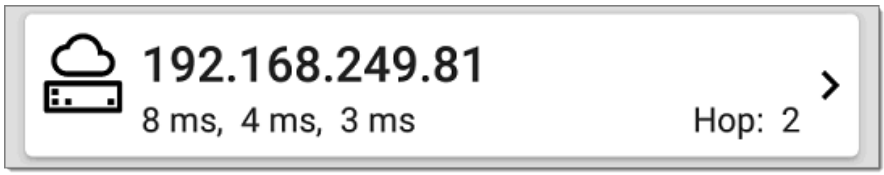
The image below shows the source EtherScope card from a Wired Path Analysis, which displays the link speed and duplex.



Beneath the EtherScope source card, the Hop cards show Layer 2 and Layer 3 devices determined to be in the Path.

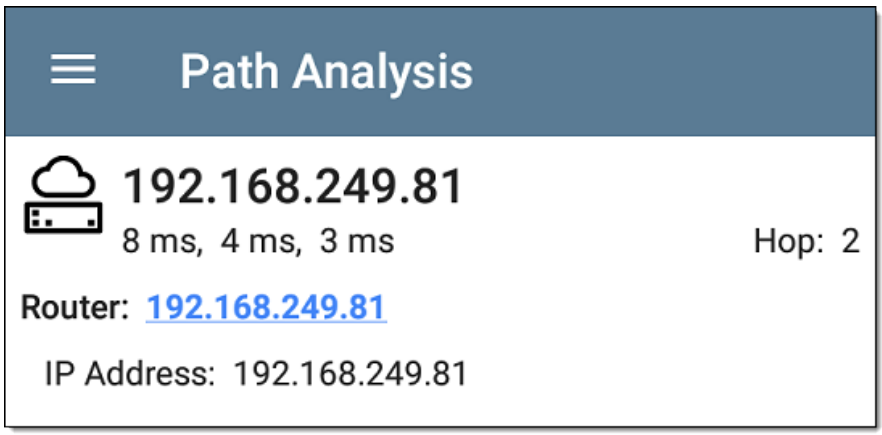
Layer 3 Hops

Each Layer 3 Hop card displays the device type icon, DNS name (if discovered), and IP address.



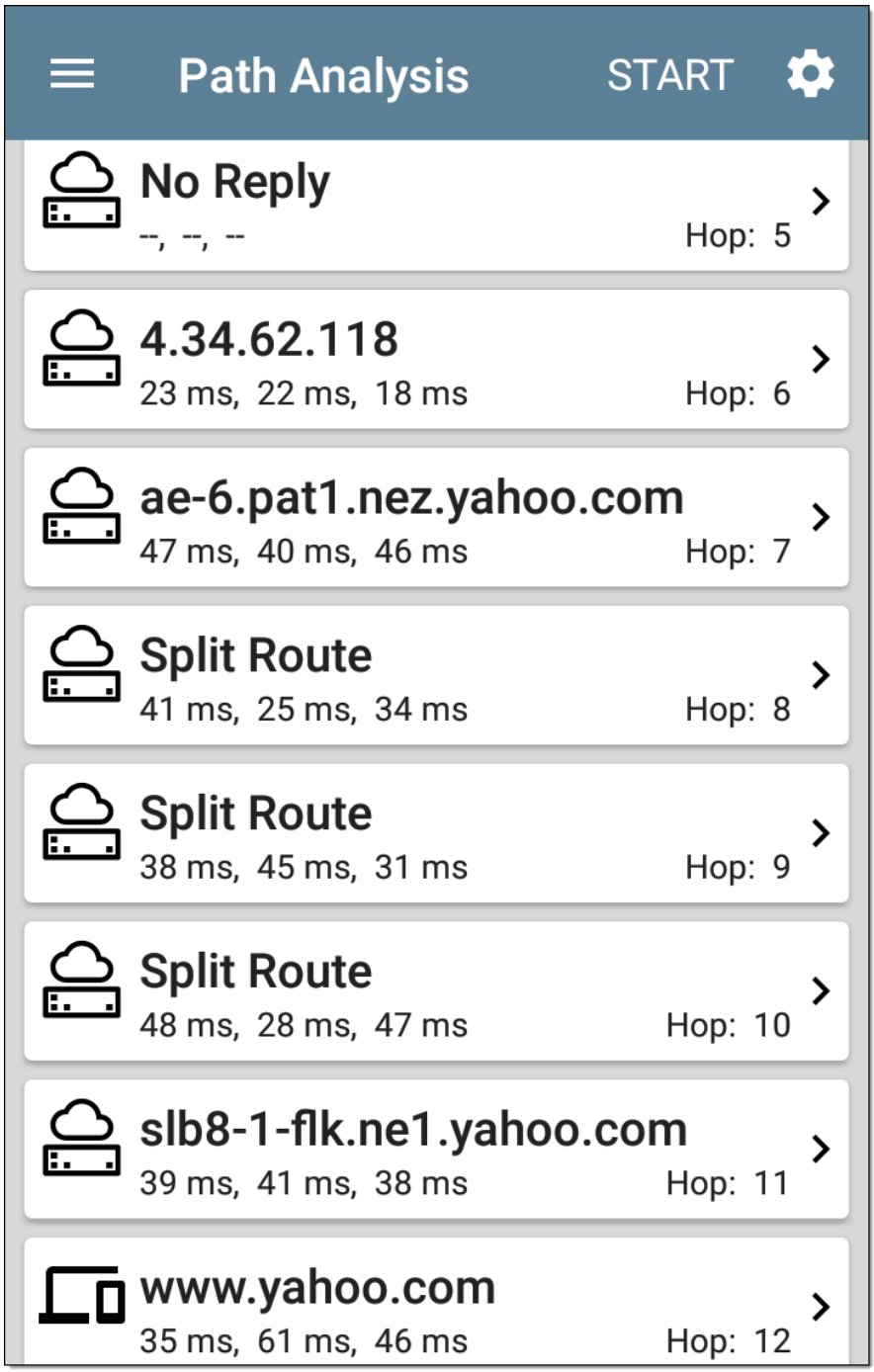
Beneath the name (or IP), the response times for each Connect (TCP), Ping (ICMP), or Echo (UDP/7) display in milliseconds. On the right side is the router Hop number of this device in the path.

Tap the card to view the hop Details screen.



No Reply

Sometimes Path Analysis displays Hop cards with "No Reply" (as shown below). This result means that the device in that portion of the path did not send an ICMP TTL timeout response.

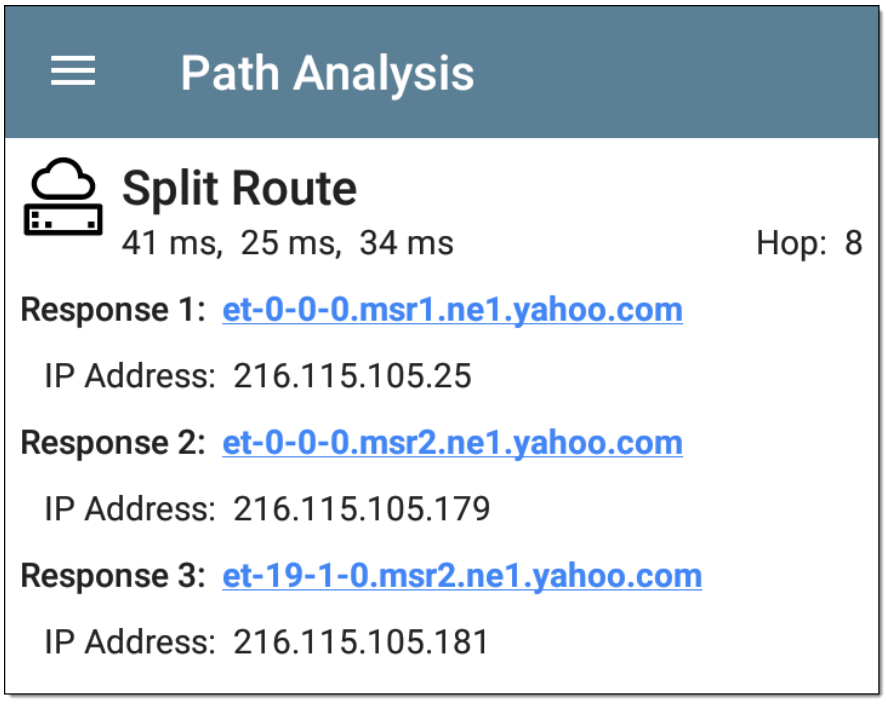


Split Route

Path Analyses may obtain a "Split Route" result (as shown above), meaning that two or three

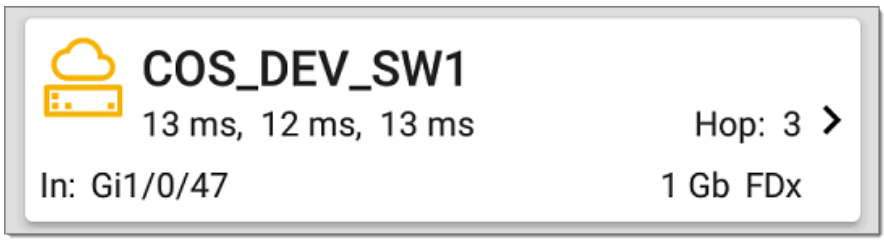
different routers within same hop responded to the three requests.

Tap a Split Route card to view the DNS names and IP addresses of the responding routers.



Layer 3 Interfaces and Statistics

Statistics for Interfaces on Layer 3 devices may be identified and measured if the EtherScope has SNMP access.



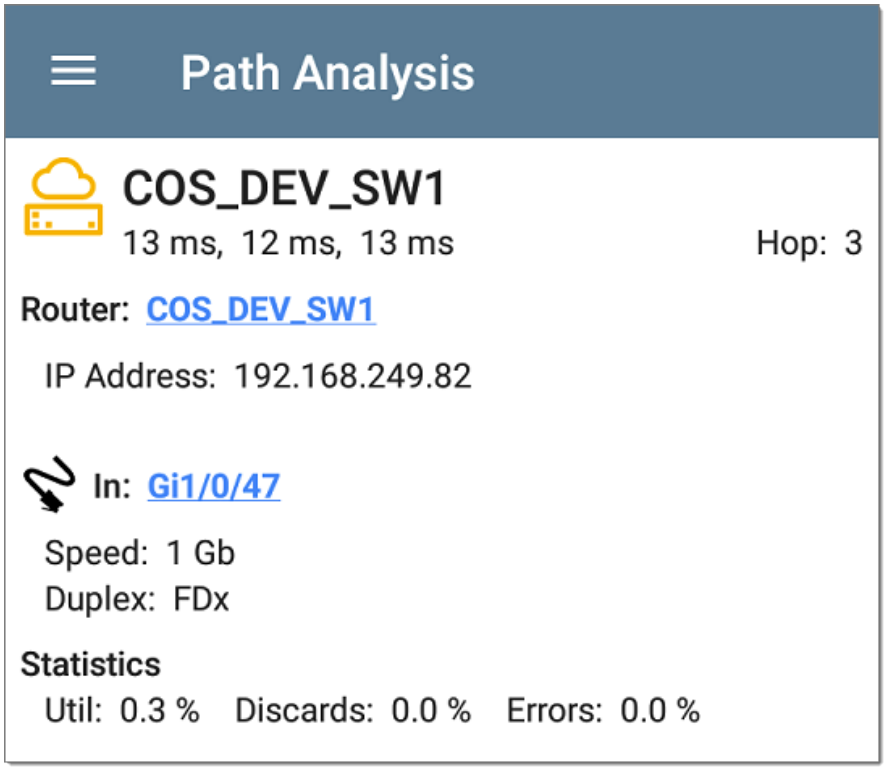
Tap a Hop card to see a summary of Interface Details and Statistics, if they are available.

See also Layer 2 Switch Interfaces and Statistics below.

Network Problems in Path Analysis

The Hop cards can also show detected Problems based on the Problem Settings in the Discovery app and display the device type icons in the corresponding colors.

The yellow switch icon in the image above indicates a **Warning** status.



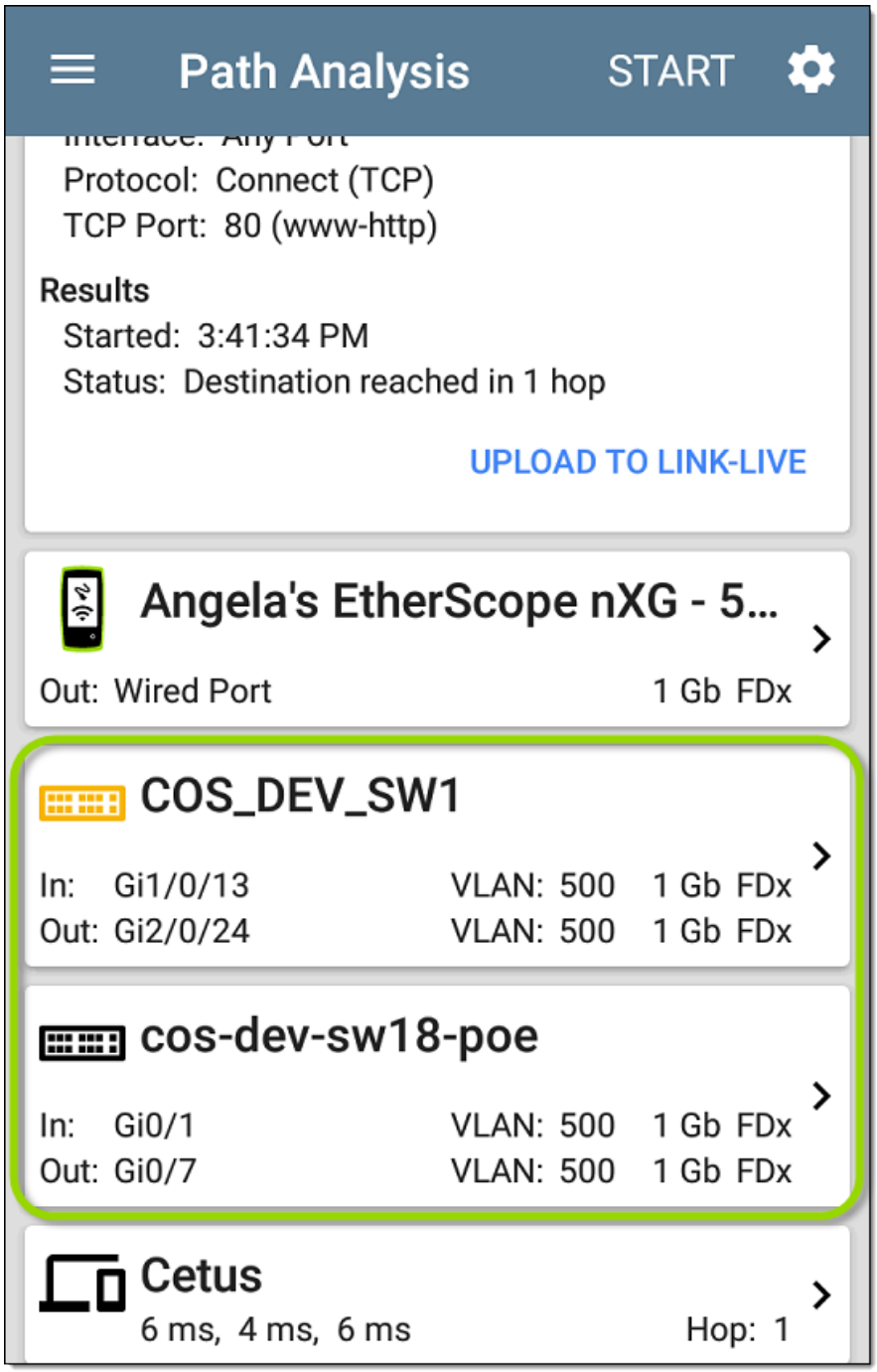
Tapping the blue linked switch name opens a Discovery Details screen for the switch, where the user can investigate the cause of the Warning.

Layer 2 Devices

Layer 2 devices can be switches or APs.

Layer 2 Switches

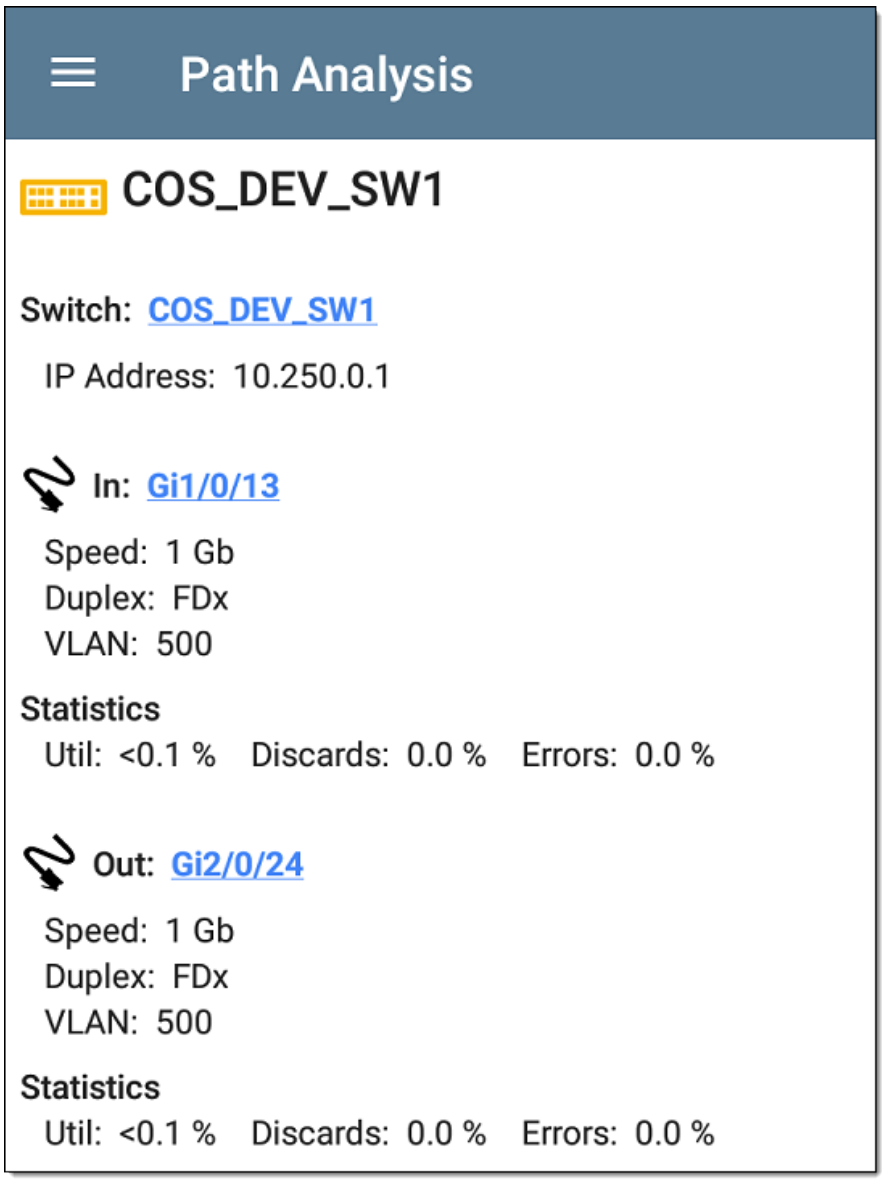
The image below displays an example of a Path Analysis to a device on the local broadcast domain with two switches in the Layer 2 portion of the path.



The EtherScope is able to identify these Layer 2 switches and their interfaces because it has configured SNMP access to the switches.

The switch cards display the In and Out Interface IDs, VLAN ID, and the link speed and duplex (if detected) of the interfaces.

Tapping a Layer 2 card opens a Details screen for the device.



A Layer 2 Details screen displays the device name and IP address at the top.

NOTE: The yellow switch icon in the image above indicates a **Warning** status. See Network Problems in Path Analysis later in this topic.

Layer 2 Switch Interfaces and Statistics

Layer 2 Switch Details screens in Path Analysis display a summary of the Interface Statistics (described below). To view all available information for these interfaces, tap their blue links to open a Interface Details screen in the Discovery app.

Statistics for Interfaces on Layer 2 switches may be identified and measured if the EtherScope has SNMP access.

In/Out: Indicates the interface type and name. The interface name often contains the physical port number where the switch is connected to the network.

Util: Percentage of total interface capacity being used

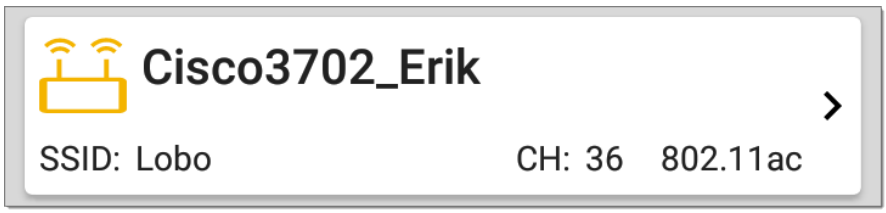
Discards: Percentage of total packets that have been dropped

Errors: Percentage of packets containing errors

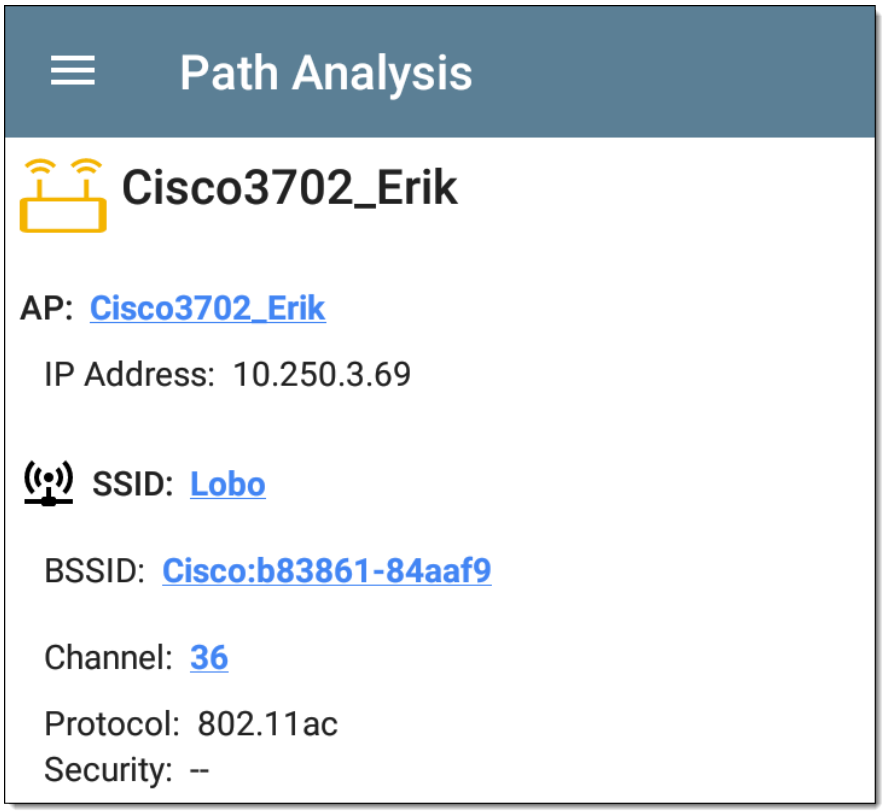
Layer 2 APs

If the Layer 2 path starts or ends with a Wi-Fi device, its AP is shown as a Layer 2 device in the path.

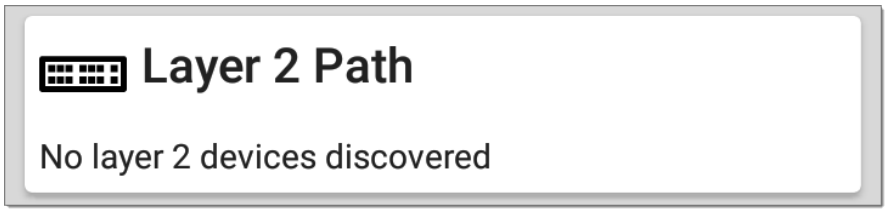
A Layer 2 AP card indicates the connected network SSID, channel, and 802.11 type in use.



Layer 2 AP Details screens allow you to further examine the wireless characteristics by selecting their blue links, which open a Wi-Fi app Details screen.



No layer 2 devices discovered



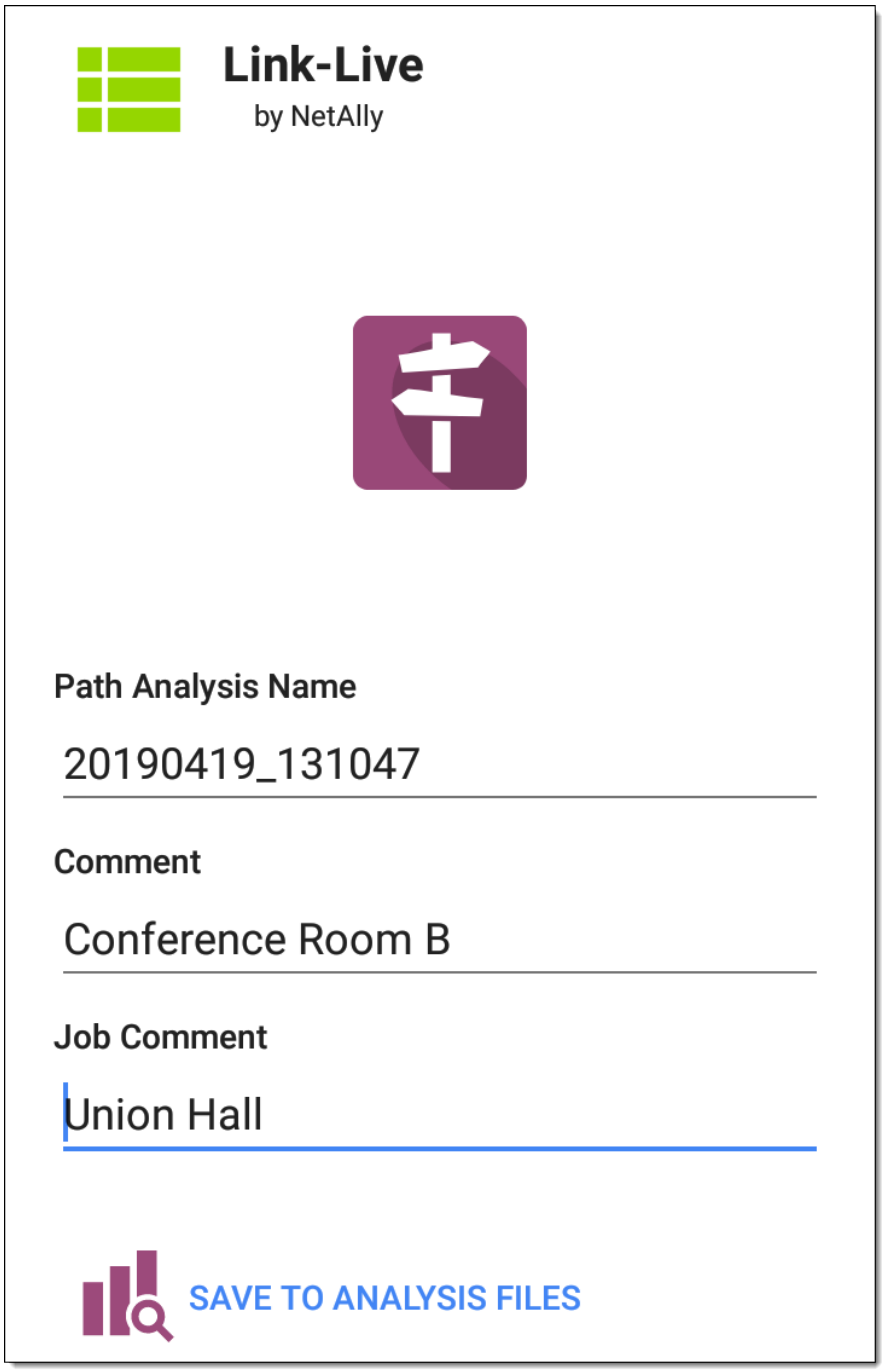
In some cases, the EtherScope does not discover Layer 2 devices between Layer 3 devices. There may not be any Layer 2 devices, or EtherScope might not have SNMP access to those switches.

The Layer 2 card may also display a result of "No switches found," which indicates that Discovery has not found any switches with SNMP access to

determine if the switches are in the path. If this is an unexpected result, check and verify your SNMP Configuration and Extended Ranges in the Discovery app settings.

Uploading Results to Link-Live

Tapping the **UPLOAD TO LINK-LIVE** link on the top card opens the Link-Live sharing screen for path analysis results:

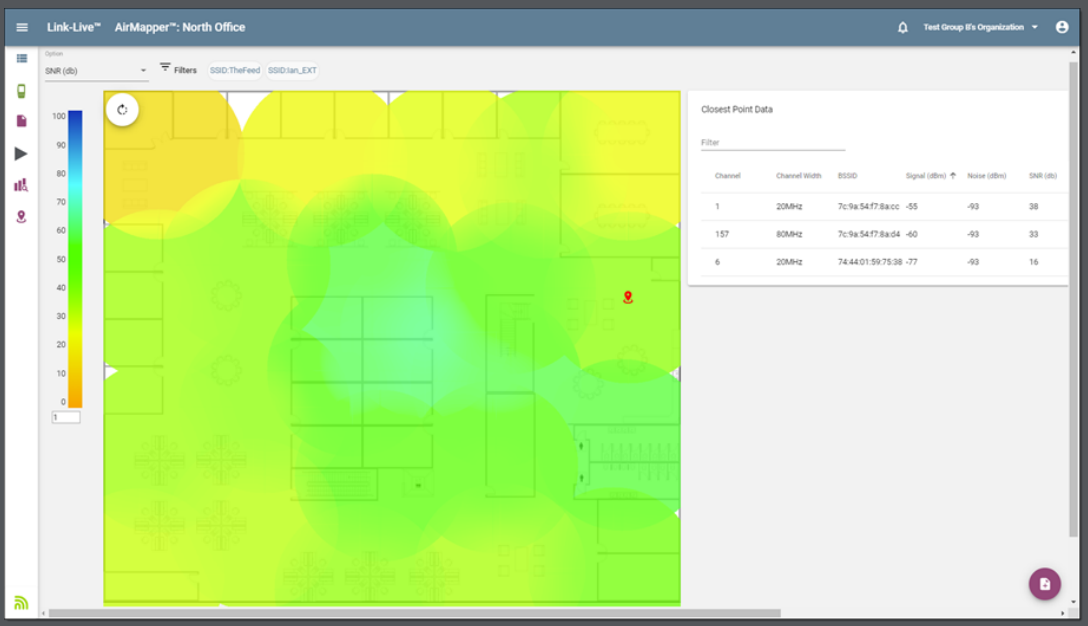


Path Analysis results are uploaded to the **Analysis** page on Link-Live.

Back to Title and Contents

AirMapper™ App

The AirMapper Site Survey application enables you to perform a Wi-Fi survey of an indoor or outdoor location and upload it to Link-Live Cloud Service. On Link-Live.com, you can view heatmaps and Wi-Fi measurements for each data collection point.



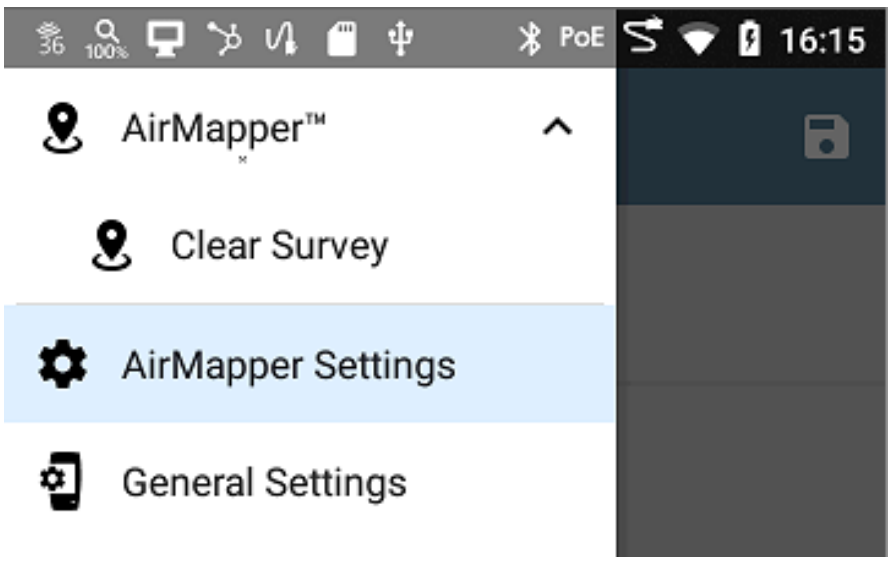
The Signal heatmap is available to all Link-Live users. **AllyCare** Support customers can also view maps of Noise, SNR, and Max TX and RX Rates. Visit NetAlly.com/Support.

AirMapper Settings

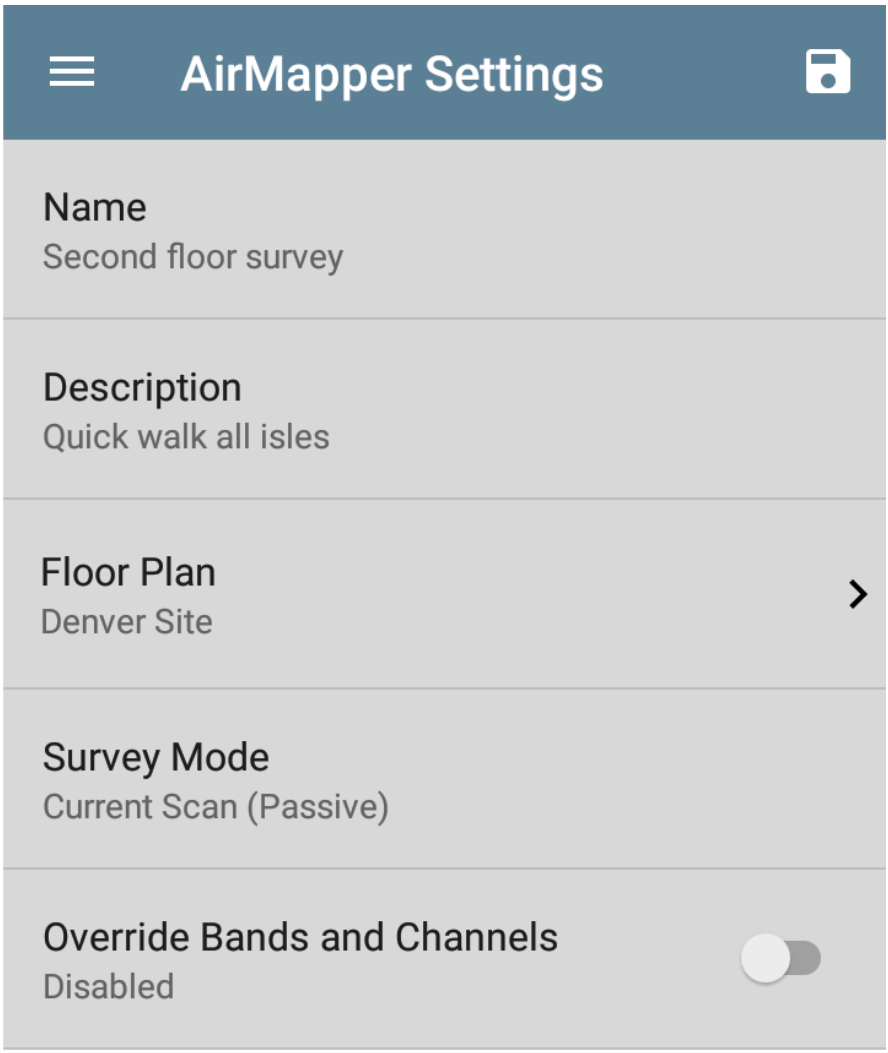
Setting up the AirMapper app to perform a survey involves naming the survey, loading a floor plan image, specifying its dimensions, setting scanning mode, and overriding bands and channels.

- Only .png and .jpg image files types are supported.
- You may need to use an image editing application to crop your floor plan image to known dimensions, such as the walls of a building or property boundary.

Access the AirMapper settings by selecting the menu icon or settings icon at the top of the main app screen.



Configuring an AirMapper Survey



Name

Tap the **Name** field to enter a custom name for your AirMapper project. This name is uploaded to Link-Live to identify this survey project.

Description

Enter any additional information you want for the survey.

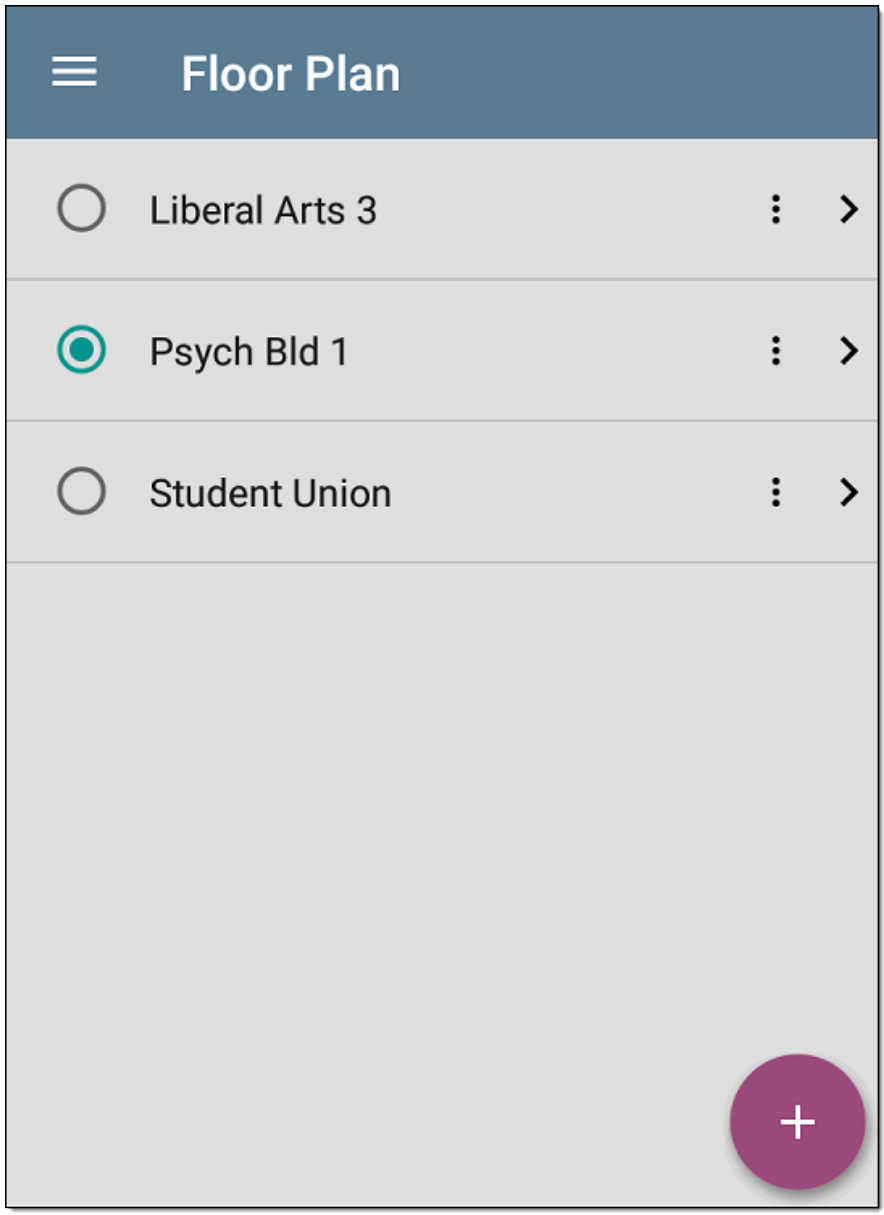
Floor Plan

NOTE: You can configure floor plans on Link-Live and then send them to your EtherScope nXG. A notification appears when a new floor plan arrives:

The new floor plan is added to the existing floor plans but is not automatically selected.

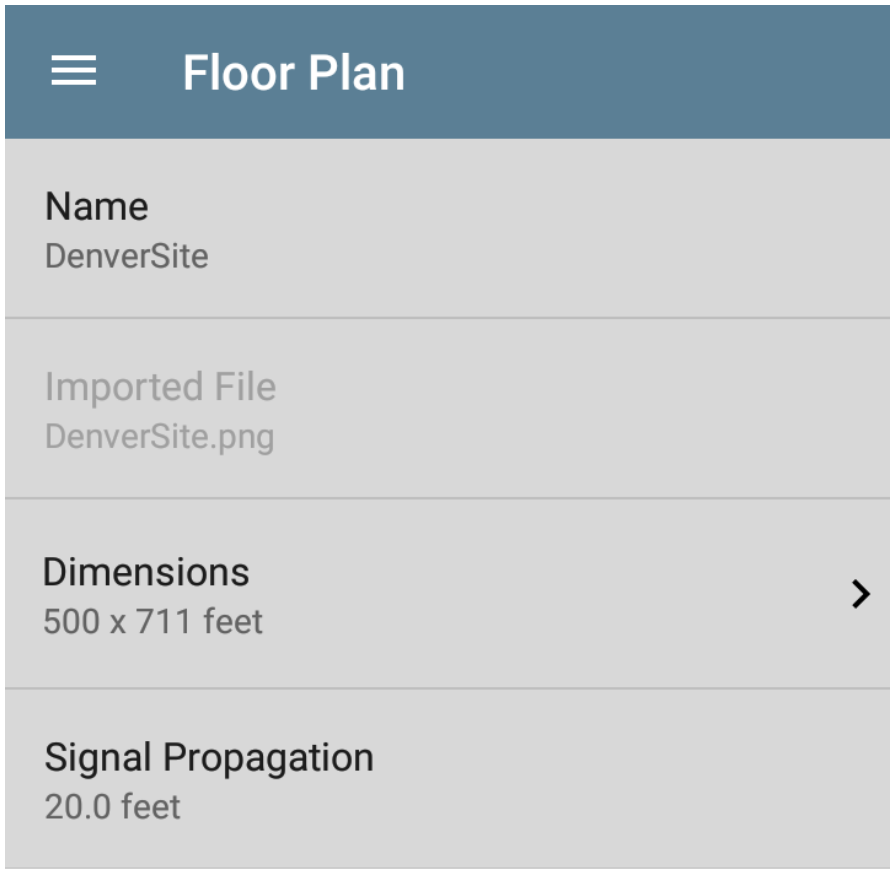
To select a floor plan:

1. Tap **Floor Plan** to open the list of available floor plans.



2. Select a floor plan or load a new floor plan by tapping the floating action button +, using the file selector to navigate to the new map image file, and then tapping the file to select it. This displays the Floor Plan menu.

3. Fill out the remaining fields for the Floor Plan as needed:



Name: Enter a name for this floor plan. This field defaults to the file name.

Imported File: The original image file name.

Dimensions: Tap this option to display the floor plan with two markers. Move the markers to two places on the floor plan that are a known distance apart. Then tap **Marker Distance** to enter the distance between the two points. (Set the units (feet or meters) in

the General Settings for the test apps, accessed from the left-side navigation drawer.) When finished, tap to return to the Floor Plan menu.

Signal Propagation: Tap to enter a value for the propagation radius for the survey sample points.

Survey Mode

Tap Survey Mode to select the Wi-Fi data collection method that best suits your Wi-Fi environment and survey data collection requirements:

1. **Current Scan** (Passive) is the default and preferred way to perform a survey. It allows immediate data collection based on the most recent AP beacon seen from each BSSID. AP BSSIDs age out after 140 seconds, and Wi-Fi clients age-out after 4 minutes. For EXG-200 only: AP BSSIDs age out after 30 seconds.
2. **Scan Once** (Passive) is more precise but more time-consuming. When a point is selected, all the BSSID information is

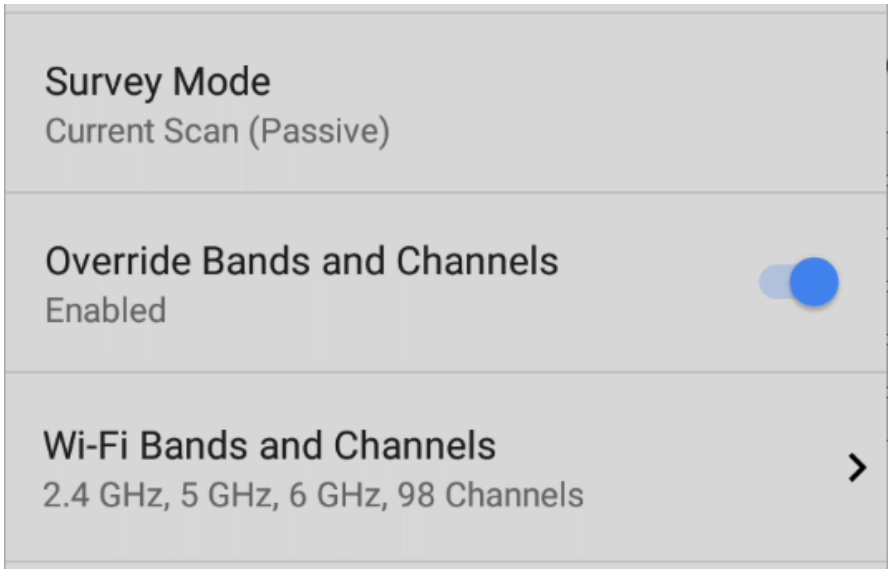
cleared, and the unit acquires a single scan of the selected channels for the selected dwell time. This gives an exact measurement. However, in congested environments any beacons not seen during the dwell time are not included in that sample point.

3. **Connected** (Active) collects data from the linked connection of the Wi-Fi Test port. NOTE: Selecting this method disables the AirMapper settings for Dwell Time and Override Bands and Channels.

Dwell Time

(Enabled for passive survey modes only.) Tap **Dwell Time** to select choose a preset dwell time or enter a custom value. See the General Settings for additional information about dwell time.

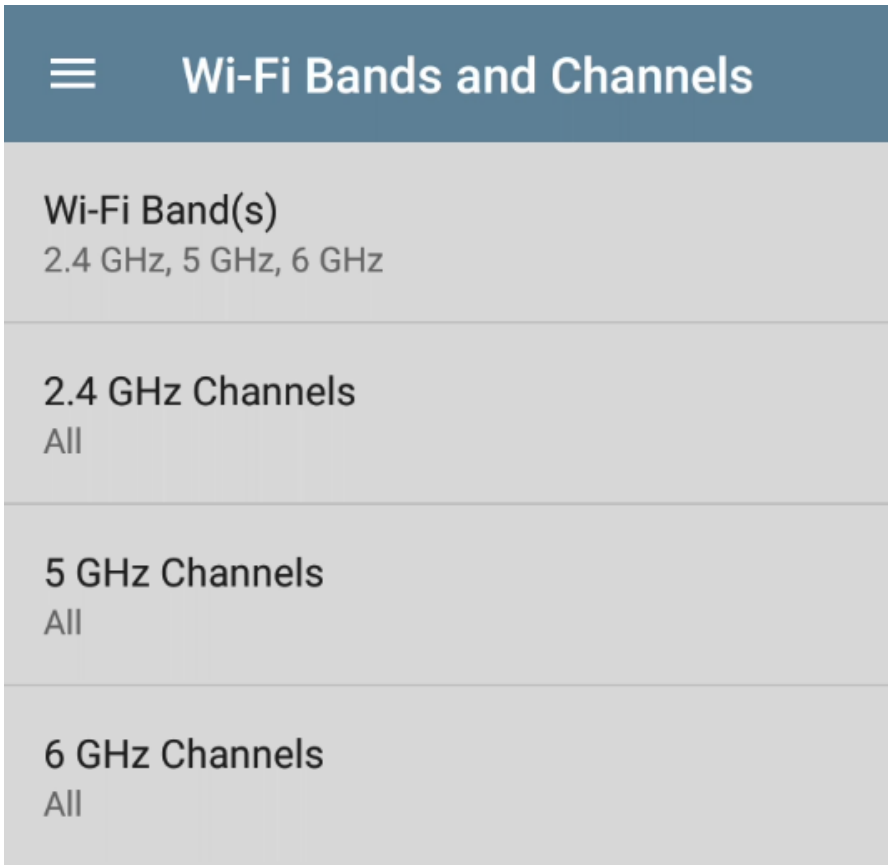
Override Bands and Channels



(Enabled for passive survey modes only.) Tap **Override Bands and Channels** to enable selection of different bands and channels than the values defined in General Settings. (These override settings are used only for AirMapper site surveys.) Enabling this setting displays the Wi-Fi Bands and Channels setting.

Wi-Fi Bands and Channels

(Enabled only when Override Bands and Channels is enabled.) Tap **Wi-Fi Bands and Channels** to open a list of frequency bands. Then tap the frequency band to open a menu to select specific channels to use for that band. See the General Settings for additional information.



Note: Selecting a subset of channels and bands lets you exclude scans of unneeded channels from the survey. This improves survey performance and reduces the amount of data collected.

Changing Settings after Starting

You can reopen the AirMapper settings to change the **Floor Plan > Dimensions** or **Signal Propagation** size after starting your survey. Existing data points are retained on the map unless you select a different Floor Plan.

Note: NetAlly does *not* recommend that you change the band, channel, or dwell time settings after you have started a survey. The survey results for the multiple settings can create confusing or less reliable results. If you wish to do so and if the **Override Bands and Channels** setting is enabled, you can use the AirMapper Settings to make changes after you have started your survey. If the **Override Bands and Channels** setting is *not* enabled you must use the General Settings to make changes.

Hidden SSIDs and APs

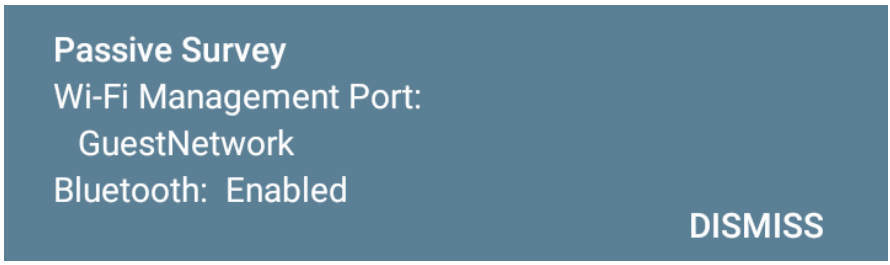
For any [Hidden] APs or SSIDs at your site that you want detected during a survey, NetAlly recommends creating and enabling a Wi-Fi Profile in the AutoTest app, configured with the appropriate credentials. Otherwise, AirMapper detects the BSSIDs associated with hidden devices but may not determine their APs/SSIDs.

Collecting AirMapper Data

Your selected floor plan appears on the main AirMapper screen.

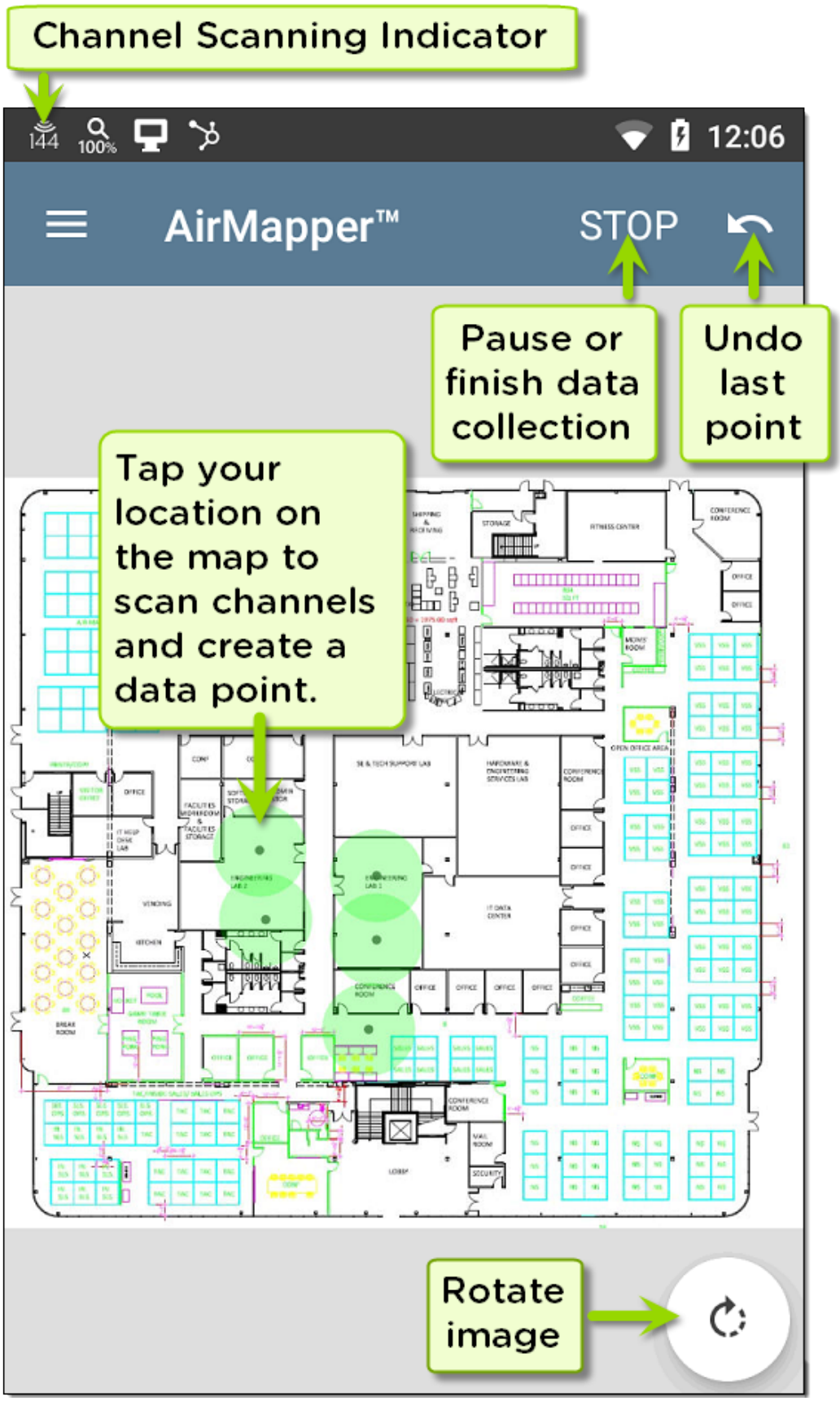
Tap **START** to begin the survey.

A message displays the survey type, radio, and Bluetooth status. This message appears each time you begin or restart or return to the survey from another app. Tap **Dismiss**.



To collect data, travel around your site, and tap the map at your current location to scan the enabled wireless channels in that spot.

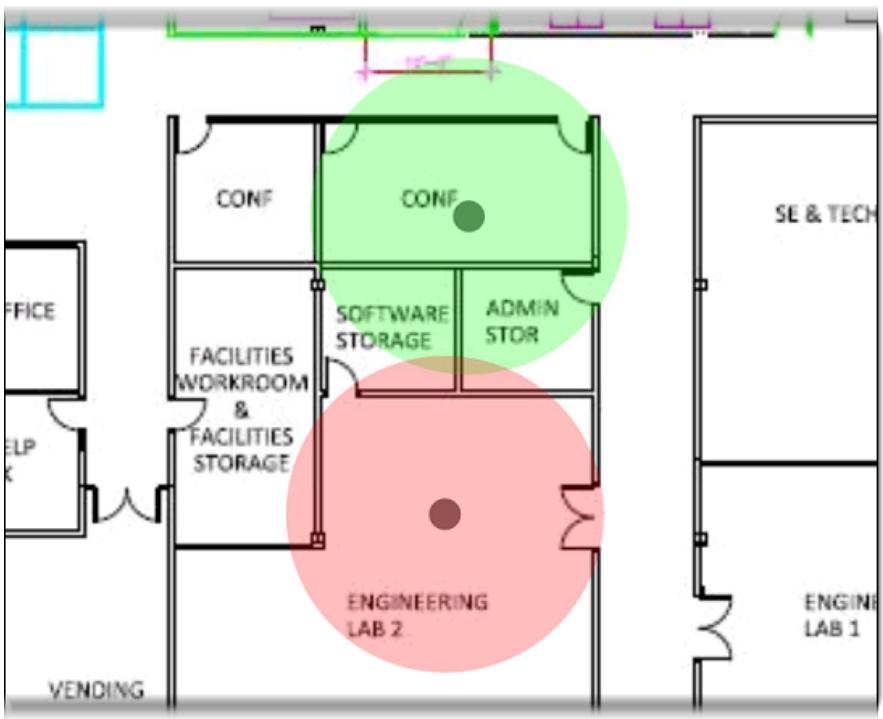
Do not move from that location until the scan is complete and the data point on the screen turns from red to green.


Channel Scanning Indicator
144
100%
12:06
AirMapper™
STOP
Pause or finish data collection
Undo last point
Tap your location on the map to scan channels and create a data point.
Rotate image

As shown in the image above, you can undo previous collection points and rotate the image as needed.

Use swiping and pinch-to-zoom gestures to pan and zoom the map.

While the EtherScope is scanning, the Signal Propagation circle is red. Once the scan is complete, the circle turns green.



The completed data points in the AirMapper app are always green. The colored heatmap is generated once you upload the AirMapper results to Link-Live.

Watch the Wi-Fi status icon  in the top status bar to see the channels the EtherScope is scanning in real time.

> NOTE: To adjust the **Dwell Time**, meaning the amount of time the EtherScope lingers on each channel gathering data, enable the Override Bands and Channels and open the Wi-Fi Bands and Channels, or open the General Settings **> Wi-Fi Bands and Channels**, accessed from the left-side navigation drawer.

When you finish adding data points, or if you want to pause, tap **STOP**.

Tap **RESUME** to add more data points.

Taking a Connected (Active) Survey

Use AutoTest to run a Wi-Fi profile and connect the desired SSID. Tap **START** to begin the survey.

If not connected to an SSID, a message is displayed at the bottom of the screen and the survey will not start.

Collect data as you would a passive survey described above.

If the connection is lost, the link notification changes to an X. EtherScope continuously tries to reconnect to the SSID.

Survey points taken during this unlinked time are displayed in Yellow. These indicate areas where there is not coverage for that SSID.

When you finish adding data points or if you want to pause the survey, tap **STOP**.

Tap **RESUME** to add more data points.

Tap the Link-Live upload icon  to send your survey results to Link-Live's AirMapper page.

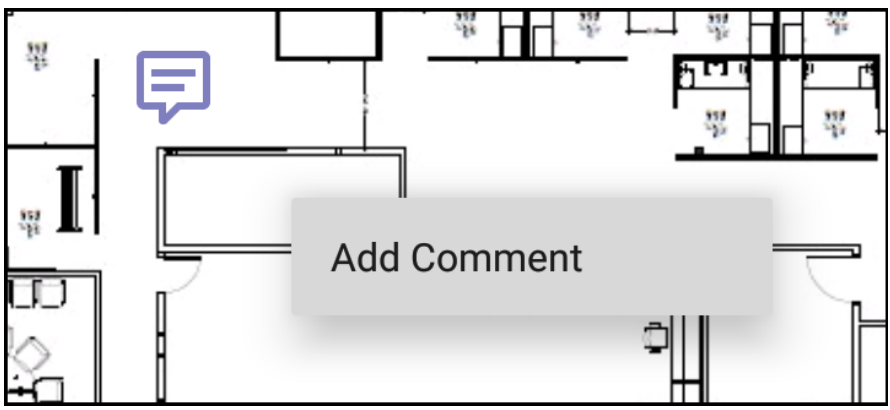
Adding Wi-Fi Management Port Data

If the Wi-Fi Management port is connected to an SSID, its active connection data is added to any survey points taken. It doesn't matter what type

of survey you are taking. This information is viewable only on Link-Live.

Adding Comments

Long press on the floor plan to add a comment. A context menu appears. Tap **Add Comment**. A dialog appears to enter your comment. Tap **OK** to add the comment.

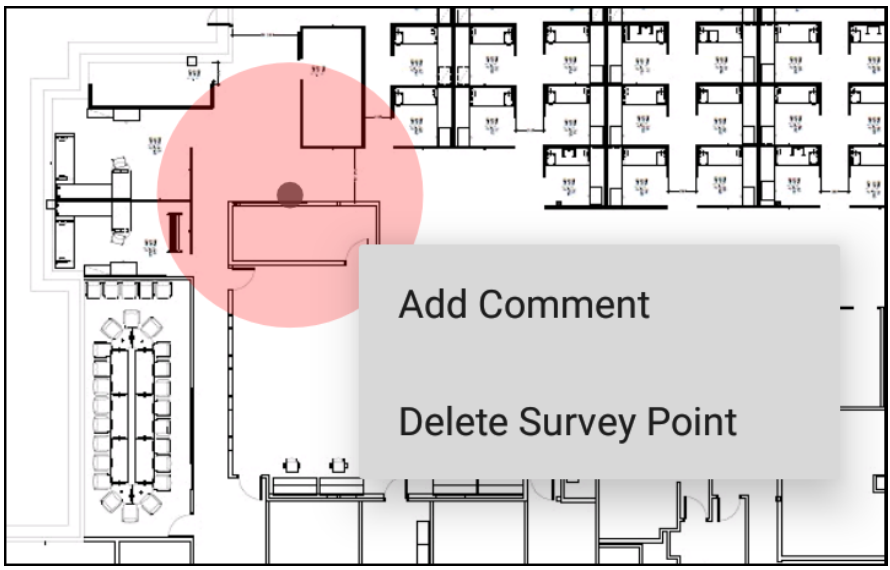


Long press over a comment to edit/delete it. The selected comment turns dark and a context menu appears. Tap **Edit Comment**. Edit the comment and tap **OK** or tap **Delete** to remove it. If two comments are very close, the closest one to the tap point is selected.

Deleting Survey Points

Long press over a survey point to delete it. The selected survey point turns red and a context

menu appears. If two survey points overlap, the closest survey point is selected. Tap **Delete Survey Point**.



NOTE: There is no undo for deleting a survey point. Once deleted, it cannot be recovered.

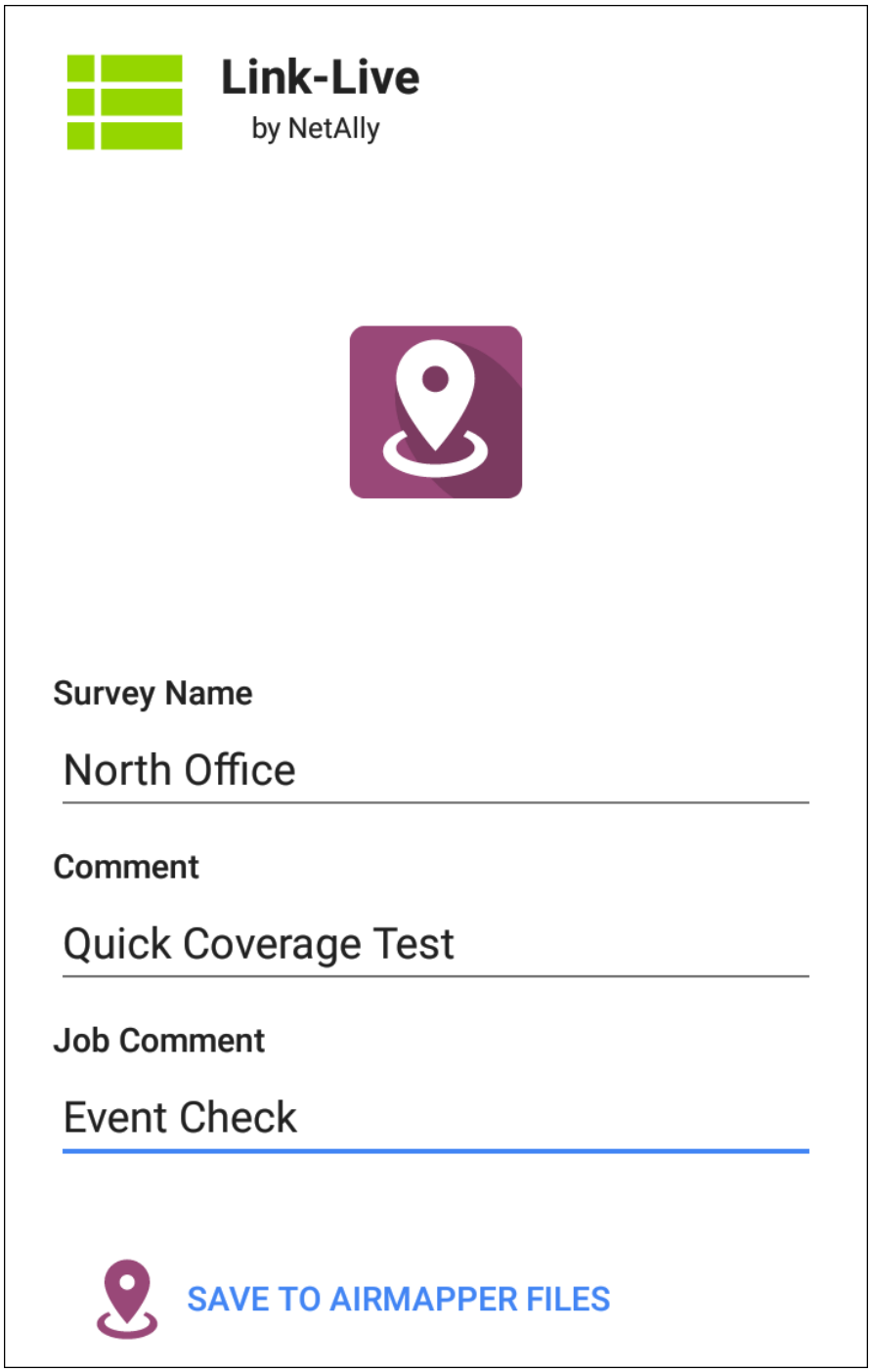
Uploading AirMapper Surveys to Link-Live

When you tap the upload icon , select **Upload to Link-Live** to display the Link-Live sharing screen.

Tap the Link-Live upload icon to send your survey results to Link-Live's AirMapper page. The upload dialog lets you enter a survey name, a comment for the overall survey, and a job

comment (such as a note about the overall job status).

NOTE: When you upload data from a survey (or save it locally), your unit also uploads/saves a Discovery analysis file to assist with data analysis on Link-Live. When you upload an active survey, the connection log is also uploaded.



Enter any **Comments** or Job Comments you want attached to your AirMapper result in Link-Live, and tap **SAVE TO AIRMAPPER FILES**.

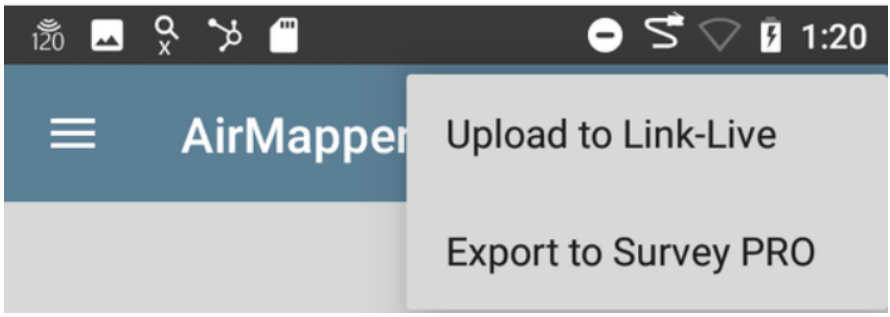
NOTE: The Job Comment remains the same until you delete or change it.

The current survey remains on the AirMapper screen until you **Clear Survey**, allowing you to add additional points if needed and re-upload.

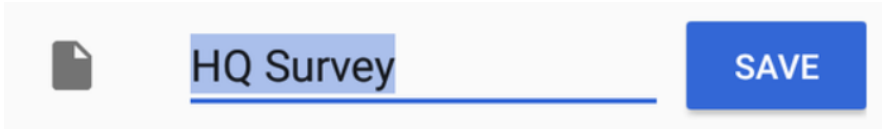
Export AirMapper Data to AirMagnet Survey PRO

Survey data can be exported as a .amp file for import into AirMagnet Survey PRO version 10 for more advanced analysis, planning and reporting.

When your survey data collection is complete, tap the upload icon and select **Export to Survey PRO** to create the .amp file.



Optionally rename the .amp file and select the Save button to create the .amp file.

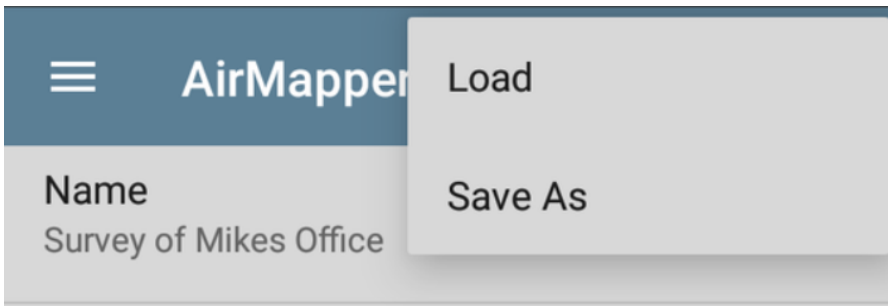


You can copy the file to external storage at a later time using the Files app.

Load and Save AirMapper Settings

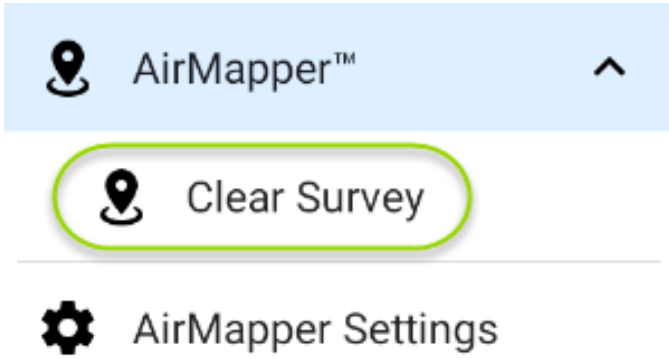
The entire survey configuration can be saved as named settings using the disk icon in the title bar.

This allows fast recall of any specific survey configuration.



Starting a New Survey

To start a new AirMapper survey, open the left-side drawer and select **Clear Survey**.



Back to Title and Contents

Spectrum Test App

The Spectrum Application is a dual-band Wi-Fi spectrum analyzer that measures Wi-Fi signal information to provide data about signal strength as well as noise. This application requires the NXT-1000 Portable Spectrum Analyzer (sold separately or included in kits), which plugs into the top USB port of your test unit.

This application offers:

- Frequency spectrum (heat map) display across the frequency band
- Waterfall display (2-minute historical) of RF
- Real time display of current, average, and max-hold signal levels

This information can help you identify both Wi-Fi and non-Wi-Fi sources in your environments.

Using the Spectrum Views

Opening the Spectrum app automatically changes the screen orientation and opens the default view: a Frequency Spectrum graph for the 2.4 GHz band. You can choose from three views of live data: Frequency Spectrum (heatmap), Waterfall, and Real Time.

Before You Begin

- Connect NetAlly's Spectrum dongle to the top USB port (USB Type-A) of your EtherScope nXG. (See Contact NetAlly to acquire the NXT-1000 Portable Spectrum Analyzer if you do not already have one.)
- Tap the Refresh icon to clear the current graph and start new measurements.
- To get more accurate test results, NetAlly recommends that you turn off your device's test and management Wi-Fi and Bluetooth. (The Spectrum app notifies you if these services are turned on.)

  To turn off test Wi-Fi:

1. Tap the Menu icon ☰ to open the Spectrum navigation drawer.
2. Tap **General Settings**.
3. Tap **Use Wi-Fi test port** to set it to Disabled.

To turn off management Wi-Fi and Bluetooth:

1. Swipe down from the top of the EtherScope screen to display the system icons.
2. Tap the Wi-Fi- icon until it indicates that Wi-Fi is off. (You can also use the General Settings to turn off management Wi-Fi.)
3. Tap the Bluetooth icon until it indicates that Bluetooth is off.

- (Optional) See "Spectrum Settings" on page 661 for instructions on changing the frequency band, changing the Waterfall View type, and saving settings.

Using Common View Actions

Use these actions in each Spectrum view to change the view details:

- **Pause:** Tap the Pause icon  to stop updates of the display. This can help you examine patterns and anomalies without updated data overriding your current view.
- **Resume:** Tap the Resume icon  to cancel a pause and continue live data updates.
- **Refresh:** Tap the Refresh icon  to clear the graph and start acquiring new data. (A refresh also cancels a pause.)
- **Display markers:** (Frequency Spectrum and Real Time views only) Tap the graph at a particular frequency that you want to examine. This displays a pink vertical marker at that frequency and lists the frequency's numerical details above the graph.
    - The Frequency Spectrum view displays the frequency and its maximum value.

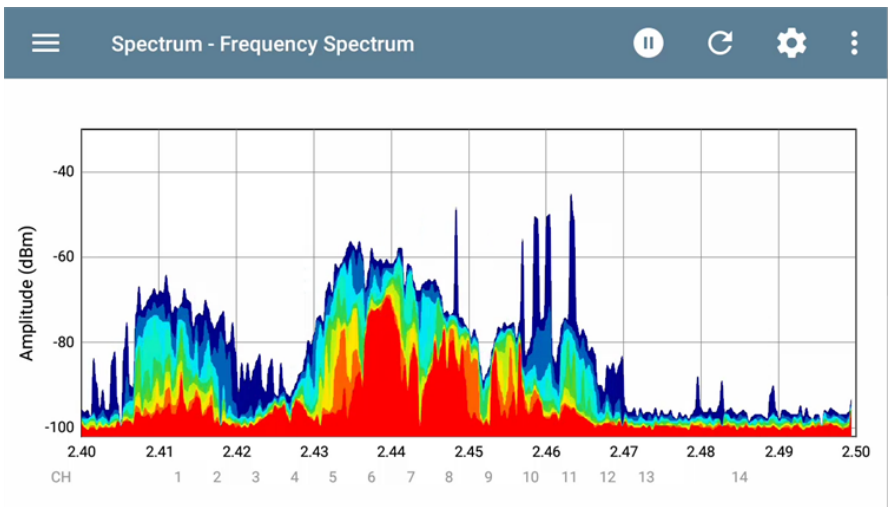
  - The Real Time view displays the frequency, the frequency's current value, the average value, and the highest measured value (Max-Hold).
  - If you have a specific frequency detail marker, double-tapping on the marker erases it. (You can reset the marker by single-tapping the graph again.)

- **Zoom in:** Double-tap the view graph to zoom in to a narrower band around a particular frequency.
  - For the 2.4 GHz band, the graph centers on a 40 MHz range around the channel closest to the frequency you tapped.
  - The 5 GHz band the graph centers on an 80 MHz range around the nearest of several predefined frequency ranges.
- **Restore to normal view:** Tap the Restore icon to close the zoomed-in view, return to the full display for the frequency band, and refresh the graph with new data.

- **Saving results:** see "Uploading Results to Link-Live" on page 659.

Frequency Spectrum View

This display uses the color spectrum to present a heatmap of the frequency band you have chosen, showing the density of recent RF measurements.

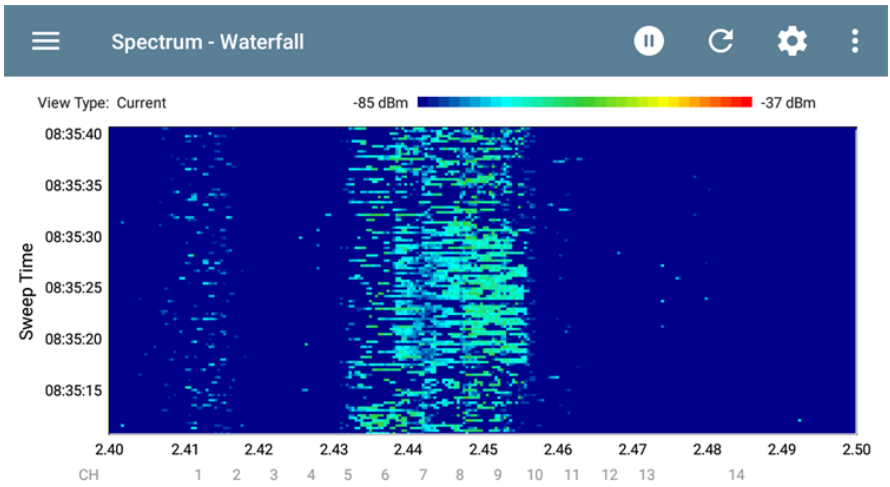


- Blues and greens ("cool" colors) indicate less RF detected at that frequency and amplitude.
- Yellow, orange, and red ("hot" colors) indicate the repeated presence of RF at that frequency and amplitude.

- Darkest blue indicates infrequent RFs while red indicates the continuous presence of RF at that amplitude.

Waterfall View

The Waterfall display draws new data at the top of the display as it scrolls older data downwards over a 2-minute interval. This provides a visualization of RF activity over time.



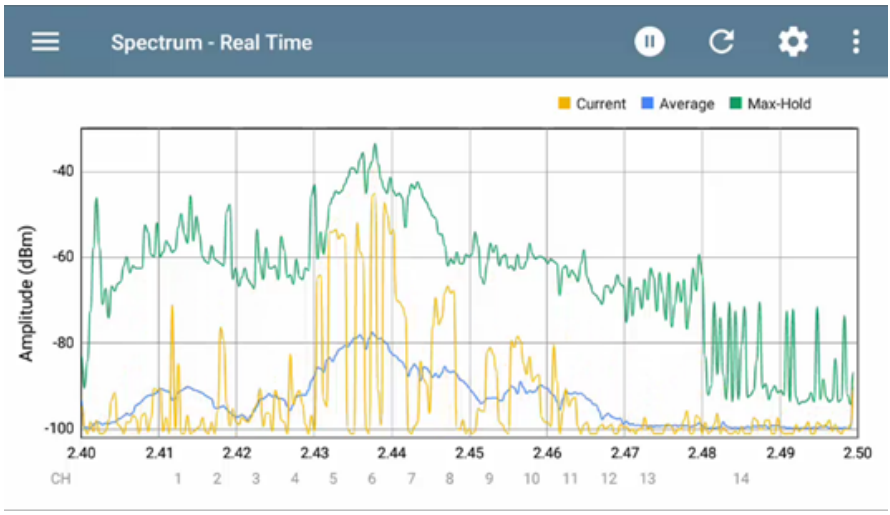
- The vertical access shows the measurement time, and the horizontal axis shows frequencies and channels.
- The colors in the waterfall represent the amplitude of a frequency at a certain time according to the scale in the upper right. Dark blue shows lower amplitude

measurements, and lighter colors show higher amplitude signals. More colors indicate more activity. For example, in the waterfall shown above, a speed test is running on Channel 8.

- The waterfall has two view types. Use Current to detect instantaneous RF. To smooth the data and see overall usage, change the type to Average 5 Sweeps, which averages five sweeps for each new line of data. This decreases the data resolution but may make the data easier to interpret in highly active RF environments. (See "Changing Spectrum Settings" on page 662 for instructions on changing the type.)

Real Time View

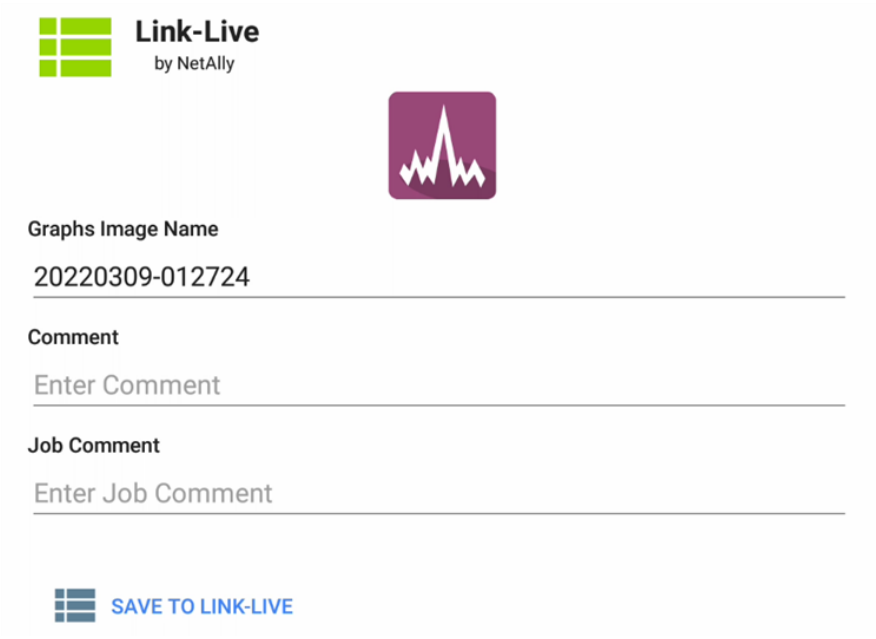
The Real Time display shows the current values across the frequency band with colorized lines for the current measurement, the average measurement, and the highest measured value (Max-Hold).



- The yellow line indicates the current values.
- The blue line indicates the average values, which are calculated using all measurements accumulated since the graph was last cleared.
- The green line indicates the highest measured value (Max-Hold).

Uploading Results to Link-Live

To send your Spectrum results to the Link-Live website, tap the action overflow icon ⋮ at the top right of the Spectrum screen, and then tap **Upload graphs to Link-Live**.



The Link-Live sharing screen opens. The system creates a file name automatically using the date. You can also enter optional Comments and Job Comments to attach to the results file. The results are displayed as images on Link-Live.com.

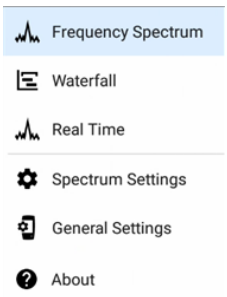
Spectrum Settings

The Spectrum navigation drawer allows you to change the data views, change frequency bands, change the Waterfall display type, and save settings.

Changing Spectrum Views

To change the Spectrum view:

1. Tap the Menu icon to open the Spectrum navigation drawer:



2. Select the view that you want: Frequency Spectrum, Waterfall, or Real Time. See "Using the Spectrum Views" on page 652 for information on using these views.

Saving Settings

To save the current Spectrum settings, tap the Save icon in the upper right corner of the

Spectrum Settings screen. This opens a menu for you to **Load**, **Save As**, **Import**, or **Export** any changes you make to the settings. See "Saving App Settings and Configurations" on page 145 for more information.

Changing Spectrum Settings

The Spectrum settings allow you to change the frequency band and to change the waterfall view type.

To change settings, tap the settings icon or tap the Menu icon and select **Spectrum Settings** from the Spectrum navigation drawer. Either action opens the Spectrum settings window:

To change the frequency band:

1. Tap **Wi-Fi Band**. This opens a selection box.
2. Tap the button for the frequency band you want, and then tap **OK** to return to Spectrum Settings.
3. Tap **OK** to return to Spectrum Settings.
4. Tap the back button  to return to the Spectrum view.

To change the waterfall view type:

1. Tap **Waterfall View Type**. This opens a selection box.
2. Tap the button for either **Current** or **Average-5 Sweeps**.
   - **Current** maintains the default display for the Waterfall view.
   - **Average-5 Sweeps** averages each line of waterfall data into five sweeps. This decreases some of the data resolution but may make the data easier to understand in highly active envir-onments.
3. Tap **OK** to return to Spectrum Settings.

4. Tap the back button  to return to the Spectrum view.

Back to Title and Contents

Performance Test App

The EtherScope nXG's line rate Performance Test provides point-to-point performance testing of a traffic stream across wired IPv4 network infrastructure. This test quantifies network performance in terms of target rate, throughput, loss, latency, and jitter.

The Performance test exchanges a stream of traffic with Peers or Reflectors and measures the performance of the traffic stream. You can simulate real-world traffic by configuring traffic flow, frame size, VLAN, and QoS options. Run the test at a full line rate of up to 10 Gbps for performance validation, or run at lower speeds to minimize disruption when troubleshooting operational networks.

The Performance Test runs from the Wired Test Port (top RJ-45 or Fiber port), and an AutoTest Wired Profile must connect successfully to establish link on the port. When you start up the EtherScope, the last Wired Profile in the list of active AutoTest profiles runs automatically if an active Ethernet connection is detected on the top RJ-45 port. Otherwise, you may need to manually run a Wired AutoTest to link. See Wired AutoTest Profiles to review.

Introduction to Performance Testing

Network performance is measured between a *Source* device, on which the test is configured and controlled, and up to four *Endpoint* devices that exchange traffic with the source. There are two endpoint types: Peers and Reflectors.

When using a Peer endpoint, separate upstream and downstream measurements can be shown for Throughput, Loss, Latency, and Jitter.

When using a Reflector, the EtherScope reports round-trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

The EtherScope nXG can act as the controlling Source for the performance test or as a Peer for a test conducted by different source device, such as another EtherScope nXG or a OneTouch AT 10G.

Other NetAlly testers work with the EtherScope to perform network performance testing:

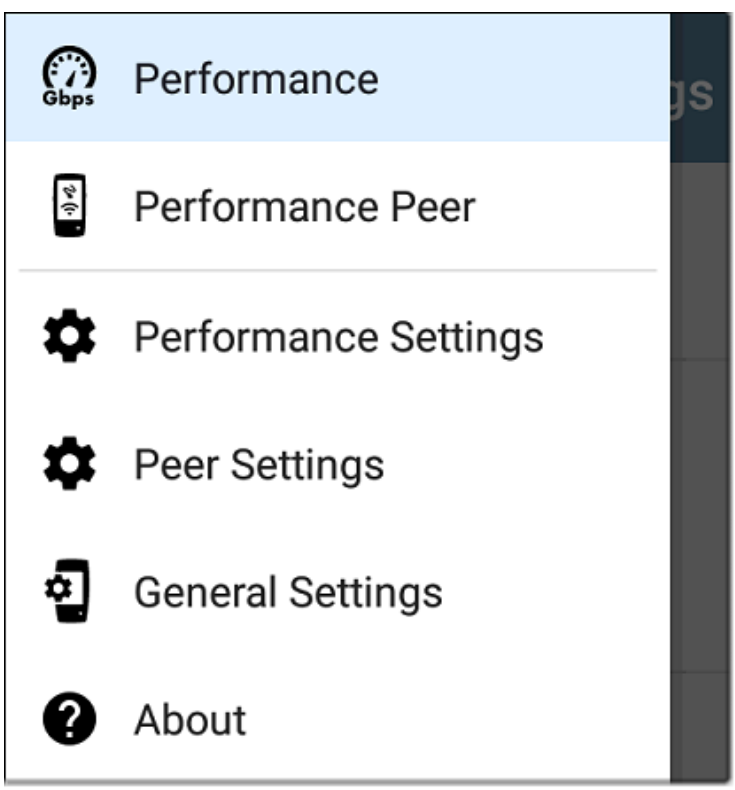
- **OneTouch AT 10G** can act as the Source or a Peer for Performance tests. (NetAlly.com/products/OneTap)
- **LinkRunner AT** and **LinkRunner G2** each have a Reflector feature for exchanging Performance test traffic. (NetAlly.com/products/LinkRunner G2)
- NetAlly's **Network Performance Test (NPT) Reflector** PC application can also act as the reflector for a Performance test. Download the free NPT Reflector software from NetAlly.com/support/downloads. Select EtherScope nXG from the drop-down menu to view the list of downloads.

In this Chapter

Performance Test Settings

The Performance app has both **Performance** settings that apply when the EtherScope is acting as the test source, and **Peer** settings that control the unit when it is acting as the test Peer.

Access the settings by tapping the settings button on the Performance Test screen or the Performance Peer screen, or open the left-side navigation drawer in the Performance app.



Performance goes to the main Performance test results screen.

Performance Peer opens the Peer results screen.

Performance Settings control the performance test settings when the EtherScope is the source.

Peer Settings control the EtherScope Performance Peer when another device is the source. See Running EtherScope nXG as a Performance Peer.

Saving Custom Performance Tests

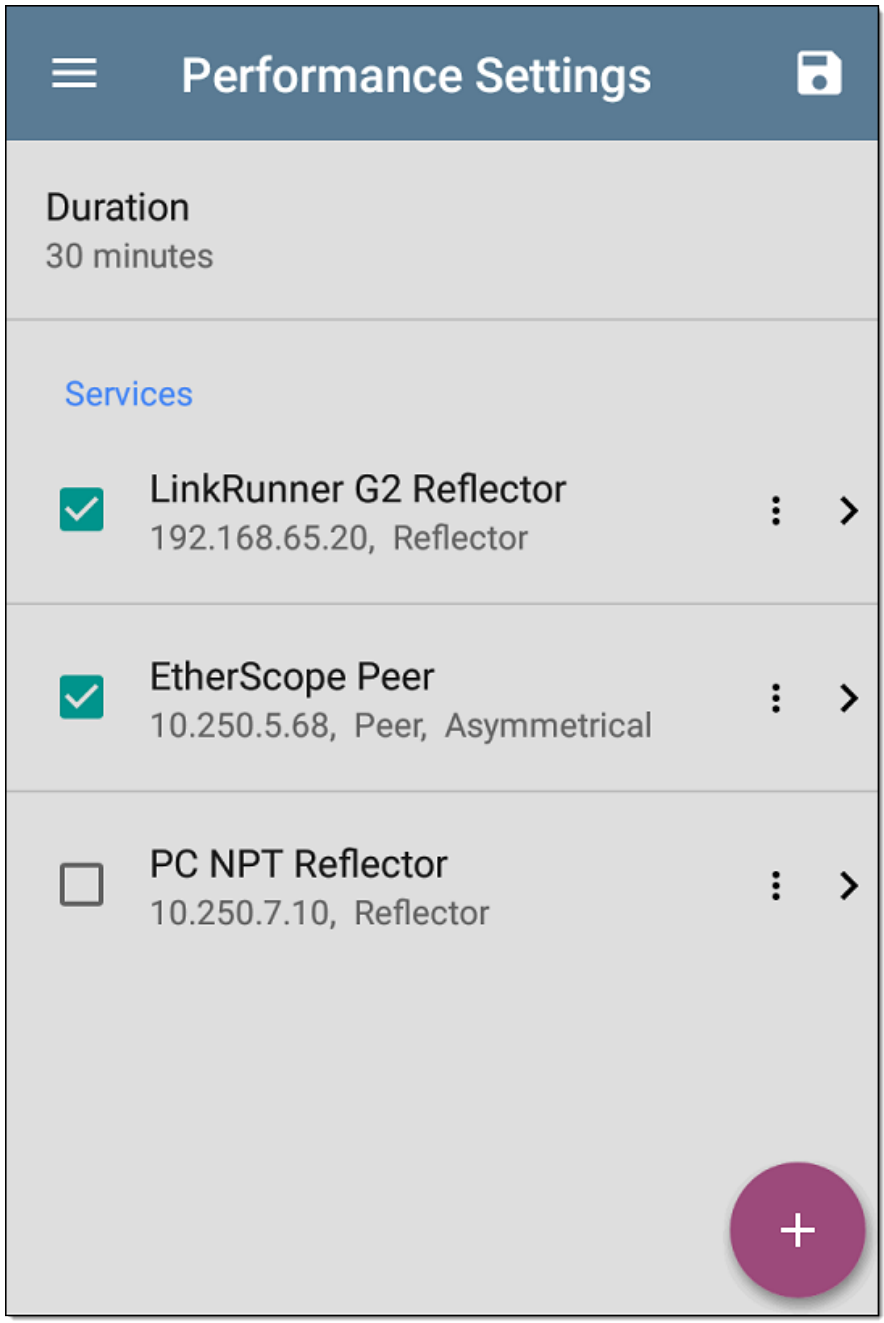
The Performance app allows you to save two levels of test configurations: individual **Services** and complete **Performance Tests** with *up to eight* enabled Services.

- **Services** include the Endpoint, Frame Size, Bandwidth, grading Thresholds, and Layer 2 and 3 Options. Services can be used in any number of saved Performance Tests.
- Saved **Performance Tests** contain a test Duration setting and the included Services.

For example, you can configure Services for multiple endpoints at different locations and with different bandwidths. A user can also create multiple Services with different QoS priorities (using the Layer 3 options) to verify that loss does not occur over the higher priority stream.

Saved Performance Tests and their Services work much like AutoTest Profile Groups, Profiles, and Test Targets. See the AutoTest Overview to review.

Open the Performance Settings screen  from the main Performance results screen or the left-side navigation drawer  .

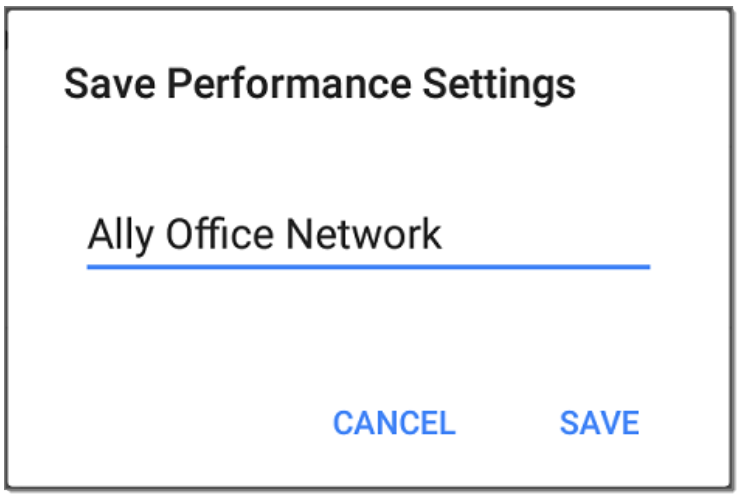


Tap the save icon to load, save, import, or export a settings configuration.

- **Load**: Open a previously saved settings configuration.

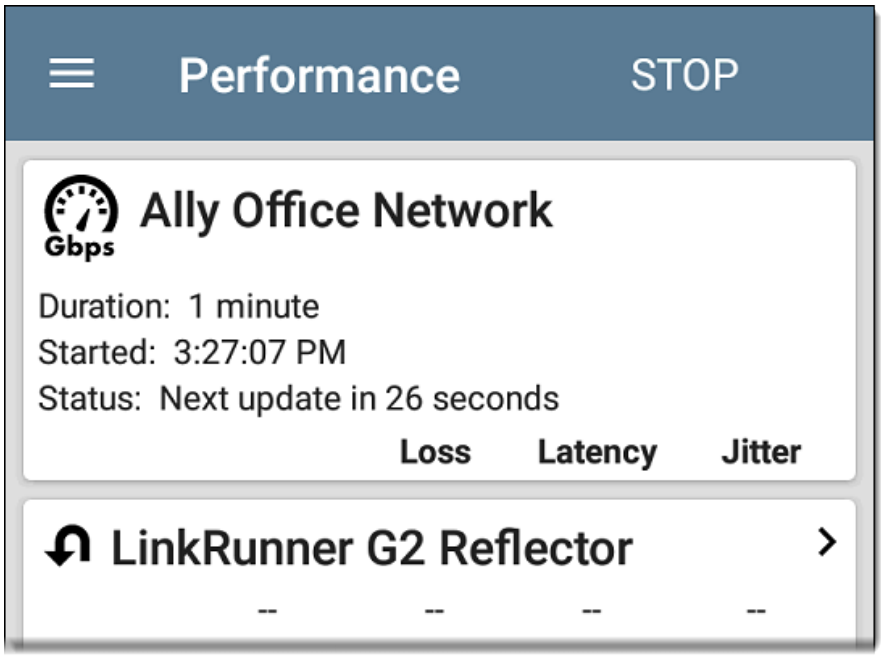
- **Save As**: Save the current settings with an existing name or a new custom name.
- **Import**: Import a previously exported settings file.
- **Export**: Create an export file of the current settings, and save it to internal or connected external storage.

See Saving App Settings Configurations for more instructions.



In the example images here, the user has saved a custom Performance Test called "Ally Office Network."

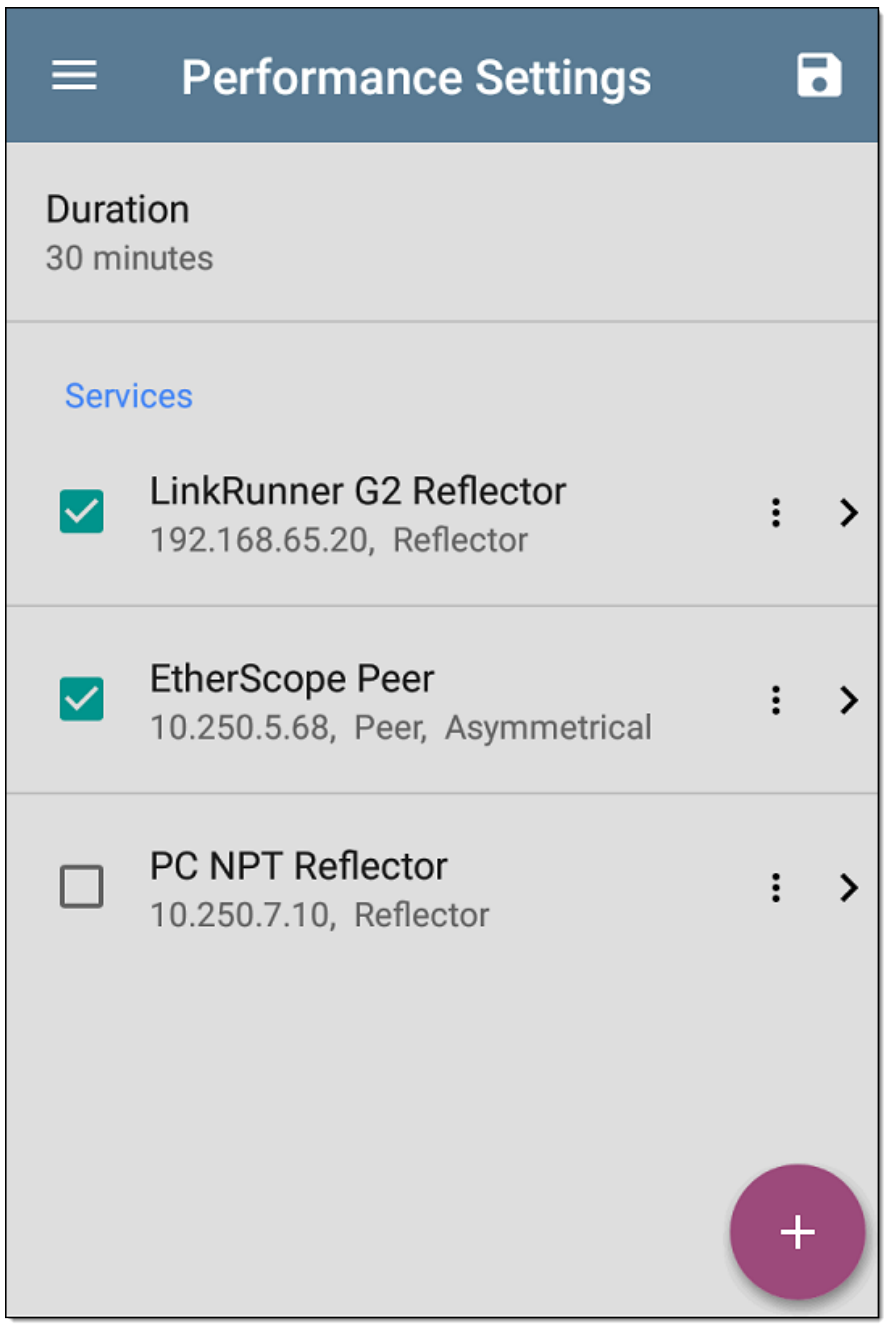
Once you save a Performance Test configuration, the custom name you entered appears at the top of the Performance Settings screen (above) and main Performance Test screen (below).



Back to Title and Contents

Configuring the Source EtherScope nXG

Open the Performance Settings screen from the main Performance results screen or the left-side navigation drawer.



Changed settings are automatically applied. When you finish configuring, tap the back button  to return to the Performance test screen.

Duration: This setting is the length of time the Performance test runs. Tap the field to select a new duration. The default is 1 minute.

Services

A Service is a configured traffic flow that simulates application traffic. You can run up to four unidirectional or bidirectional services simultaneously to emulate and test the QoS levels on your network.

The Services configurations include the Endpoints, Frame Size, Bandwidth, Thresholds, and Options the EtherScope uses to measure and grade performance.

Your collection of configured Services is available across all of your saved Performance Test configurations, and if you delete a Service, it is deleted from all Performance Tests.

On the Performance Settings screen, you can perform the following actions:

- Check or uncheck the boxes to include or exclude Services in the list of active Performance tests.

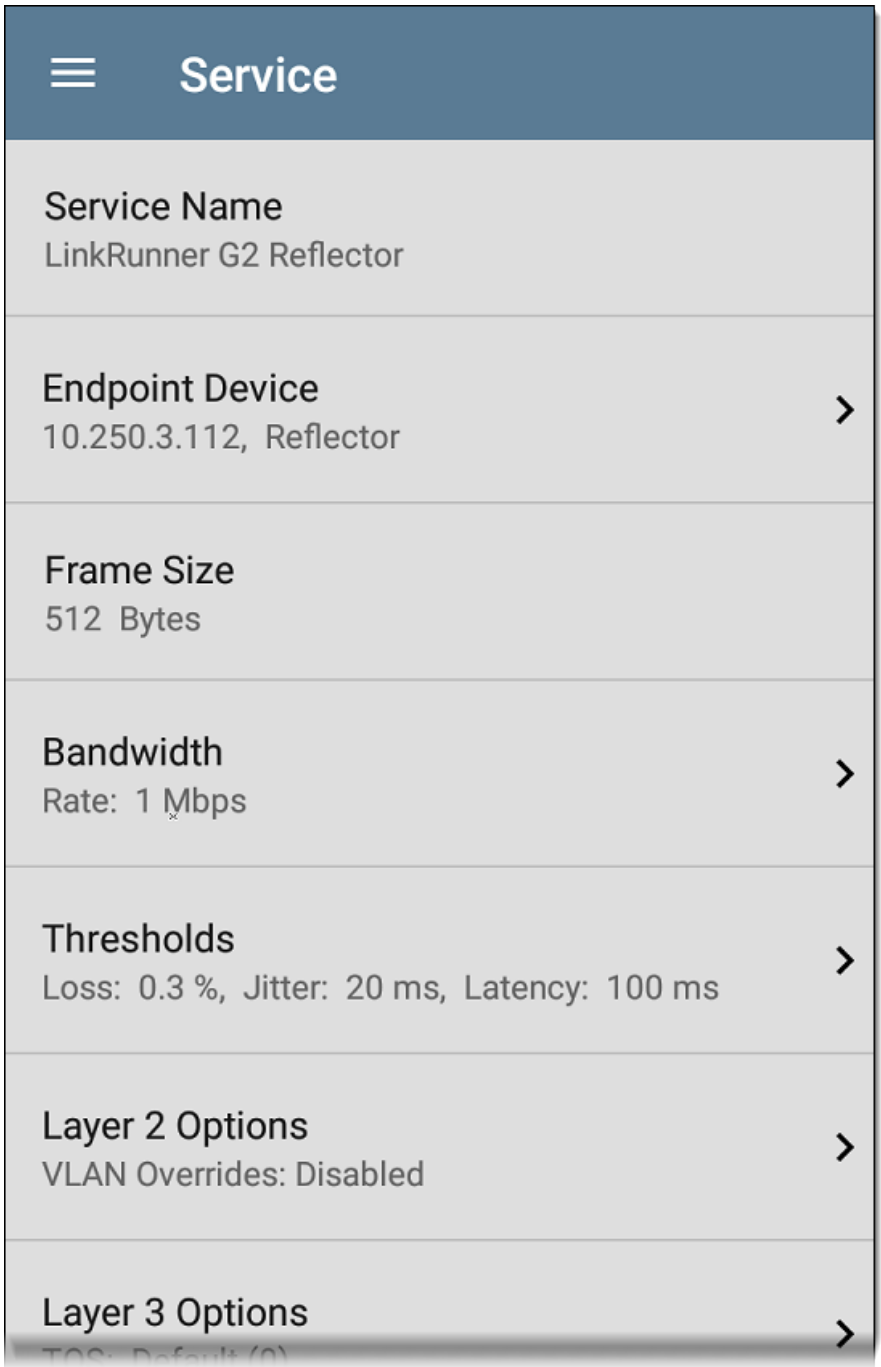
  NOTE: You can run a Performance Test on up to eight Services at once. If you select more than eight Services, the Performance Test fails.

- Tap the action overflow icon ⋮ to **Duplicate**, **Move Up/Down**, or **Delete** a configured Service.
  CAUTION: When you delete a Service, you delete it from all Performance Test configurations. To remove a Service from the current test, simply uncheck it.

  NOTE: All Services are tested at the same time, so the order of Services listed on this screen does not affect how the test runs.

- Tap the FAB icon  to add a new Service.

- Tap any Service's name, or add a new Service, to open its settings, where you can enter a custom Service name, endpoint address, performance thresholds, and other Service characteristics.



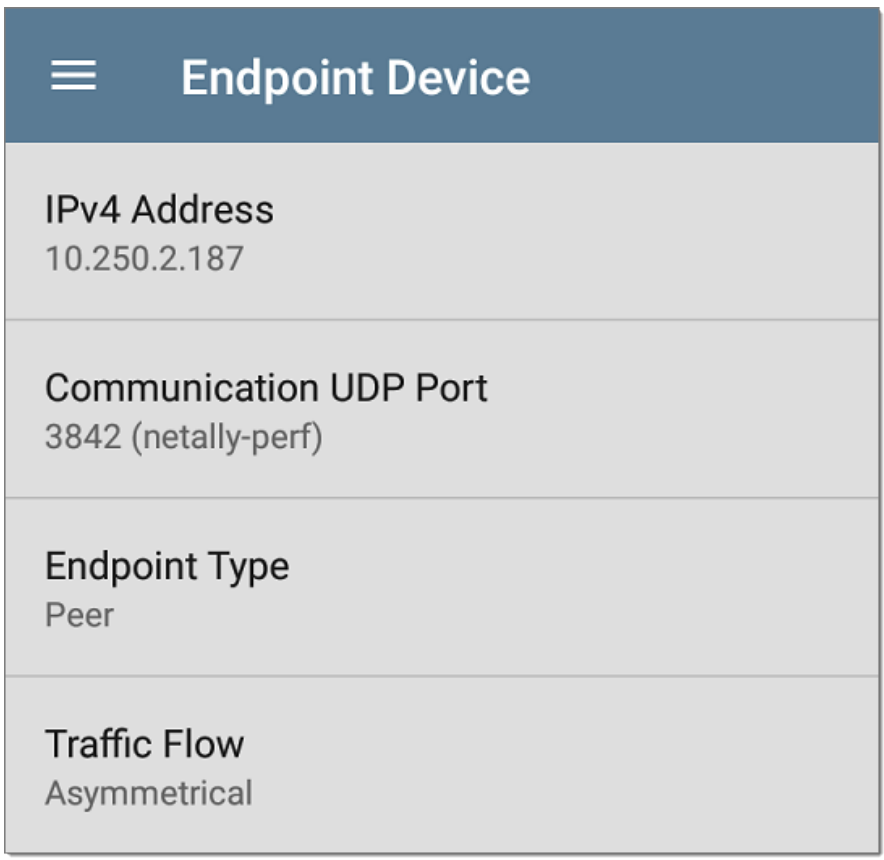
Service Name

Tap the **Service Name** field to enter a custom name for the endpoint and associated settings.

This name appears on the Services screen and the Performance test screen.

Endpoint Device

Open this screen to configure the Endpoint Address, Type, and Traffic Flow.



IPv4 Address: Tap the field to enter the IPv4 address of your endpoint device.

Communication UDP Port: If needed, tap to enter a different UDP Port number. The default NetAlly performance test port is 3842.

NOTE: The UDP port number entered here must match the port number used by your Peer endpoint device.

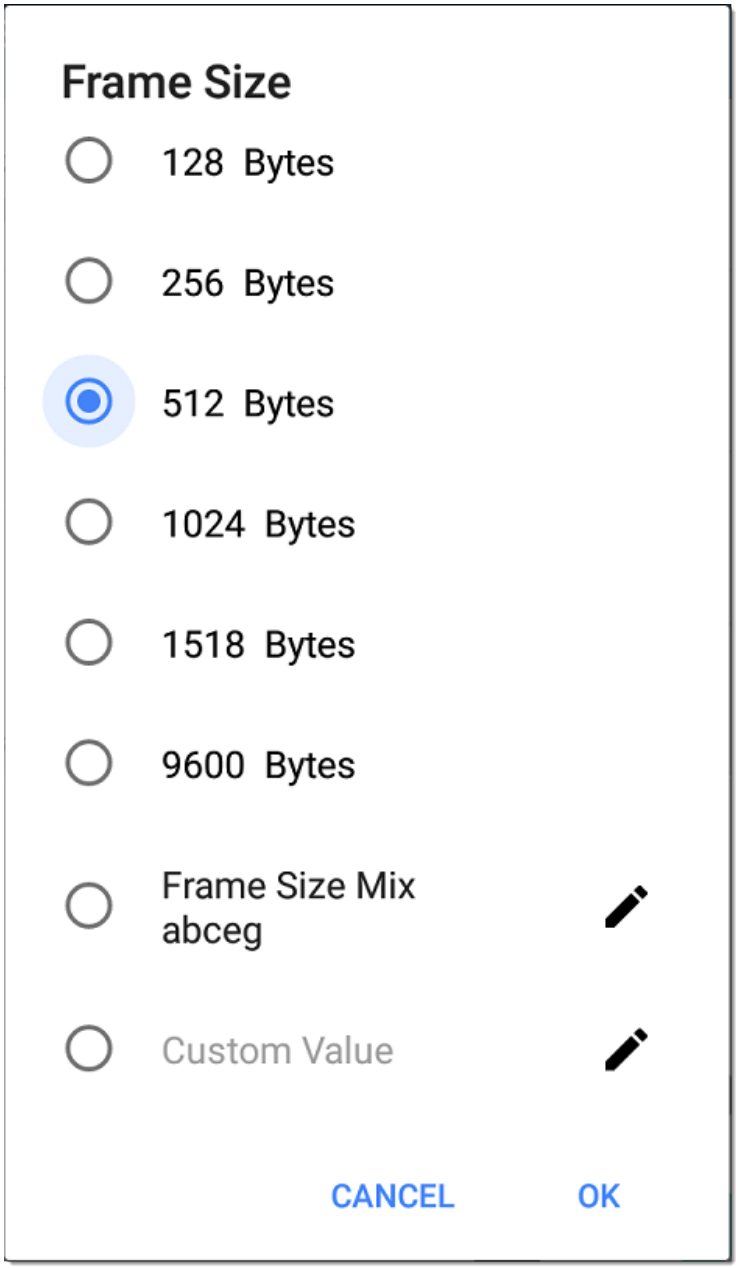
Endpoint Type: Select **Peer** or **Reflector** depending on the type of endpoint you are using for the performance test.

Traffic Flow: This setting only appears when **Endpoint Type** is set to **Peer**.

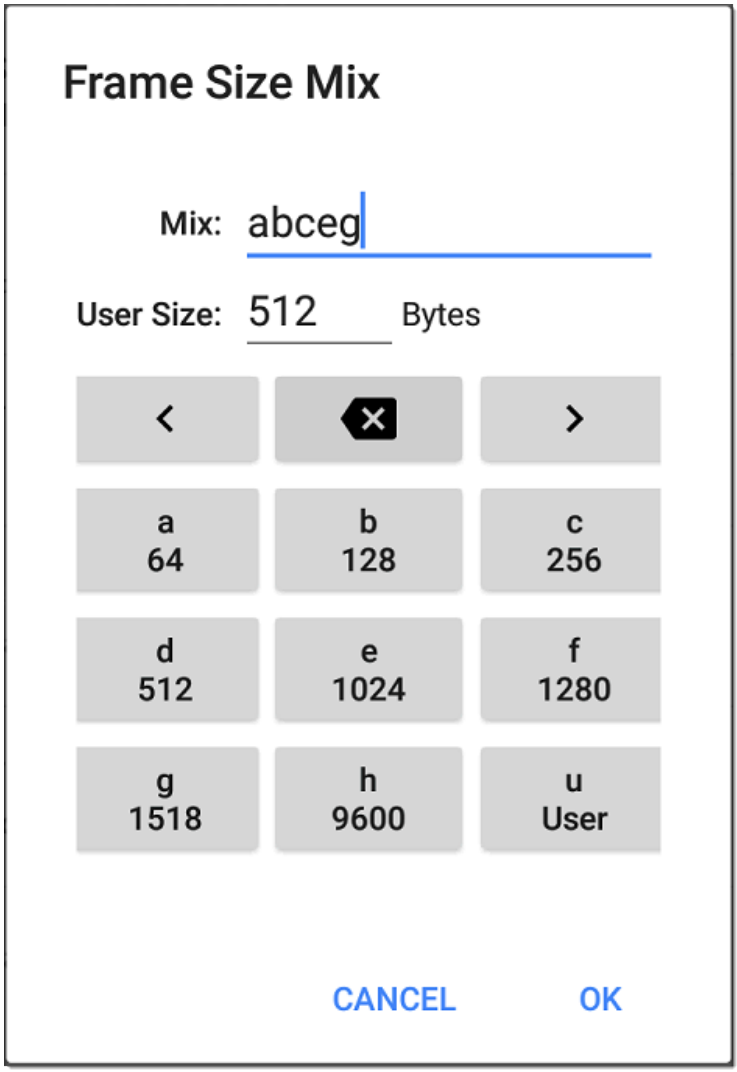
- Select **Upstream only** or **Downstream only** to test only the single traffic flow direction specified.
- Select **Asymmetrical** to test each direction using a different **Target Rate** (set under **Bandwidth** below). Asymmetrical is the default traffic flow for a Peer endpoint.
- Select **Symmetrical** to test both directions using the same Target Rate.

Frame Size

Tap the **Frame Size** field to select a new single frame size, the Frame Size Mix option, or to enter a Custom Value. The default is 512 bytes.



Selecting **Frame Size Mix** creates traffic with variable frame size patterns, generated in a repeating sequence. Tap the edit icon ✎ to revise the frame size pattern.



On the Frame Size Mix keyboard shown above, each letter (a through h) is associated with a frame size. The default pattern is "abceg," meaning the traffic pattern follow a repeating sequence of 64, 128, 256, 1024, and 1518 bytes. Use the letter keys along with the arrows and backspace button to edit the mix sequence as desired.

The **u** key enters a user-defined size into the mix. Select the field next to **User Size:** to enter your desired frame size, between 64 and 9600 bytes. Tap the **u** key to insert the new size where you want it in the pattern.

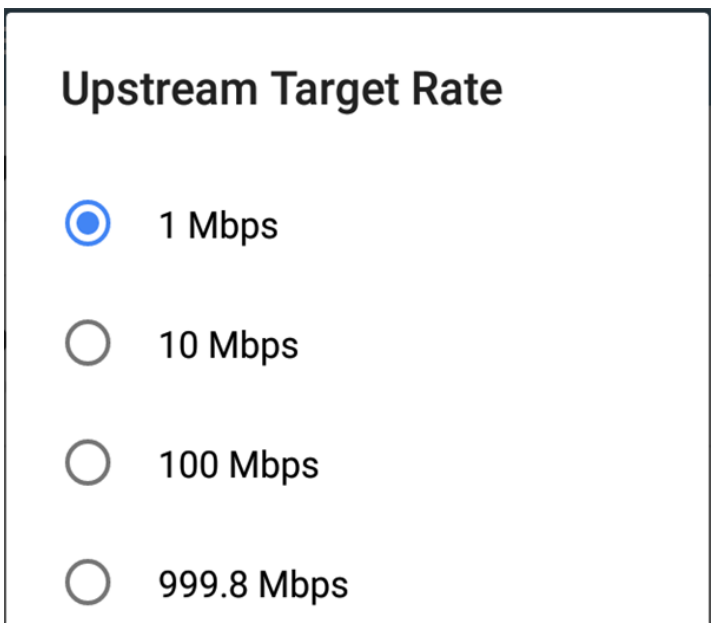
> NOTE: If the Performance Test runs on a VLAN (configured in the Wired AutoTest Profile or the Performance Layer 2 options shown below), the frame sizes are four bytes longer. You do not need to account for this frame size increase in the settings.

Bandwidth

Tap to open the **Bandwidth** screen and select or enter a **Target Rate** for one or both traffic directions.

- If you are configuring a Reflector endpoint or you have selected Symmetrical Traffic Flow for a Peer endpoint, only one Target Rate is used.
- For a Peer with an Asymmetrical Traffic Flow configuration, you can select a different Upstream and Downstream Target Rate for each direction.

Tap the **Target Rate** field(s) to select or enter a new rate.



Target Rate: The requested rate of round-trip traffic

Upstream Target Rate: This is the requested rate of upstream traffic, from the source to the endpoint.

Downstream Target Rate: This is the requested rate of downstream traffic, from the endpoint to the source.

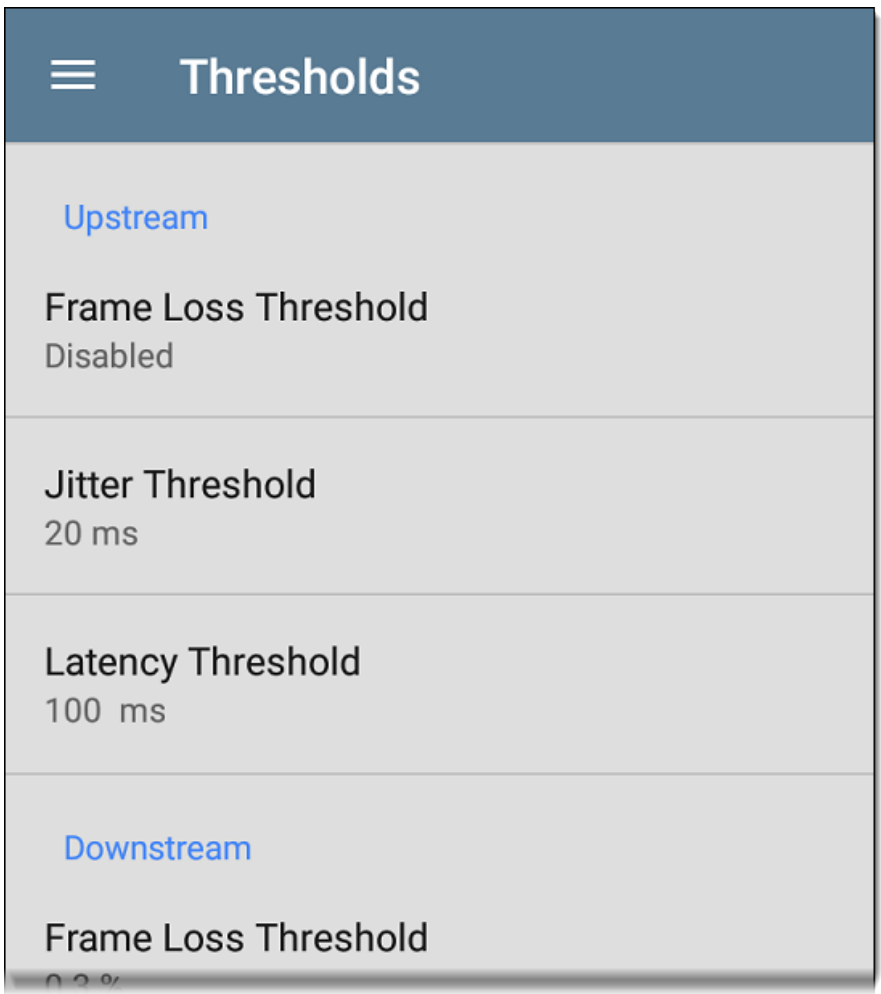
> NOTE: The 99.98 Mbps and similar values provided in the Target Rate options are meant to test the maximum, worst case throughput on an Ethernet link. Though greater rates are possible under perfect conditions, the limitation of 99.98% of the link rate results from asynchronous clocks in Ethernet. The IEEE 802.3 Ethernet standard allows link partners to differ by up to 0.02% of their clock signals. Therefore, end-to-end throughput in the worst case may be limited to 99.98% of the source link rate when the traffic traverses a link and maximum clock differences occur between the two link partners.

Thresholds

Thresholds define the **Pass**/**Fail** criteria the EtherScope uses to grade the test. The

Performance Test thresholds are Frame Loss, Jitter, and Latency.

- If you are configuring a Reflector endpoint or you have selected Symmetrical Traffic Flow for a Peer endpoint, the same threshold values grade each traffic direction.
- For a Peer with an Asymmetrical Traffic Flow configuration, you can select different Upstream and Downstream thresholds.



Tap each Threshold field to select or enter the maximum value allowed. If a measured value exceeds the threshold value, the test fails.

Frame Loss Threshold: The Frame Loss Threshold is the percentage of frames that can be lost before the test fails. The default is 0.3%. Tap the field to select or enter a new threshold or to disable grading based on frame loss altogether.

Jitter Threshold: Jitter is a measure of the variation in frame-to-frame latency in milliseconds. The default threshold is 20 ms.

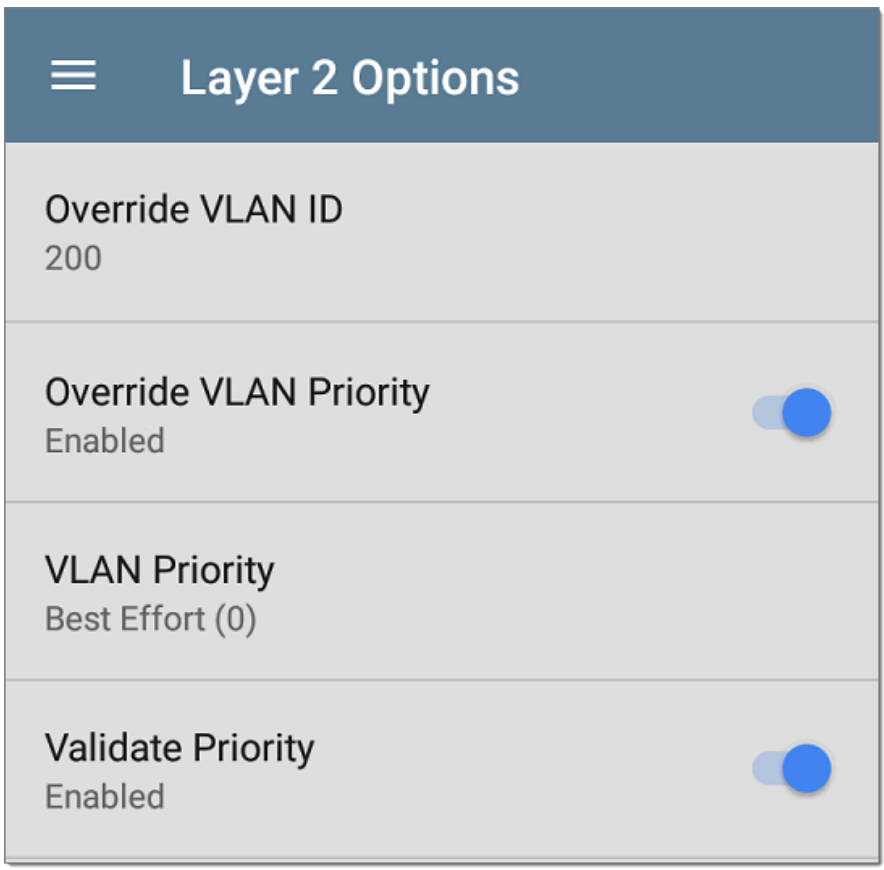
Latency Threshold: Latency is the amount of time it takes for a packet to go from the source to the endpoint and endpoint to source in milliseconds. The default threshold is 100 ms.

Layer 2 Options

The Performance Test runs over the Wired Test Port link established by an AutoTest Wired Profile. Therefore, by default, the Performance Test runs using the VLAN ID configured in the settings of the Wired AutoTest Profile that established the link.

To test other VLANs, for example, those that make up a trunk port, configure the Layer 2 Options in your separate Services to test the corresponding VLANs.

Open **Layer 2 Options** in the Performance app settings to override the VLAN settings from AutoTest.



Override VLAN ID: Tap to select or enter a VLAN ID number. The Override VLAN ID function tags frames with a particular VLAN (for example, a VLAN used for voice, video, or data). If Override

VLAN ID is not enabled, the VLAN is set to the value used for the Wired Test port.

Override VLAN Priority: Tap the toggle button to enable. By default, the VLAN priority is set to Best Effort (0). Use this setting to simulate a traffic stream of a certain type. If Override VLAN Priority is not enabled, the VLAN priority is set to the value used for the Wired Test port.

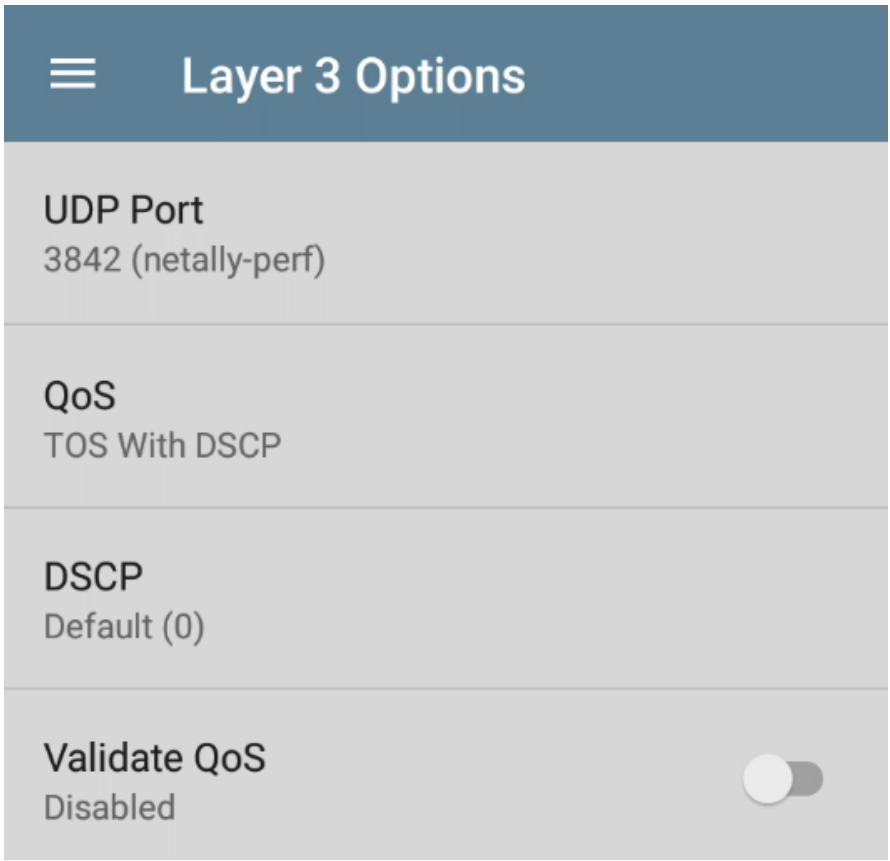
VLAN Priority: This setting only appears if the **Override VLAN Priority** setting above is Enabled. Tap to select a VLAN Priority.

Validate Priority: Tap the toggle button to enable the EtherScope to validate the selected VLAN priority. When the Validate Priority option is enabled, EtherScope checks the packets it receives to ensure that the priority field has been maintained from source to destination. If it has been altered, packets are counted as lost and included in the Frame Loss measurement.

Layer 3 Options

Layer 3 options are useful when testing QoS (Quality of Service) on your network. You can create up to four Services using different DSCP

priority or IP precedence to verify that loss does not occur on the higher priority streams.



UDP Port: Tap to enter a specific UDP port number. This can help you simulate prioritized traffic on ports reserved for specific uses such as video, voice, or backup data or to match ports allowed by a firewall.

QoS: Select the methodology used on your network: **TOS with DSCP** (Type of Service with Differentiated Services Code Point or **TOS with IP Precedence** (legacy). Then, configure the priority using the settings below.

DSCP: This field is only available when **TOS with DSCP** is selected in the setting above. Using the DSCP control, you can specify a priority for the generated traffic by changing its classification. This is a six-bit field. The default value of zero specifies “Best Effort.” Tap the field to select a different DSCP.

IP Precedence: This field is only available when **TOS with IP Precedence** is selected. Tap the field to select an IP Precedence other than the default of Routine (0).

IP Precedence Type: This field is also only available when **TOS with IP Precedence** is selected. Tap the field to select an IP Precedence Type other than the default of Normal (0).

Validate QoS: When this setting enabled, the EtherScope checks received packets to ensure that the QoS field has been maintained throughout the route. If the QoS field has been altered, packets are counted as lost.

Back to Title and Contents

Configuring Performance Endpoints

EtherScope nXG can run a Performance Test to any of the following Endpoints:

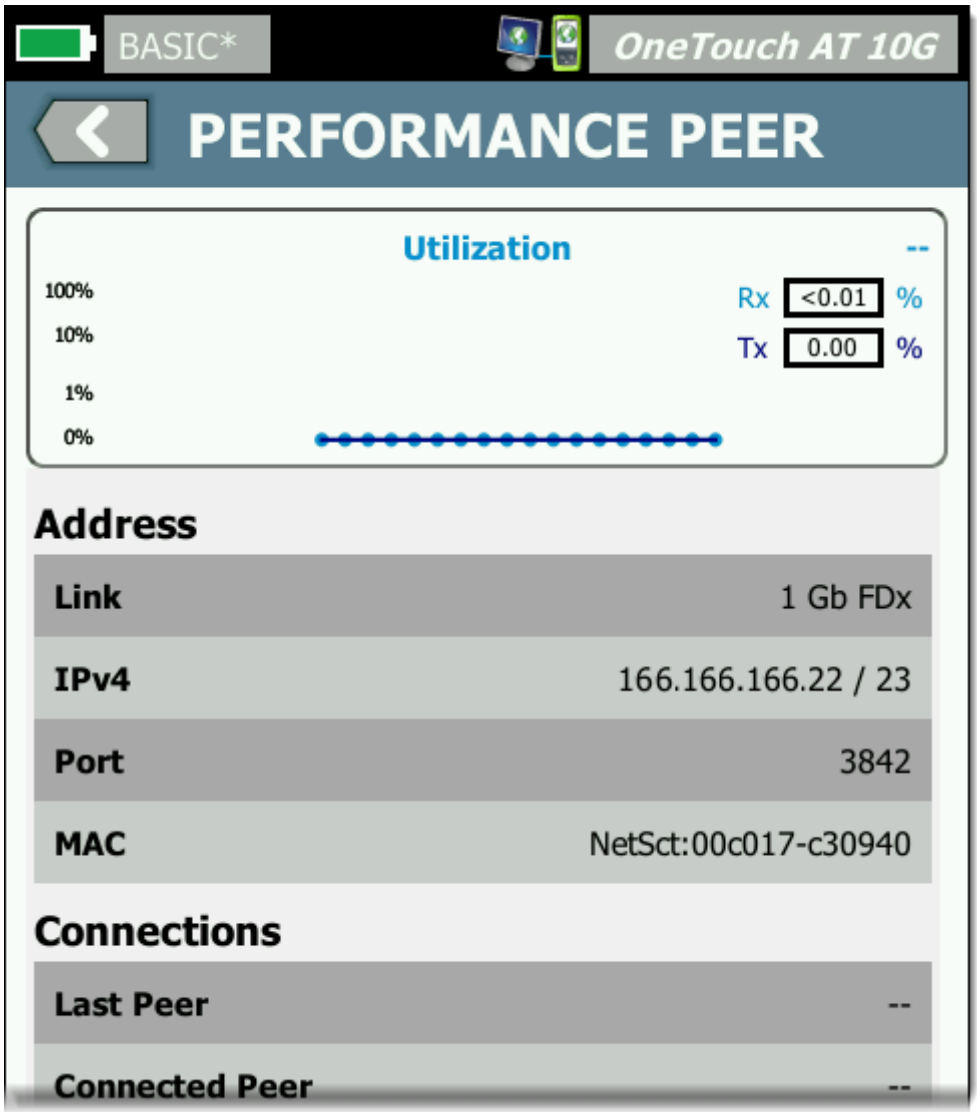
- Another EtherScope nXG (Peer)
- A OneTouch AT 10G (Peer)
- A LinkRunner G2 or LinkRunner AT (Reflector)
- NPT Reflector Software (Reflector)

See our website NetAlly.com for more information about OneTouch and LinkRunner and to download the free NPT Reflector PC application.

EtherScope Performance Peer

To run an EtherScope nXG as a Performance Peer, see the Running as a Performance Peer topic.

OneTouch 10G Performance Peer



Follow these steps to set up a OneTouch 10G Performance Peer:

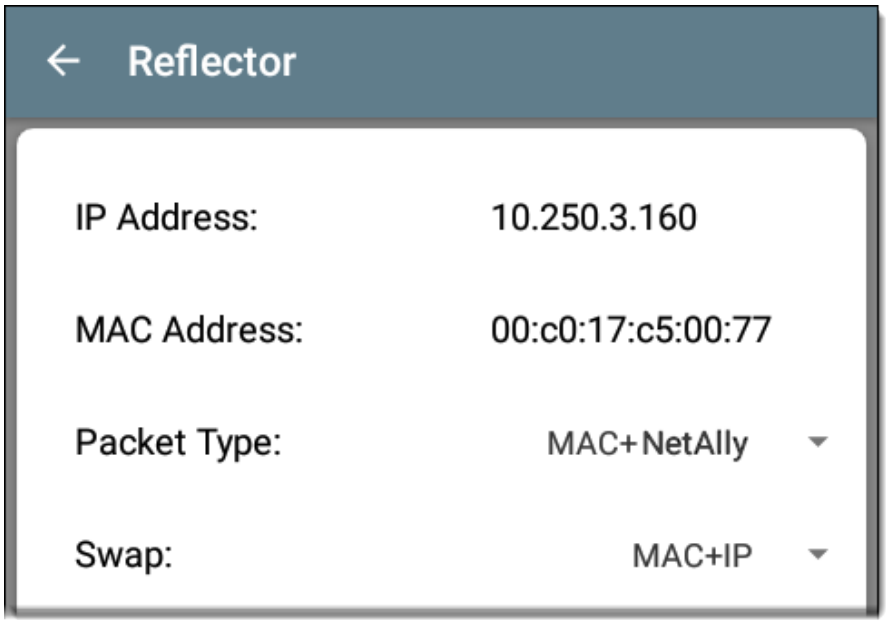
1. Ensure the OneTouch is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.

2. With the unit powered on, tap the TOOLS  icon on the Home screen.
3. In the TOOLS menu, select **Testing Tools > Performance Peer**.
4. Select the appropriate UDP **Port** number if other than the default of 3842.
   NOTE: The port number set on your endpoint must match the port number used by your source EtherScope.
5. Turn on **Enable AutoStart** to cause the Performance Peer function to start automatically when the OneTouch is powered on.
6. Tap the **START** button.

   The PERFORMANCE PEER screen appears, and a network link is automatically established.
7. The IPv4 address of the peer is displayed on the screen. Enter this address on the Endpoint Device screen in the EtherScope nXG's Performance test Services settings.

For additional details on the OneTouch Performance Peer, see the OneTouch 10G User Manual, available online.

LinkRunner G2 Reflector



Follow these steps to set up a LinkRunner G2 Reflector:

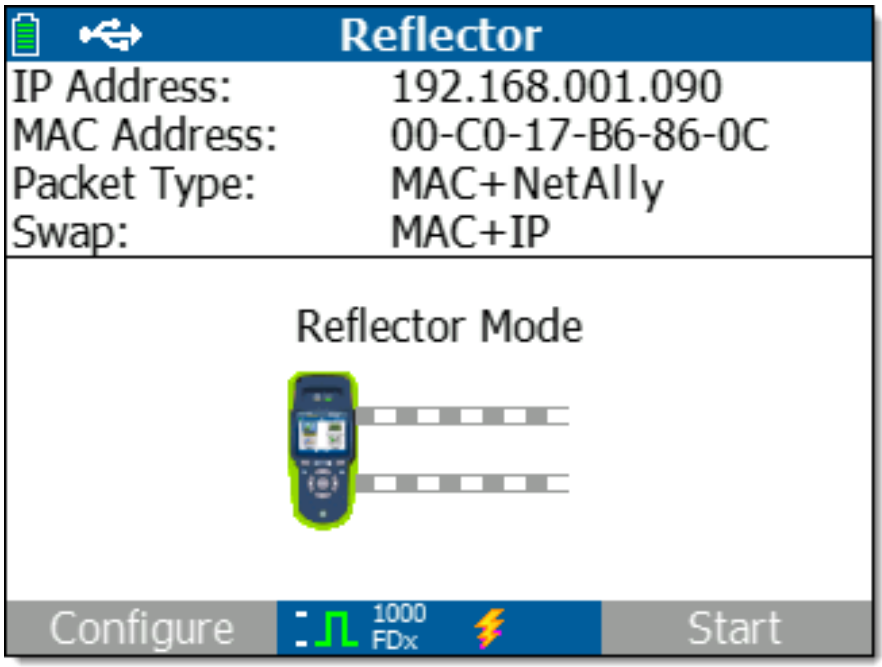
1. Ensure the LinkRunner is connected to an active network via the top RJ-45 or Fiber test port and is plugged into AC power.
2. Start the LinkRunner G2 testing application by tapping the NetAlly logo at the bottom of the screen.

3. In the testing app, open the left-side navigation drawer by tapping the menu button .
4. Select **Reflector** 

.
5. Configure the **Packet Type** and **Swap** settings as required. The default settings, Packet Type: MAC + NetAlly and Swap: MAC + IP, are recommended to avoid any undesired traffic on your network.
6. Once the LinkRunner G2 Reflector has acquired an IP address, tap the floating action button (FAB) at the lower right to start the Reflector.
7. The IP address of the Reflector is displayed at the top of the screen. Enter this address on the Endpoint Device screen in the EtherScope nXG's Performance Test Services settings.

For additional details on the LinkRunner G2 Reflector feature, see the User Guide on the LinkRunner G2 Home screen.

LinkRunner AT Reflector



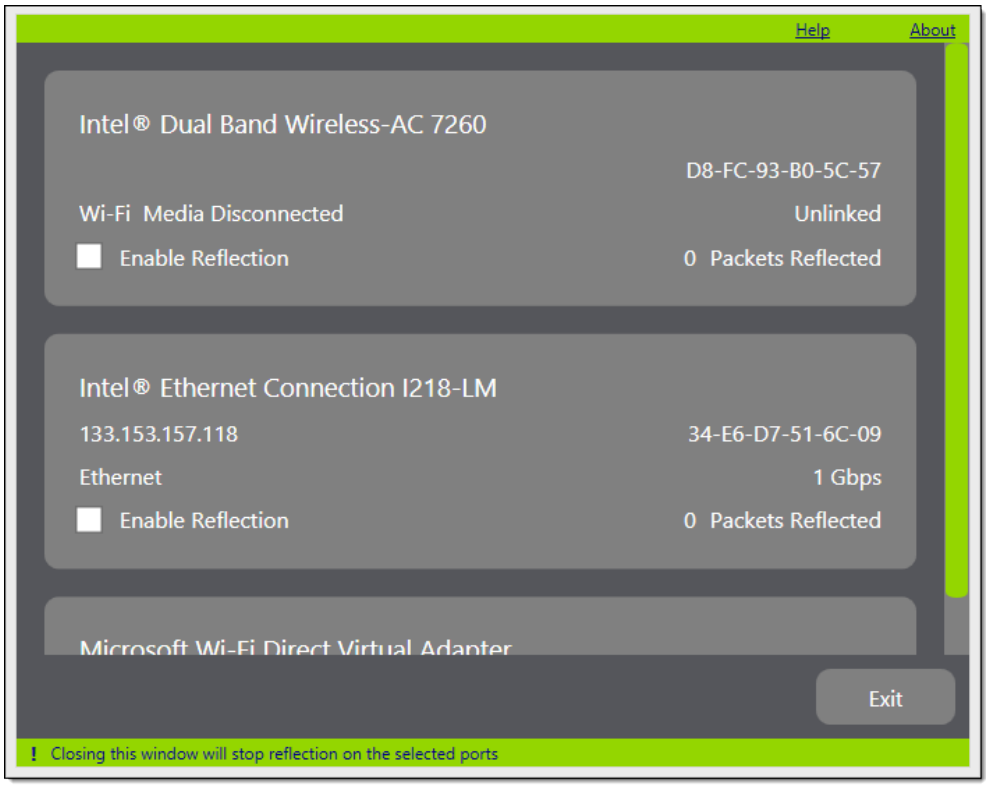
Follow these steps to set up a LinkRunner AT (2000) Reflector:

1. Ensure the LinkRunner is connected to an active network via the RJ-45 or Fiber test port and is plugged into AC power.
2. On the Home screen, select **Tools**.
3. In **General Configuration > Manage Power**, ensure the **Auto Shutoff Enabled** is unchecked to prevent the unit from powering down during the test. **Save** the changed setting.
4. In the Tools menu, select **Reflector**.

5. On the Reflector Screen, **Configure** the **Packet Type** and **Swap** settings as required. The default settings, **Packet Type: MAC + NetAlly** and **Swap: MAC + IP**, are recommended to avoid any undesired traffic on your network.
6. Select **Save** to apply any changed settings.
7. Select **Start** (F2) to run the Reflector.
8. The IP address of the Reflector is displayed at the top of the screen. Enter this address on the Endpoint Device screen in the EtherScope nXG's Performance test Services settings.

For additional details on the LinkRunner AT Reflector feature, see the LinkRunner AT User Manual, available online.

NPT Reflector Software



Follow these steps to set up the NPT Reflector PC application:

1. Download the software from NetAlly.com/support/downloads. Select EtherScope nXG from the drop-down menu to view the list of downloads.
2. Install the Reflector on your PC by running the .exe file.
3. Open the Reflector application.

Once open, the application automatically detects available network interfaces and their link status.

4. Check the box next to **Enable Reflection** for each network interface you want to use as a Reflector Endpoint for your Performance Test.
5. Leave the application window open on your PC during Performance testing.
6. Enter IP addresses for the interfaces you want to test against on the Endpoint Device screen in the EtherScope nXG's Performance Test Services settings.

Refer to the **Help** in the NPT Reflector software for additional information.

Running a Performance Test

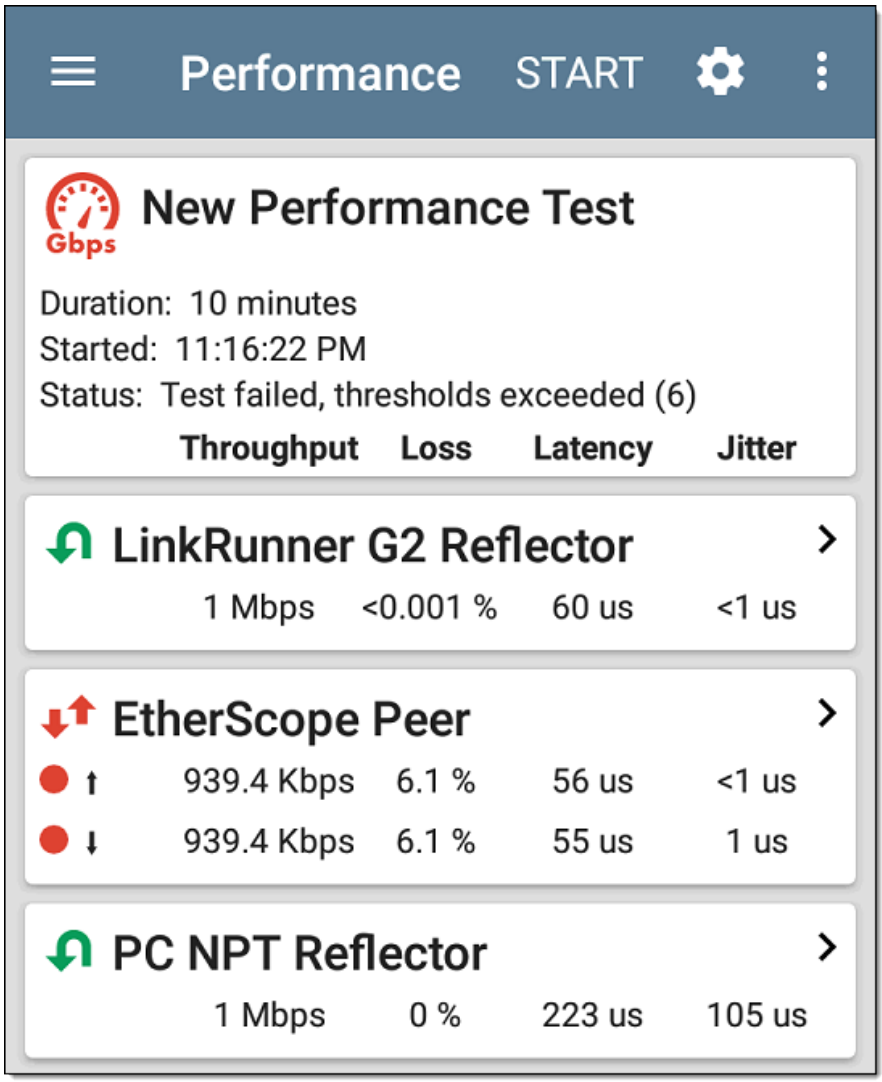
Note the following before running:

- The Performance Test can only run from the Wired Test Port (top RJ-45 or Fiber port), and an AutoTest Wired Profile must connect successfully to establish link on the port. If you receive a Status message such as "The wired test port is not linked" or "No IP address" but you have an active network connection, go to AutoTest and run a Wired Profile to troubleshoot your connection.
- All configured Performance Test Services are tested at the same time. If one Service fails to meet the thresholds for the test, the entire test fails.
- Only four Services can run at once. If you have selected more than four Services in the Performance Settings, the test fails with the Status message, "Too many services enabled (56)."

- Newly configured Services may not display on the main Performance Test screen until you tap START.

To run your configured Performance Test, tap **START** on the main Performance screen.

Performance Test Results



Performance results update every five seconds if you are using only Reflector endpoints, and/or an EtherScope nXG Peer running v1.2 or newer software, with a test Duration of 4 hours or less. If you are running a 10 second test, all results display after 10 seconds. Otherwise, results update every 30 seconds.

Performance Test results are presented on cards. The top card shows the test duration and status.

Duration: The test duration selected in the Performance Settings

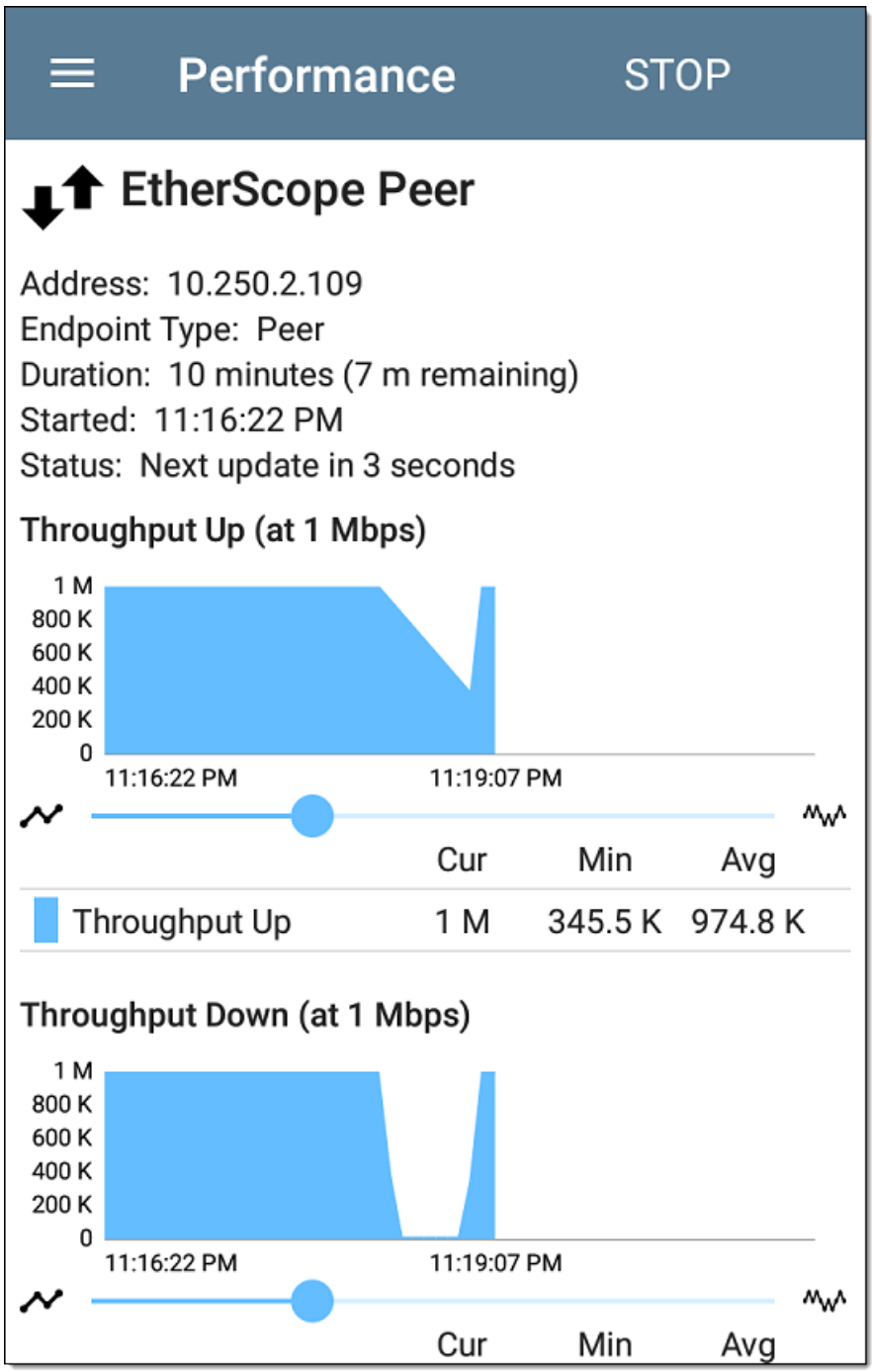
Started: Time at which the test began

Status: Current status of the test, including any error messages

Each card beneath corresponds to a configured Service and displays the Up, Down, or Round Trip measurements for Throughput, Loss, Latency, and Jitter. Remember, Peer endpoints can return Upstream and Downstream measurements, while Reflectors only provide round trip measurements.

Tap a Service card to view more details.

Performance Service Detailed Results



The Service results screen displays detailed test characteristics and graphs of performance.

Address: IP address of the endpoint

Endpoint Type: Peer or Reflector

Status: Current status of the test, including any error messages

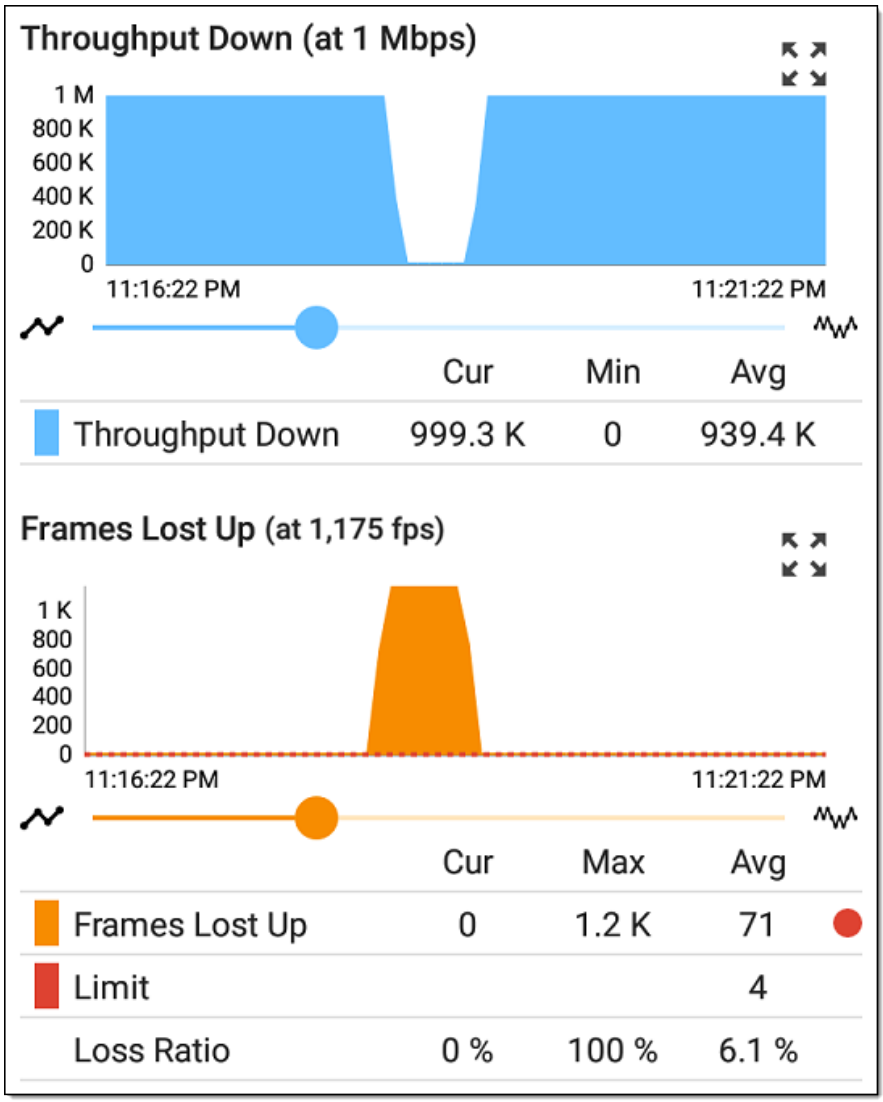
Rerunning Tests from Detailed Results

You can rerun a Performance Test from the detailed results screen by tapping **Start** at the top of the screen. This repeats the Performance Test *only* for the Service that you are viewing.

Throughput, Loss, Latency, and Jitter Graphs

The graphs described in this section update every 5 or 30 seconds for as long as the test is running. The graphs save and display data for the entire test duration, with a max duration of 24 hours.

Peer endpoints display separate Up and Down graphs (as shown below) for Throughput, Frames Lost, Latency, and Jitter, while Reflector endpoints display one round trip measurement for each.



Touch and drag (or swipe) left and right on each graph to move backward and forward in time, and double tap or move the slider to zoom in and out. See the Trending Graphs topic for an overview of the graph's pan and zoom controls.

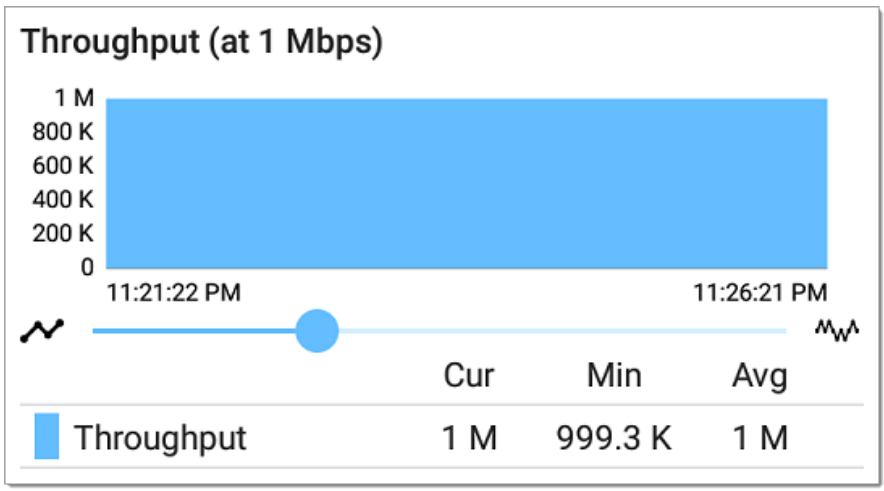
Graph Legends

Under each graph, a legend table indicates the meanings of the colors that correspond to

different measurements. The **Limit** shown for each graph is the set Threshold from the corresponding Service settings. Measurements that fall outside the Limit are indicated with a red dot next to the failing measurement. In the image above, the test has failed because Frames Lost Up was above the Limit.

The table also displays the Current, Maximum, and Average measurements. The Current columns contain measurements from the last interval (5 or 30 seconds). The Min, Max, and Avg columns show cumulative measurements gathered during the test duration.

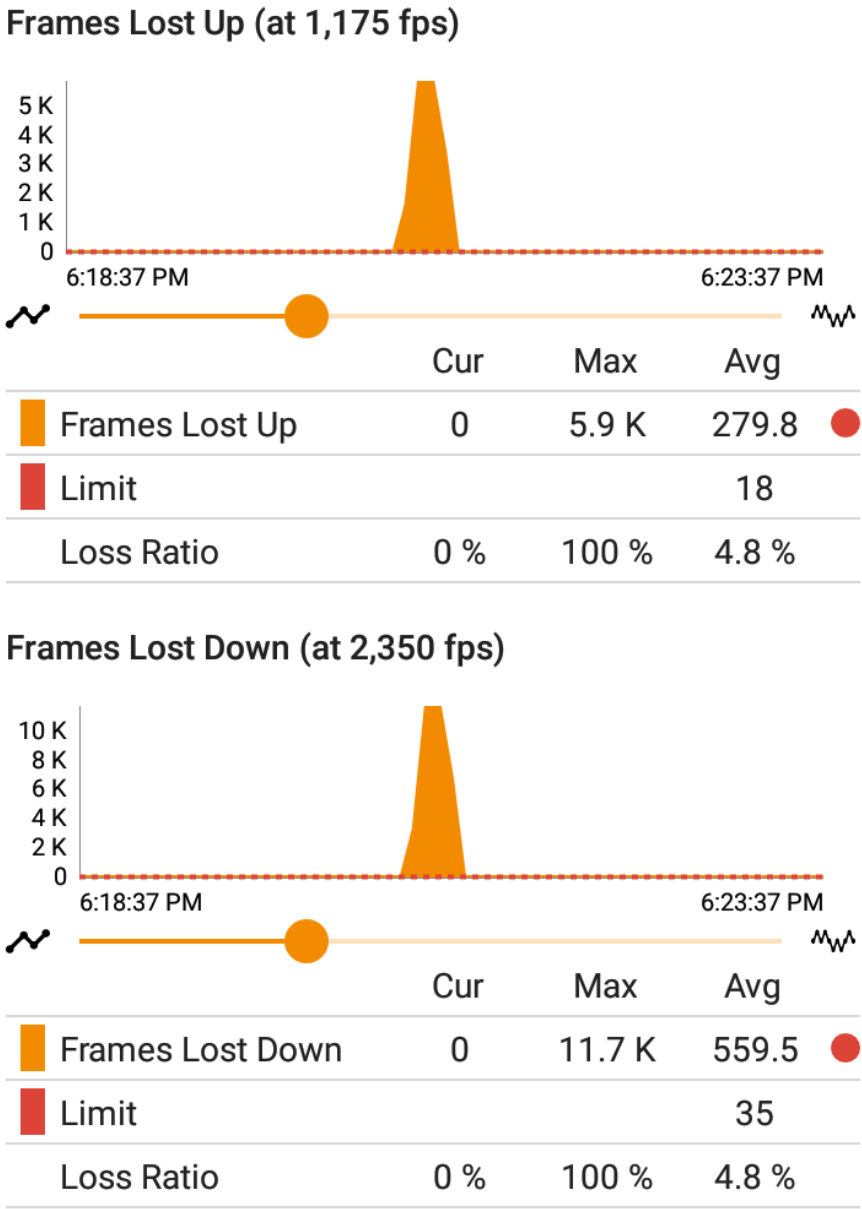
Throughput



Throughput (Up/Down) (at Target Rate): Throughput is the measured bit rate based on the number of frames sent and frames received.

The configured Target Rate from the Performance Settings is shown in parentheses next to the Throughput heading. In the image above, the configured Target Rate is 1 Mbps.

Loss



Frames Lost (Up/Down): Frame loss is quantified by the number of frames received subtracted from the number of frames sent.

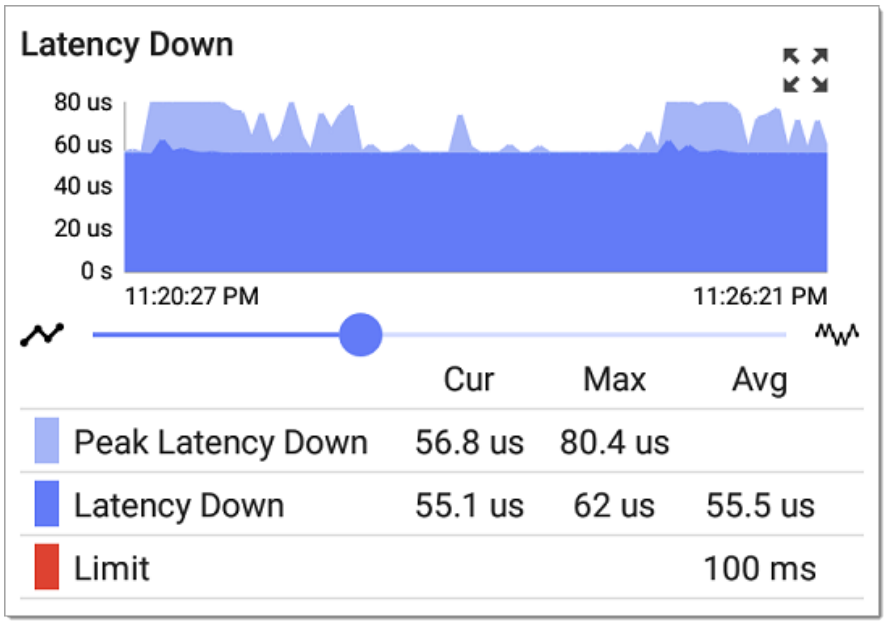
Limit: This is the Frame Loss Threshold for one interval. It is computed from the Frame Loss

Threshold, Frame Size, and Bandwidth settings for the Service. The Limit is also displayed on the graph as a horizontal red dotted line (if the measurements are close enough to the Limit value for it to appear on the graph).

Loss Ratio: The percentage of total frames that were lost

> NOTE (for 10G Rate Performance tests): Low-level electrostatic discharge (ESD) and low-power Electric Fast Transient (EFT) events, also called impulse noise, can interfere with newer, faster data links with less noise margin. These events could include static from a person's clothing or interference from electrical appliances and motorized equipment. When running a full 10G line rate test, ESD and EFT events can cause periodic spikes or a spike that then resolves on the Frame Loss graph.

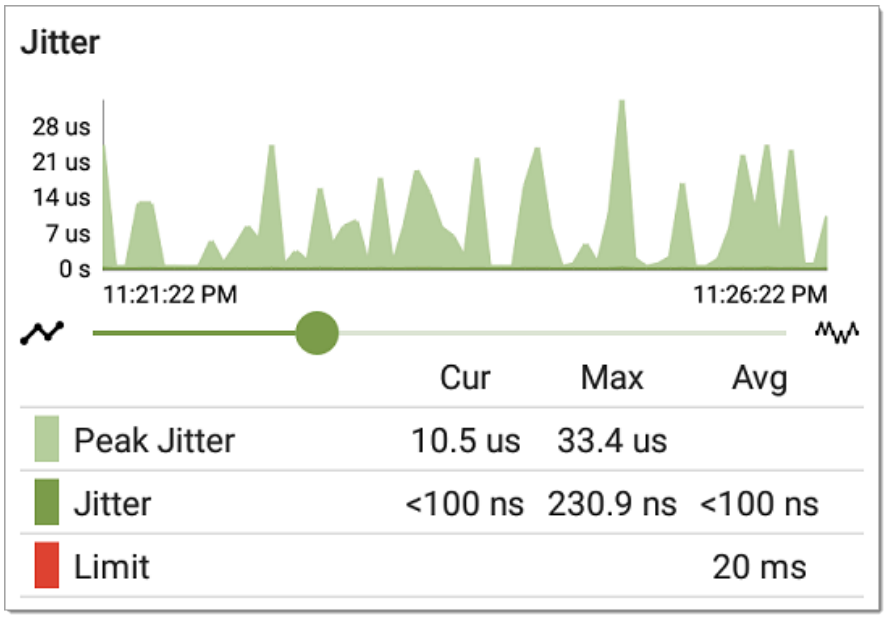
Latency



Latency (Up/Down): Latency is the amount of time it takes for a packet to go from the source to the endpoint or from the endpoint to the source (in milliseconds). Latency is calculated by averaging the thousands of latencies measured during each interval. The one-way latency measurements are actually round trip measurements, divided by two.

Peak Latency: The highest measured latency. The Current column shows Peak Latency from the last test interval, and Max shows the highest latency measured during the entire test.

Limit: This is the Latency Threshold from the Performance app's setting.



Jitter (Up/Down): Jitter is a measure of the variation in frame-to-frame latency in milliseconds.

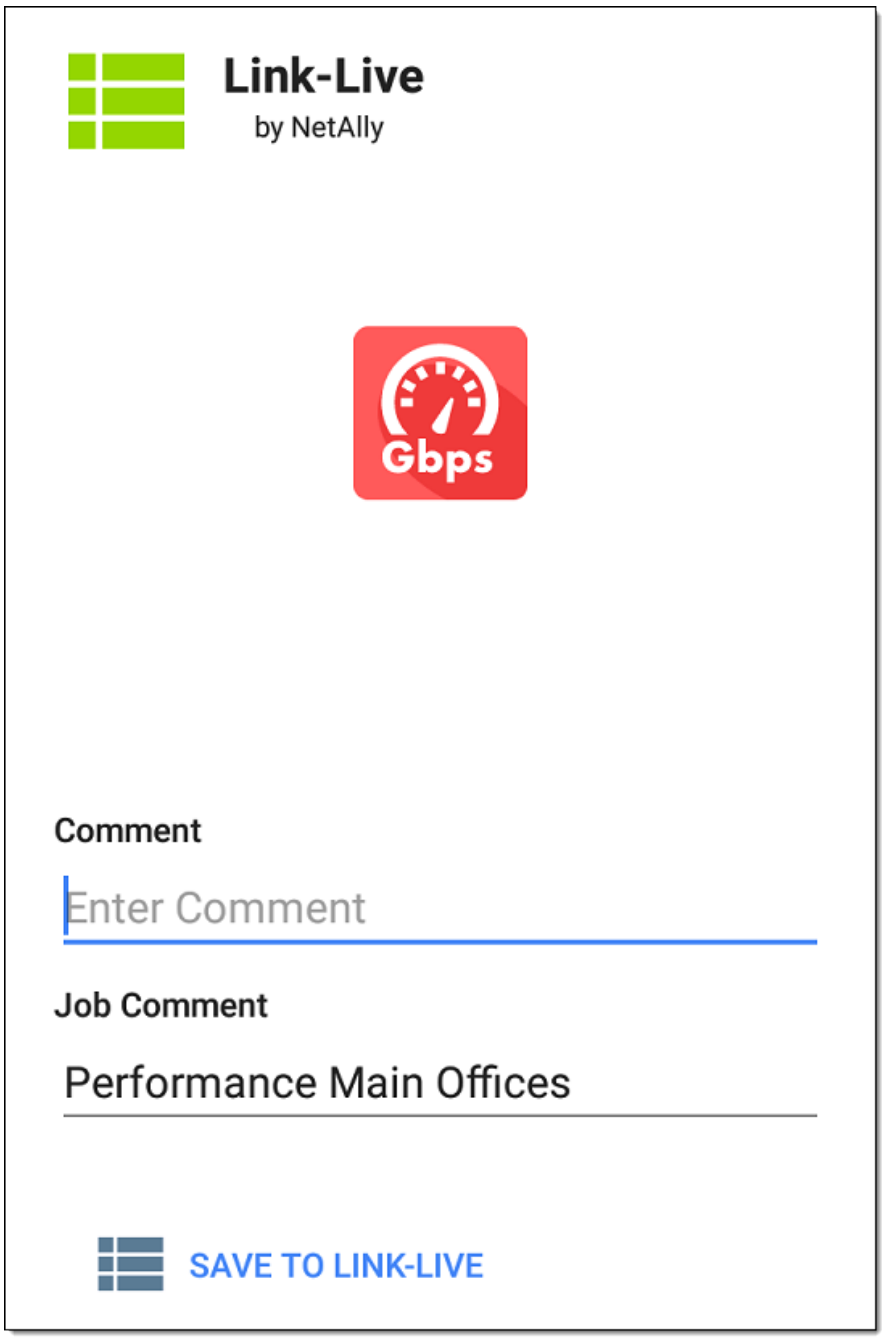
Peak Jitter: The highest measured Jitter. The Current column shows Peak Jitter from the last test interval, and Max shows the highest Jitter measured during the entire test.

Limit: This is the Jitter Threshold from the Performance app's settings.

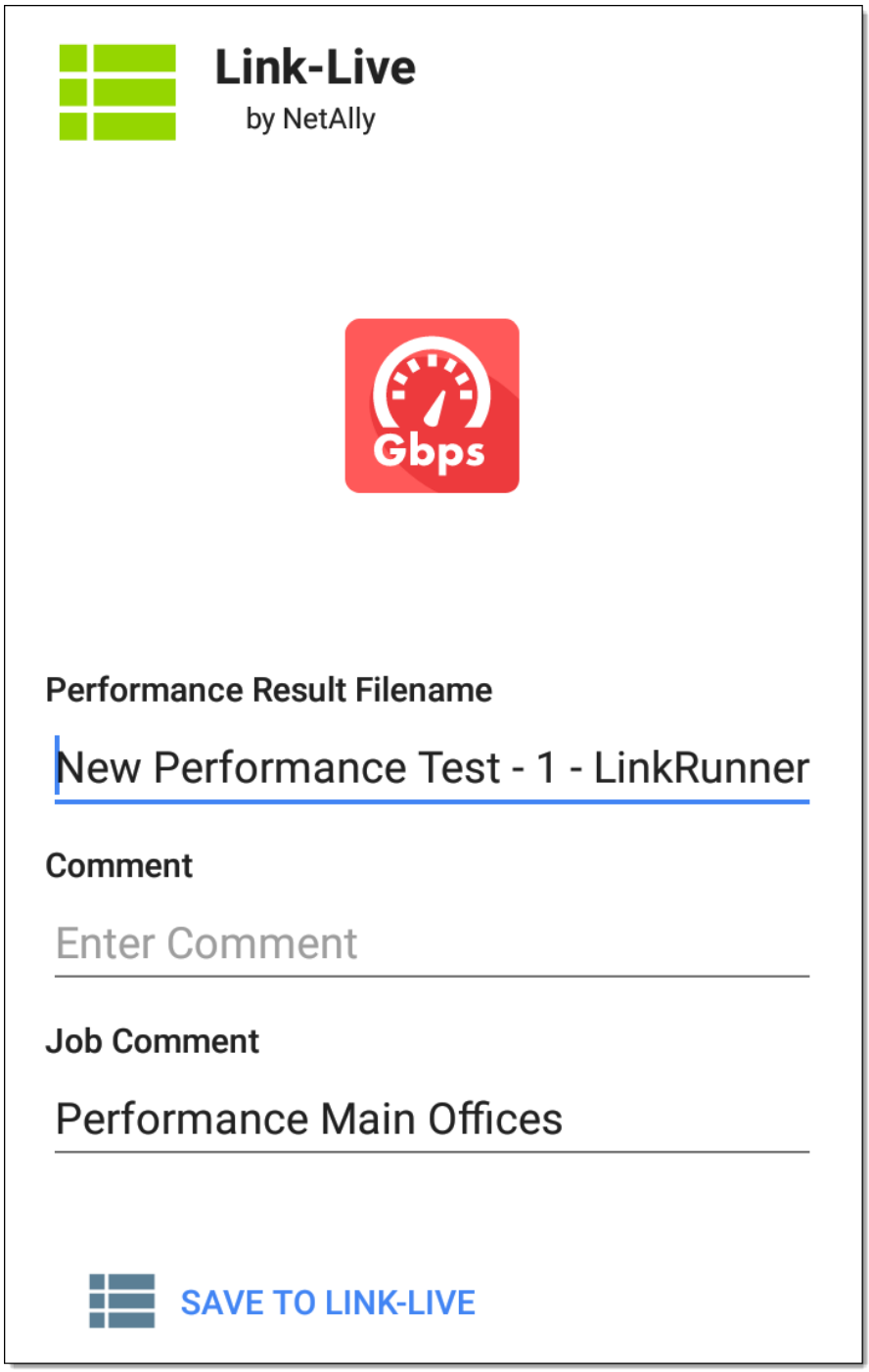
Uploading Results to Link-Live

Tap the action overflow icon ⋮ at the top right of the main Performance test screen, and select **Upload to Link-Live** to send the current latest

results to the Results page on Link-Live.com.



An image file of a complete Service results screen, including all the graphs, can also be uploaded to Link-Live and attached to the main test results. From the main Performance test screen, tap a Service card to view the Service detailed results, then tap the action overflow icon  at the top right of the screen, and select **Upload graphs to Link-Live**.



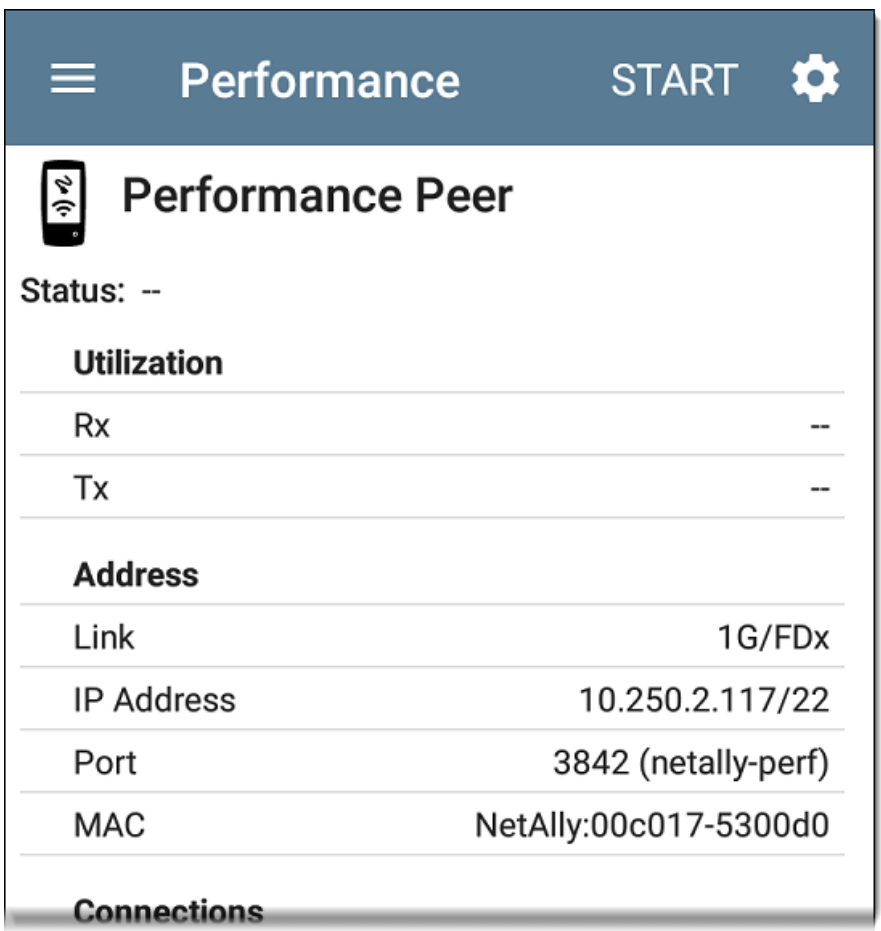
See the Link-Live chapter for more information.

Back to Title and Contents

Running EtherScope nXG as a Performance Peer

In addition to running a Performance Test as the controlling source device, EtherScope nXG can also act as a Peer for another EtherScope nXG or a OneTouch AT 10G acting as the source and controller.

To access the EtherScope Performance Peer, tap the menu button in the Performance app and select **Performance Peer**.



The Wired Test Port must be linked (by running an AutoTest Wired Profile) for the Performance Peer function to run. If the port is not linked, a Status message displays, "The wired test port is not linked."

Performance Peer Setting

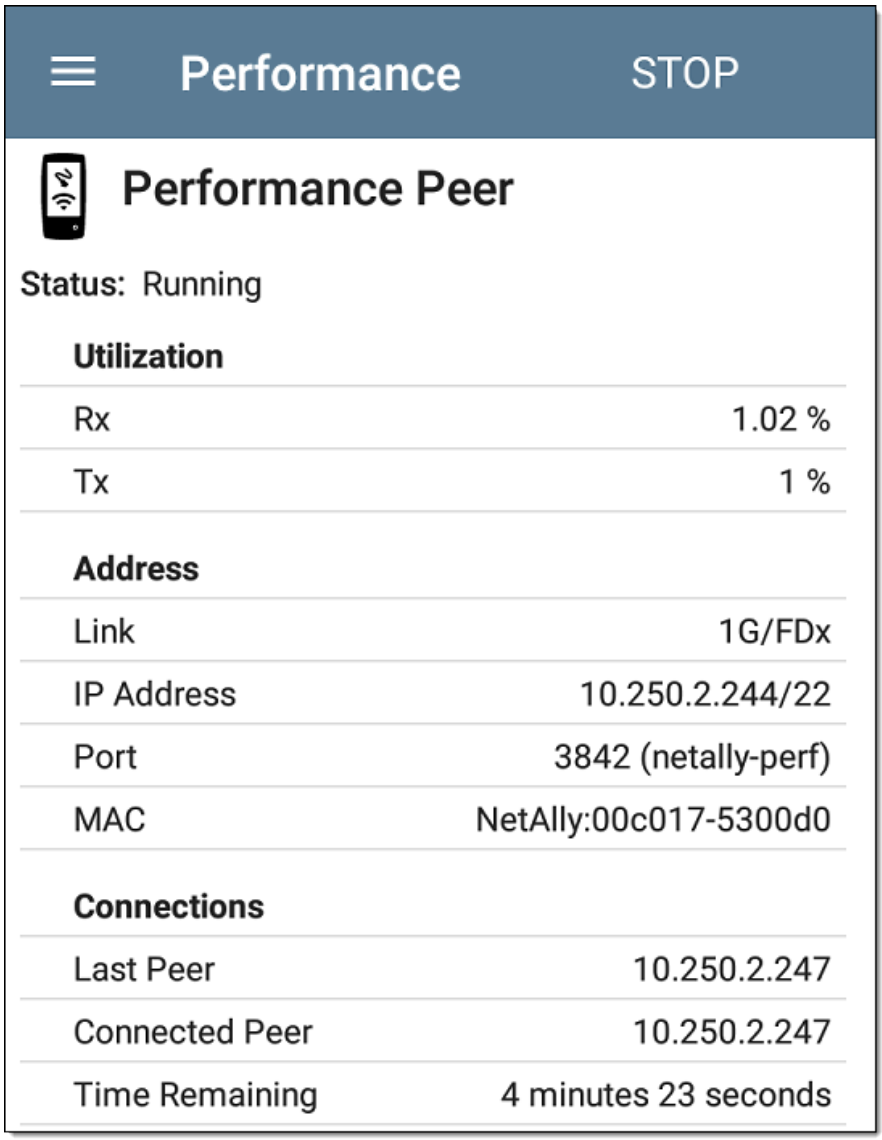
The only setting for the Performance Peer function is the **Communication UDP Port**.

Tap the settings button on the Performance Peer screen to change the port number. The default NetAlly performance test port is 3842.

> NOTE: The UDP port number entered here must match the port number used by your source device.

Running the Peer

Tap **START** on the Performance Peer screen to start the Peer.



The screen displays real-time status, utilization, and rates for as long as the test is running.

Status: The current status of the peer

Utilization

Rx: Receive percentage of the link speed

Tx: Transmit percentage of the link speed

Address

Link: Link speed and duplex of the established Wired Test Port connection

IP Address: Address of the EtherScope to be entered into the controlling source device

Port: UDP Communication port in use by the peer

MAC: The EtherScope's MAC address

Connections

Last Peer: Address of the previous peer that was connected to the EtherScope

Connected Peer: Address of the peer that is currently connected to the EtherScope

Time Remaining: Amount of time left for the current test

Back to Title and Contents

iPerf Test App

iPerf is a standardized network performance tool used to measure UDP or TCP throughput and loss.

The iPerf app runs an iPerf3 performance test to a NetAlly Test Accessory or an iPerf server endpoint.

The NetAlly Test Accessory runs network connection tests, uploads results to Link-Live Cloud Service, and acts as an iPerf server endpoint for iPerf tests run by other NetAlly handheld testers.

Learn more about the Test Accessory from **NetAlly.com/products/TestAccessory**.

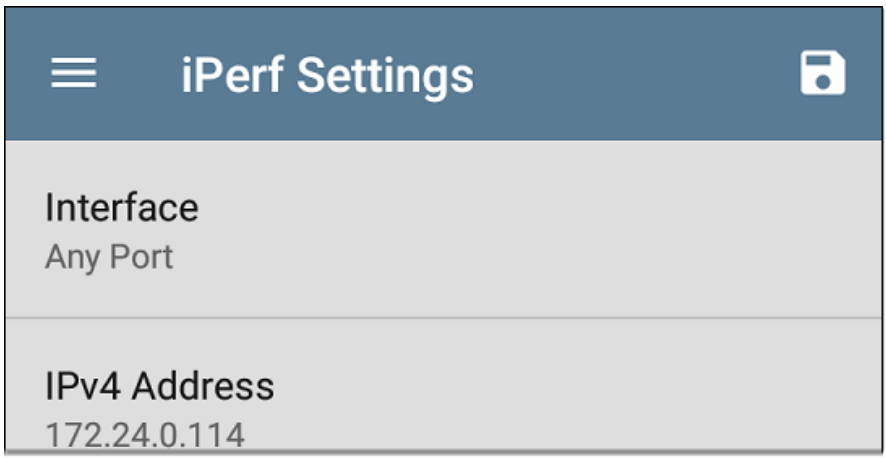
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the EtherScope iPerf test. You can download iPerf server software from **https://iperf.fr**.

iPerf Settings

To run an iPerf test, you must configure your EtherScope unit to communicate with your iPerf endpoint. You can manually enter an iPerf server address, or select a NetAlly Test Accessory's address in the iPerf settings.

Saving Custom iPerf Settings

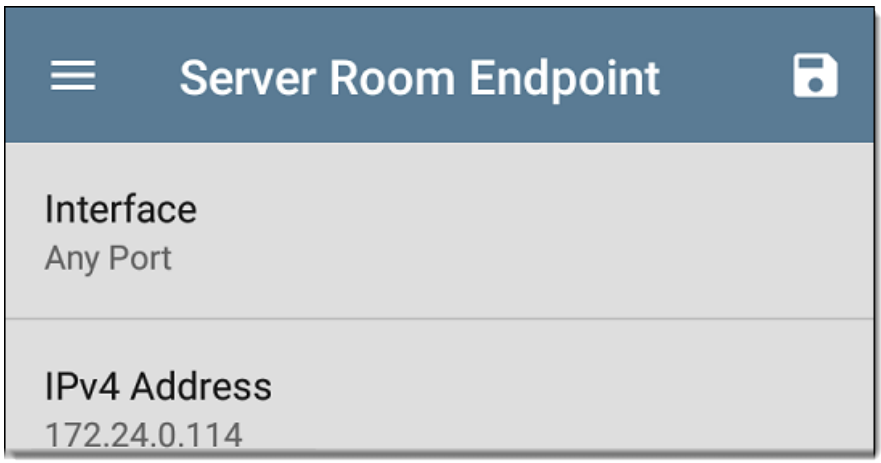
The iPerf app allows you to save a configuration of settings for running an iPerf test to the same endpoint later.

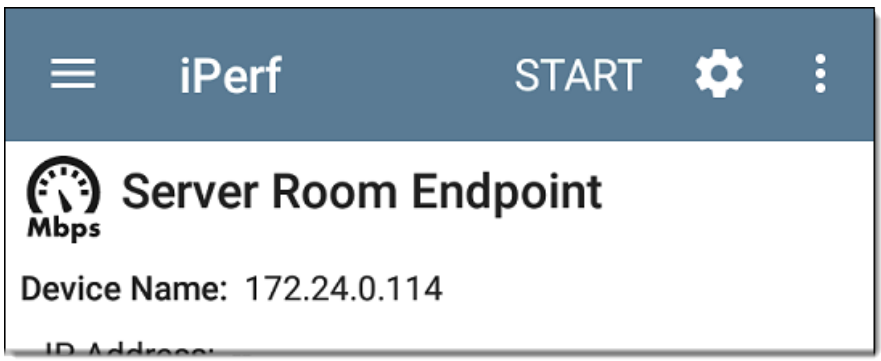


Tap the save icon to load, save, import, and export configured settings. See Saving App Settings Configurations for more instructions.

Once you save a settings configuration, the custom name you entered appears at the top of

the iPerf settings and results screens. In the example images here, the user has saved a custom iPerf configuration called "Server Room Endpoint."



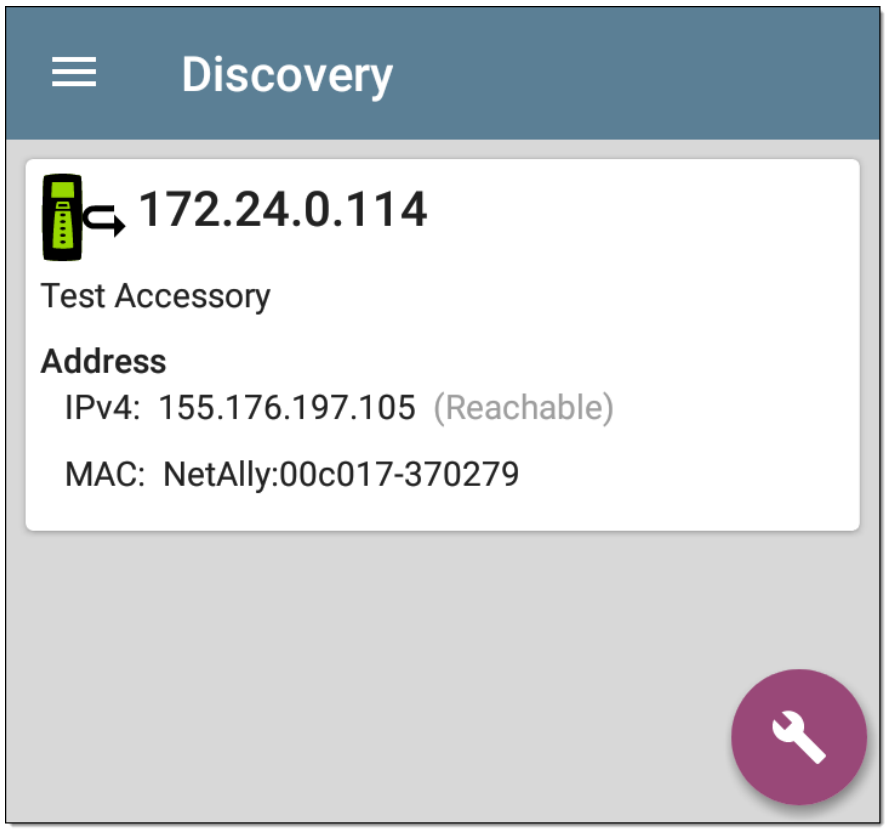


Test Accessories in Discovery

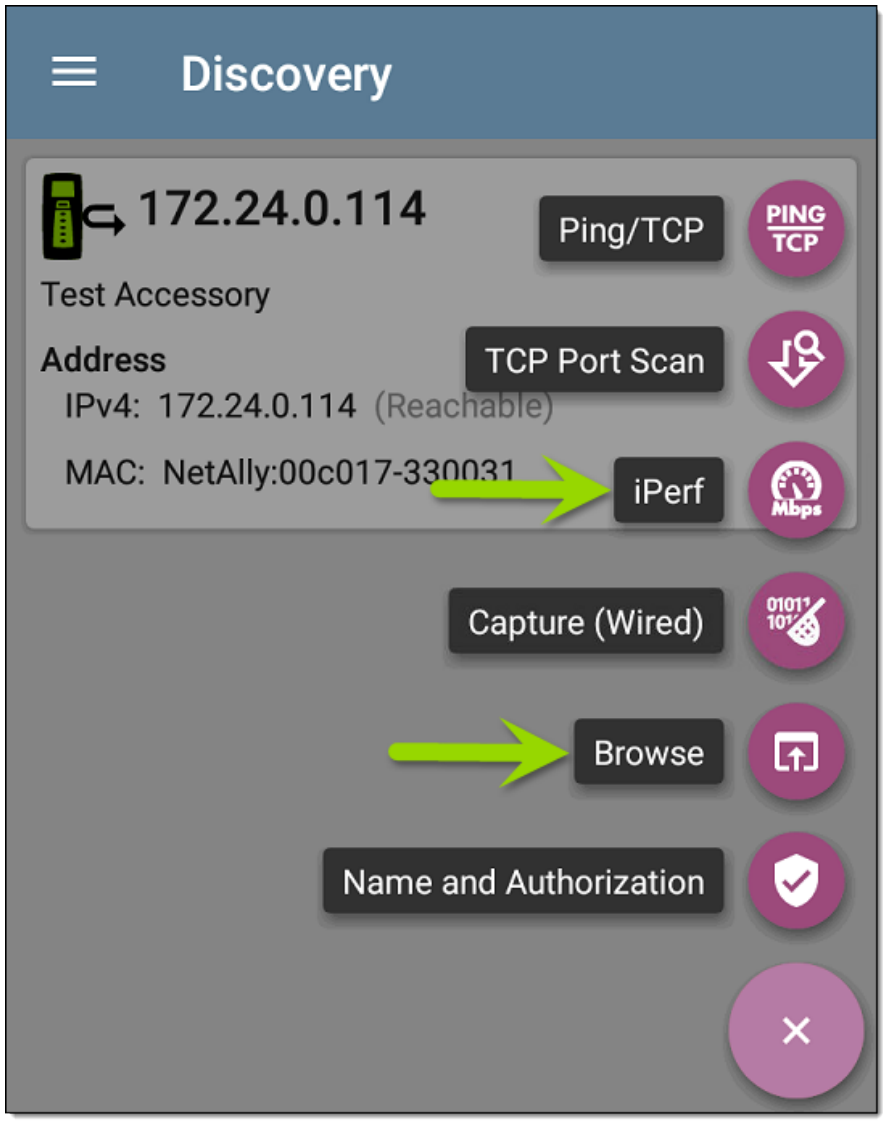
You can start an iPerf test from the Details screen for a Test Accessory in the Discovery app using the floating action button.

1. Open the Discovery app, and select an active **Test Accessory** from the main

Discovery list to open its Details screen.



2. Tap the floating action button (FAB) to open the action menu.

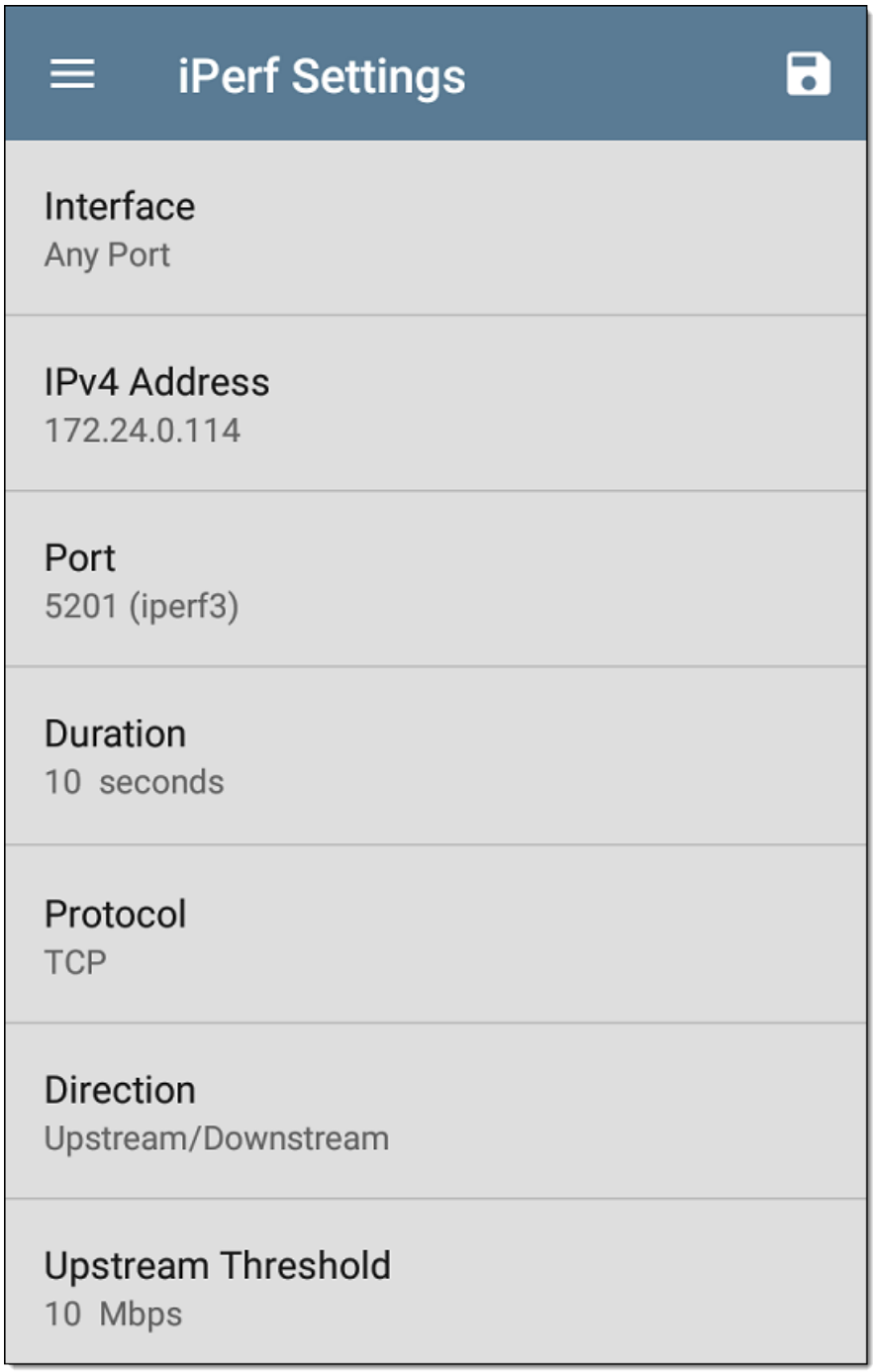


3. Select the **iPerf** app button to open the iPerf app with the IP address populated from the Test Accessory in Discovery.

   NOTE: You can also select **Browse** in the FAB menu to open the Test Accessory's Web Interface, where you can view its status and configure its settings.

Configuring iPerf Settings

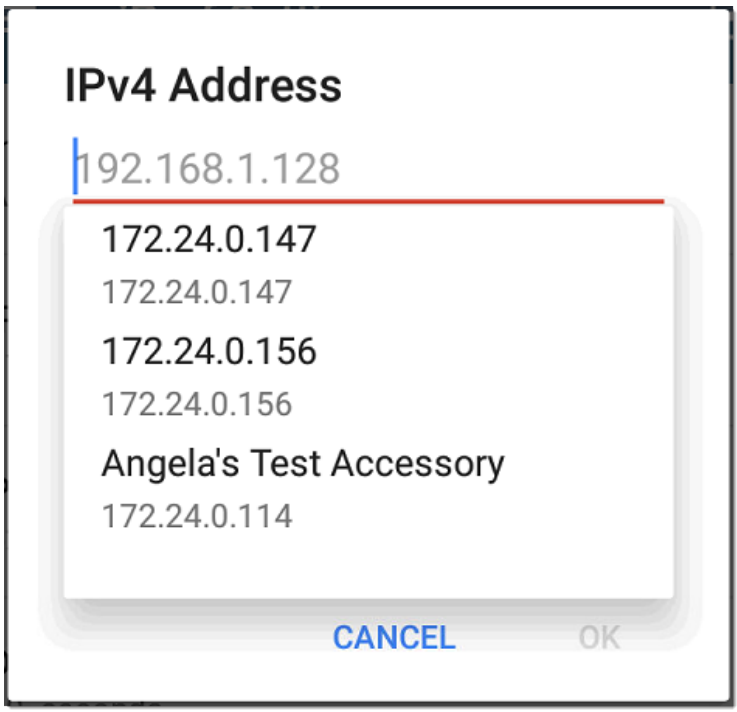
To configure the iPerf test settings manually, open the settings on the iPerf screen.



Tap each field to enter or revise selections as needed. Changed settings are automatically applied. When you finish configuring, tap the back button to return to the iPerf test screen.

Interface: This setting specifies which EtherScope port runs the scan. (See Selecting Ports for explanations of the different ports.)

IPv4 Address: Tap the field to enter or select the IPv4 address of the target iPerf server. Only IPv4 addresses are allowed for iPerf testing.



A drop-down list in the IPv4 Address dialog shows all the Test Accessories the EtherScope has discovered through the discovery process, as

well as any Test Accessories that are claimed to the same Link-Live organization as your EtherScope.

> NOTE: Clear the address field in the dialog to see the full list of discovered Test Accessory addresses.

Port: The default iPerf3 port number is 5201. Tap the field to enter a different port number.

> NOTE: The iPerf port number entered here must match the port number used by your iPerf server. If needed, consult the Test Accessory User Guide (NetAlly.com/products/TestAccessory).

Duration: This setting is the length of time for one direction, Upstream or Downstream, of the iPerf test. If the Direction setting below is set to both Upstream/Downstream, the total test time is twice the value set here. Tap the field to select a new duration or enter a custom value. The default is 10 seconds.

Protocol: TCP is the default protocol. Tap the UDP selector to switch to UDP.

NOTE: iPerf tests running the TCP protocol automatically run at the fastest rate possible. When running a UDP protocol test, the iPerf app attempts to run at the selected Bandwidth.

Direction: You can run an iPerf test Upstream, Downstream, or both. The default is Upstream and Downstream. Tap this field to set the test for only one direction.

Upstream and Downstream Bandwidth: These fields only appear if the **UDP Protocol** is selected. They specify the desired target bandwidth for the iPerf Test using the UDP protocol.

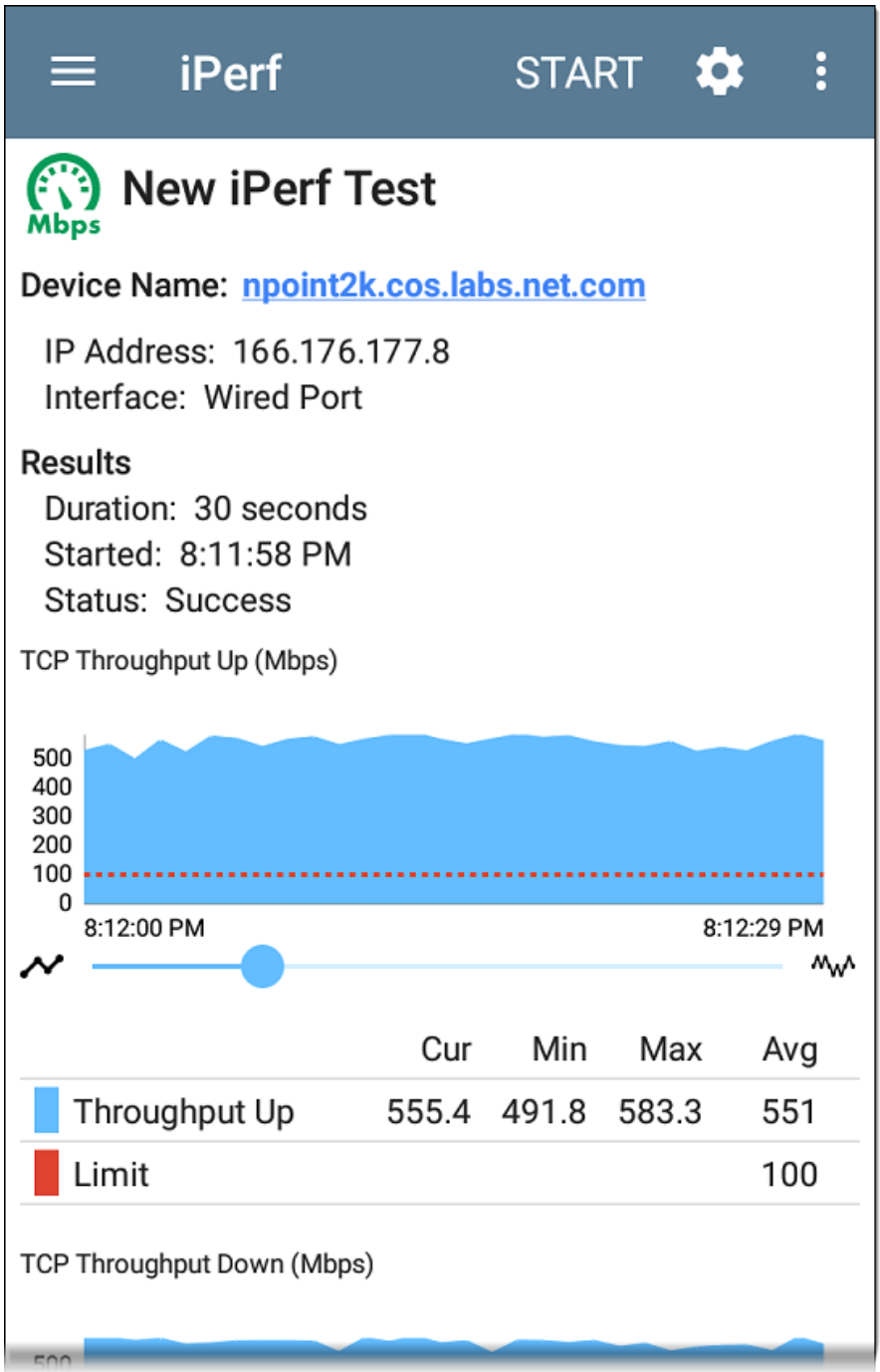
Upstream and Downstream Thresholds: Thresholds are the values the EtherScope uses to grade the test as **Pass** or **Fail**. iPerf thresholds are throughput rates. The default is 10 Mbps. Tap the threshold fields to select a different value or enter a custom one.

Back to Title and Contents

Running an iPerf Test

Ensure that you have an active link on the Interface (Test Port) from which you are running the iPerf test. Wired and Wi-Fi test ports require that an AutoTest Wired or Wi-Fi Profile has run to establish a link. The AutoTest Wired Profile runs automatically, but you must open the AutoTest app to run a Wi-Fi Profile and link on the Wi-Fi test port. Management ports link automatically if a connection is available.

Tap the **START** button on the main iPerf screen to begin testing.



Test characteristics and status are displayed at the top of the iPerf results screen while the lower part of the screen displays a real-time graph of the TCP or UDP Upload and/or Download speeds.

To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

Device Name: Hostname or address of the iPerf server or Test Accessory.

IP Address: IPv4 address of the iPerf server.

Interface: The EtherScope Test Port from which the test is running.

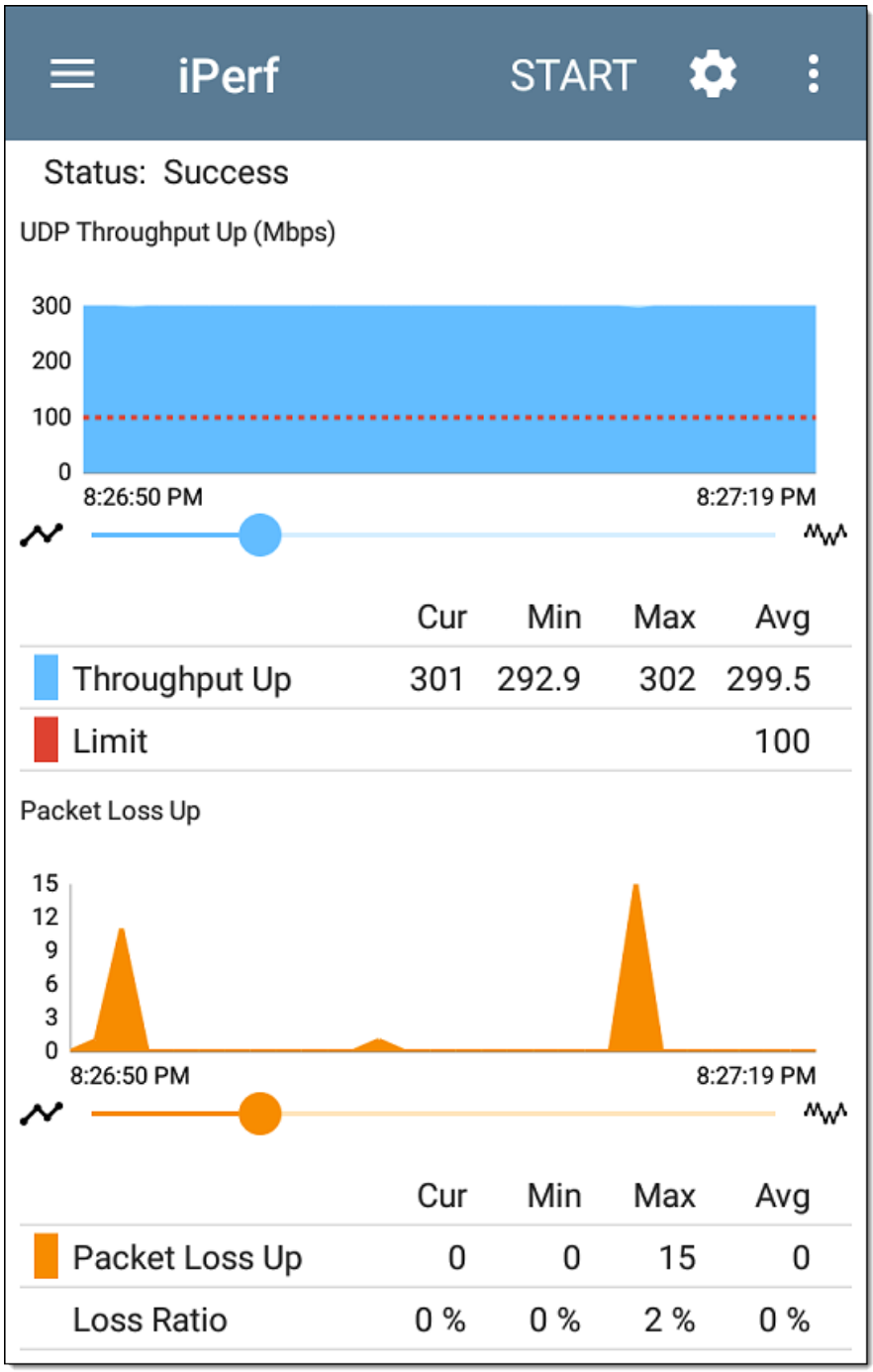
Results

- **Duration**: Configured Duration from the iPerf settings
- **Started**: Time the test started
- **Status**: Success or failure status of the test.

TCP/UDP Throughput Up and Down graphs: The iPerf graphs plot the throughput rate to (Up) or from (Down) the iPerf server in Mbps.

The table below each graph displays the Current, Minimum, Maximum, and Average rates.

Limit: This is the **Threshold** from the iPerf app's settings. The threshold value is also displayed on the graph as a red dotted line.



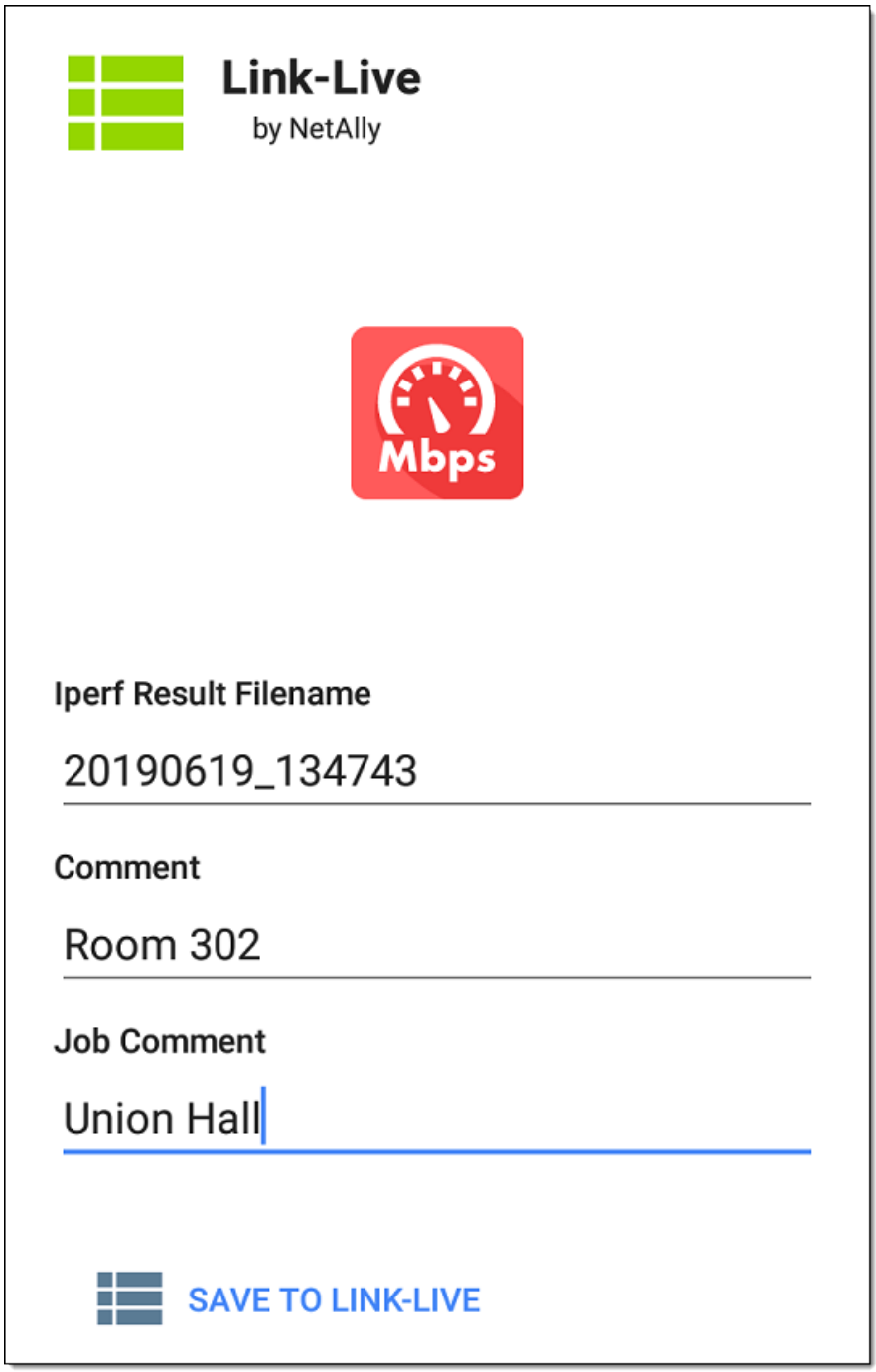
UDP Packet Loss Up and Down graphs: When running a UDP protocol test, the iPerf results also display graphs and tables of Packet Loss. Values for the number and percentage of packets lost are displayed in the table below the

graph. The Packet Loss Up graph and table do not display measurements until results are received from the iPerf server at the end of the upstream test.

Note that the Packet Loss Up number could be much less than the Packet Loss Down number.

Uploading Results to Link-Live

To send your iPerf results to the Link-Live website, tap the action overflow button  at the top right of the iPerf screen, and then tap **Upload to Link-Live**.



The Link-Live sharing screen opens and allows you to revise the auto-generated file name and attach comments to the iPerf result, which is displayed on the Results page on Link-Live.com.

Back to Title and Contents

LANBERT™ Test App

LANBERT is a Bit Error Rate Testing application that transmits IEEE 802.3 data frames over LAN media and measures the number of frames sent, lost, and errored.

The LANBERT app runs a loopback test on fiber or copper media using:

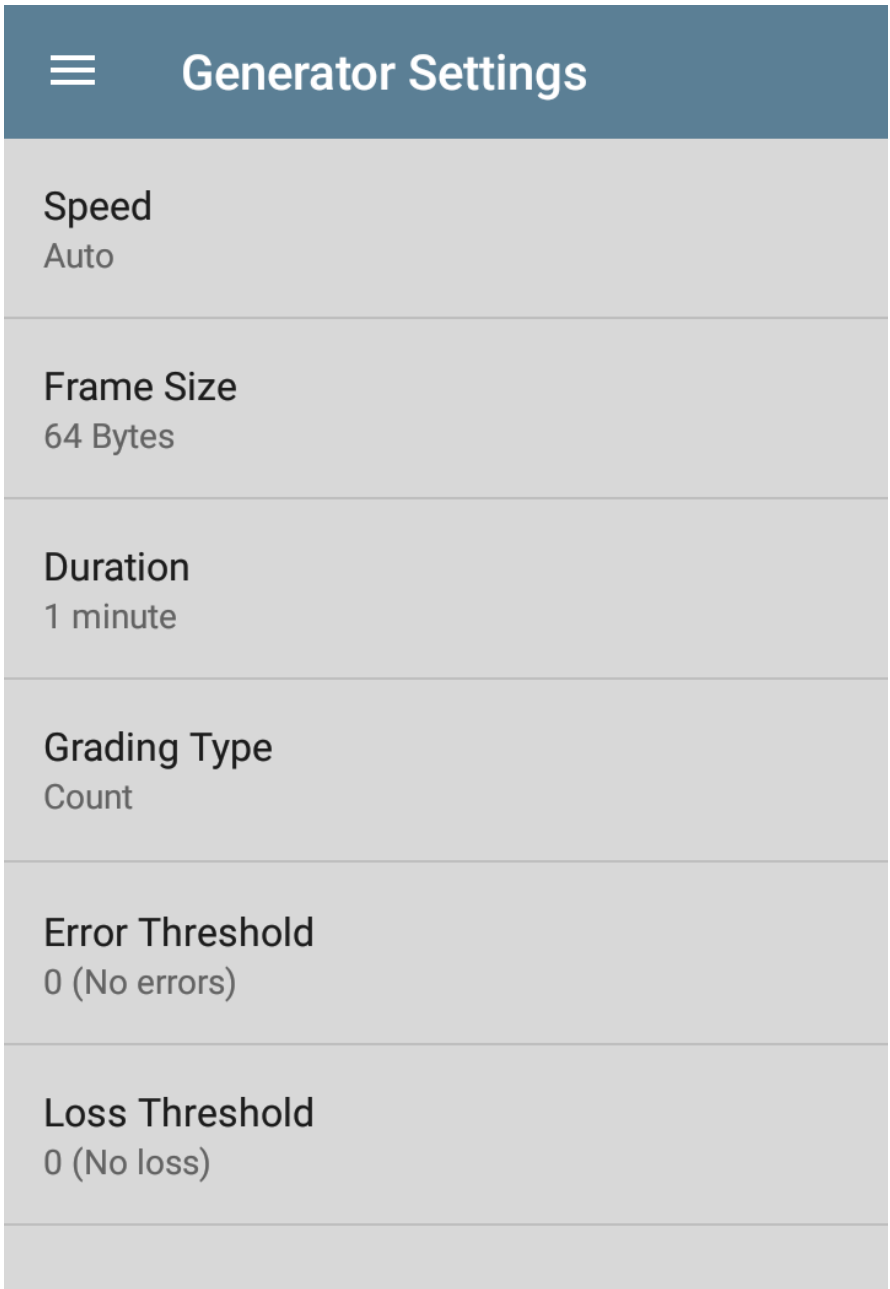
- A second testing device to act as the loopback endpoint. This device can be an EtherScope nXG or a LinkRunner 10G.
- A switched port available with some Ethernet switches.
- A physical loopback device.

LANBERT Settings

To run a test with LANBERT, you must configure the generator settings. If you are using this unit as an active loopback device, see Configuring LANBERT Loopback Settings.

Configuring LANBERT Generator Settings

To configure the LANBERT settings, open the settings  icon on the LANBERT screen or tap the Menu icon  and select **Generator Settings**.



Tap each field to enter or revise selections as needed. Changed settings are automatically applied. When you finish configuring, tap **OK** or **Cancel** to return to the settings screen. When you finish configuring, tap the back button to return to the LANBERT test screen.

Speed: This setting sets the link speed at which the Ethernet frames are sent to and received from the loopback destination.

- You can choose 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, 10 Gbps to match the capacity of the media you want to test. (All settings are full duplex.)
- **Auto** lets the generator and loopback devices auto-negotiate the speed. (The speed may vary if there are errors or impairments.)

Frame Size: Sets the size of the Ethernet frames to be sent during the test.

- You can choose presets of 64, 128, 256, 512, 1024, 1518 bytes.

  NOTE: Because the object of your bit error rate test is often to "stress" the media path with large amounts of data, choosing the minimum frame size of 64 bytes allows the maximum number of frames to be sent in the duration of the test.

- **Random** varies the frame size at random to simulate variations in real data.
- Tap the pencil icon to open an editing screen to enter a **Custom Value** for the frame size.

Duration: Sets the time for the test. Presets range from 10 seconds up to 24 hours.

Grading Type: Sets counts or percentages to grade error or loss thresholds. Both counts and percentages are always shown on the screen.

- **Count**: counts the total number of frames encountering errors or loss of frame and sets the Error Threshold and Loss Threshold presets to numbers.
- **Percent**: calculates the percentage of frames encountering errors or loss of frame and sets the Error Threshold and Loss Threshold presets to percentages.

Error Threshold: Defines what constitutes a failed test in terms of frames that were successfully sent and received but that encountered errors that changed the frame check sequences.

- Select a value from the presets:
  - For a Grading Type of Count: 0 (no errors), 1, 10, 100, or 1000.
  - For a Grading Type of Percent: 0.0% (no errors), 0.001%, 0.01%, 0.1%, or 1%.
- **Disabled** turns off grading of errors.
- Tap the pencil icon ✎ to open an editing screen to enter a **Custom Value** for the error threshold.

Loss Threshold: Defines what constitutes a failed test in terms of frames that were unsuccessfully sent and received.

- Select a value from the presets:
  - For a Grading Type of Count: 0 (no errors), 1, 10, 100, or 1000.
  - For a Grading Type of Percent: 0.0% (no errors), 0.001%, 0.01%, 0.1%, or 1%.
- **Disabled** turns off grading of losses.
- Tap the pencil icon ✎ to open an editing screen to enter a **Custom Value** for the loss threshold.

Configuring LANBERT Loopback Settings

To configure this EtherScope as an active loopback device, select the LANBERT icon  from the Home screen, then tap the Menu icon  and select **Loopback Settings**. When you finish configuring, tap the back button  to return to the LANBERT test screen.

The only available setting is **Speed**.

- Match the speed to the speed you selected for the transmitting test device. You can choose 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, or 10 Gbps. (All settings are full duplex.)
- **Auto** lets the EtherScope automatically negotiate the speed.

Back to Title and Contents

Running a LANBERT Test

Before You Begin

- Identify the cable or channel path that you want to test. (Note that LANBERT uses Ethernet frames to test LAN pathways, including copper or fiber cables. It cannot function on wide-area networks or devices that use IP addresses to route traffic.)
- Plug one end of the LAN cable into the EtherScope Wired Test Port.
- Set up a loopback device at the other end of the LAN pathway to relay the received Ethernet frames back to the LANBERT generator. This device can be:
  - A physical loopback device for either copper or fiber media.
  - An Ethernet switch with a loopback feature. (Consult the manufacturer's documentation for instructions on setting up the loop.)

- A NetAlly EtherScope nXG or LinkRunner 10G with the LANBERT application running as the LANBERT Loopback. (Either device can function as the loopback relay and can collect data at the endpoint of the test.) See "LANBERT Settings" on page 737 for instructions on setting up the loopback settings.

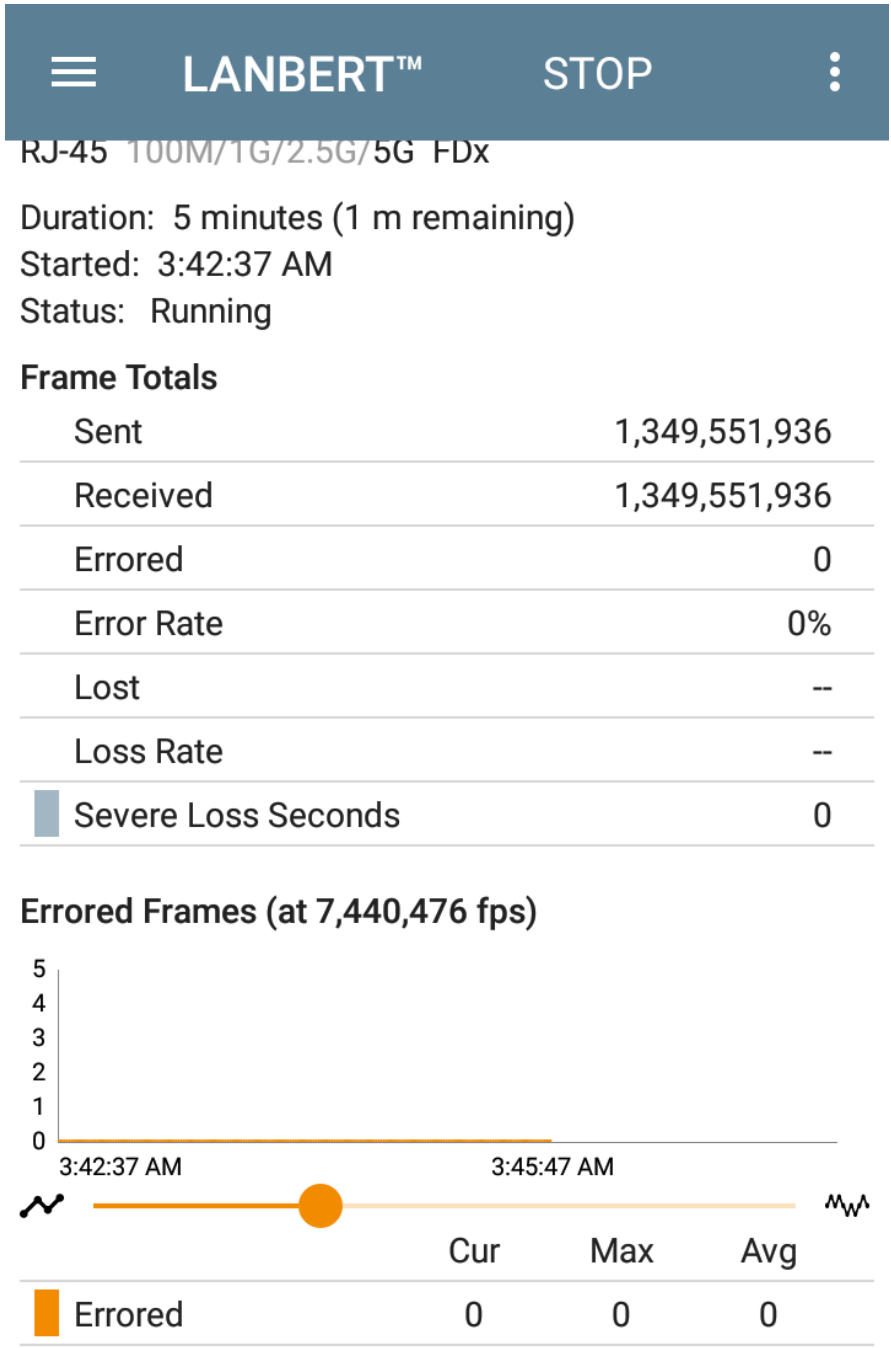
  NOTE: The Loopback mode is designed to stop whenever the LANBERT app is not displayed on the screen. If you plan to run a long test, make sure that the loopback unit is plugged into its AC power supply and that you have turned off the sleep function (go to system Settings, tap **Display > Sleep > Never**).

Run the Test

You can set up and start either the LANBERT generator or the LANBERT loopback unit first. This procedure starts with the generator.

1. On the Tester unit, open the LANBERT application.

2. Tap the **START** button.



The Status shows the current activity:

- Linking: the devices are setting up a connection.
- Waiting for loopback: the generator is waiting for a response from the loopback device.

3. On the loopback unit (if you are using an EtherScope nXG or LinkRunner 10G as the loopback device):
   a. Open the LANBERT application.
   b. Tap on the top left menu icon and tap on **LANBERT Loopback**.
   c. Tap the **START** button.
   d. The Status changes to Linking as the connection is set up with the LANBERT generator.
4. Verify that the Status changes to Running.
   - Test status, frame information, a graph of errored frames are displayed. Multi-gigabit details are also displayed when an RJ-45 line is connected to the Wired Test Port and the link speed is 2.5G, 5G,

or 10G.

- To pan and zoom on the graphs, you can swipe, double tap, and move the slider. See the Trending Graphs topic for an overview of the graph controls.

5. Let the test run to completion. The Status shows the test result (Success or Failure) and may display additional information, such as not connecting at the fastest advertised speed.

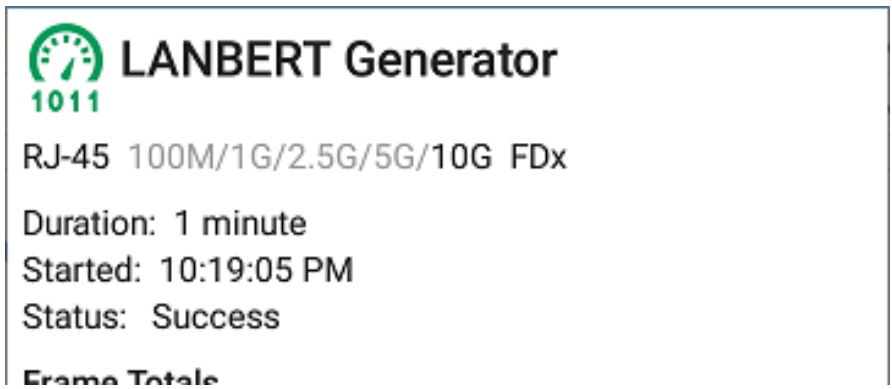
About LANBERT Results

- The color of the LANBERT icon indicates success or failure (green for success, red for failure).
- The first line below the icon displays information about the connection including:
  - Connector type
  - Speed (in bold). Other speeds shown as grayed out values are the ones that were advertised by the link partner but not selected. See the Wired Link Test Results

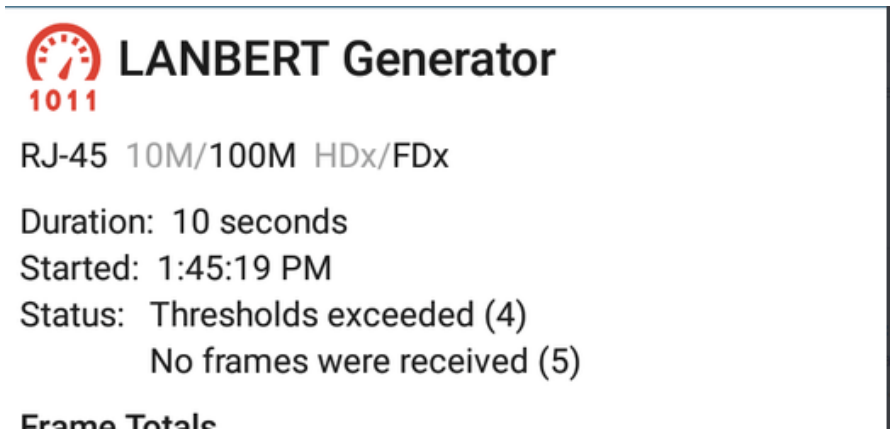
for more info about advertised speeds.

- Half versus full duplex ability.

The following example below shows a successful test for an RJ-45 connector that transmitted frames at 10 Gbps at full duplex.



The following example shows an unsuccessful test for an RJ-45 connector that transmitted frames at 100 Mbps at full duplex.



- SFP details are shown when using a fiber connection. These include:
  - Wavelength
  - Temperature
  - Voltage
  - Tx Bias Current
  - Tx Power
  - Rx Power
  - Rx Reference Power
  - Rx Power Difference
  - **SET REFERENCE** button (displayed only while test is running): Latches the Rx Reference Power value to the current Rx Power value.
  - **CLEAR REFERENCE** button (displayed only while test is running): Clears the Rx Reference Power value.

    NOTE: The LANBERT generator and LANBERT Loopback both use the same reference power value. This

reference power is reset or cleared on a power cycle.

- Loss figures are not displayed until the test ends.
- Severe Loss Seconds occur when the LANBERT generator detects ≥ 1% frame loss for one second.

Frame Totals	
Sent	128,020
Received	0
Errored	0
Error Rate	--
Lost	128,020
Loss Rate	100%
Severe Loss Seconds	10

Uploading Results to Link-Live

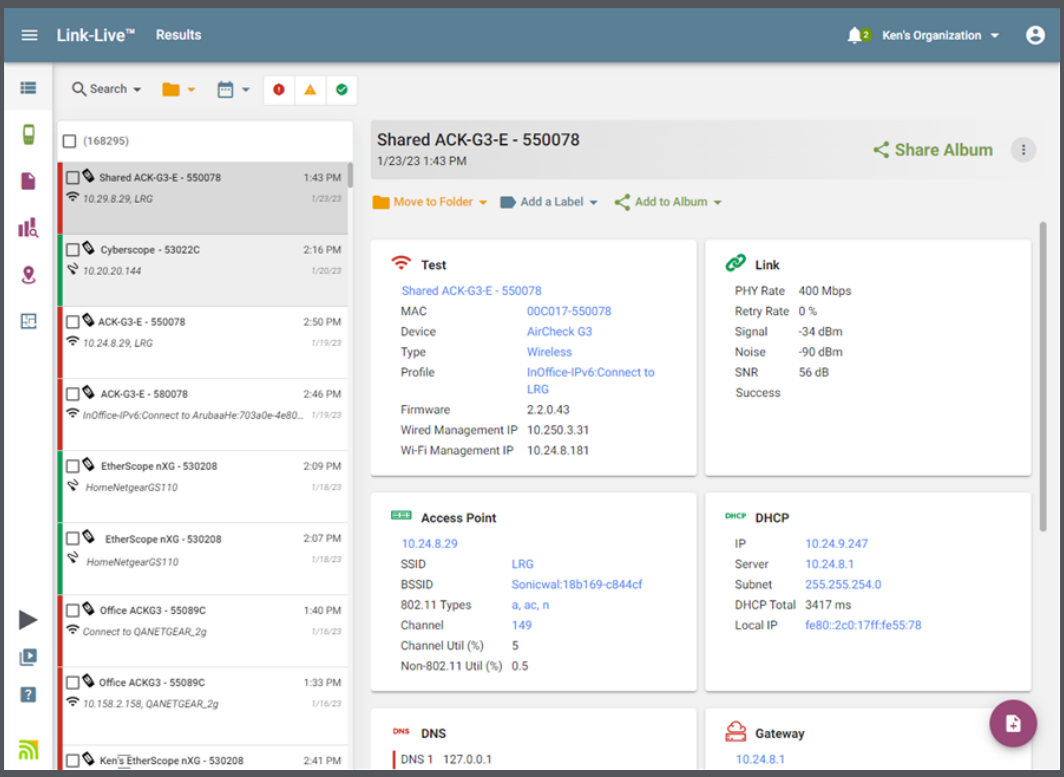
To send your LANBERT results to the Link-Live website, tap the action overflow button  at the top right of the LANBERT screen, and then tap **Upload to Link-Live** or **Upload graphs to Link-Live** (which includes the data graphs with the upload).

The Link-Live sharing screen opens. You can enter a file name (for active surveys only) and attach comments to the LANBERT results. The

results are displayed on the Results  page on Link-Live.com.

Back to Title and Contents

Link-Live Cloud Service



Link-Live Cloud Service is a free, online system for collecting, tracking, organizing, analyzing, and reporting your test results. AutoTest results are automatically uploaded once your EtherScope nXG is claimed.

The comprehensive EtherScope nXG offers more features for analyzing your network in Link-Live than previous testers. Claim your EtherScope to Link-Live.com to access these functions:

- Check for software updates and update your EtherScope nXG software.
- Download third-party applications from the NetAlly App Store to use on your EtherScope.
- Automatically upload AutoTest results each time you run AutoTest.
- Attach test and Job comments to Link-Live uploads, and automatically sort your results and files into folders in Link-Live.
- Upload test, discovery, and analysis results from the NetAlly apps, including Discovery, Wi-Fi, Path Analysis, AirMapper, Performance, and iPerf. See Link-Live and Testing Apps for more about uploading.

Getting Started in Link-Live Cloud Service

To start, create a user account at Link-Live.com, and sign in. You can open the Link-Live website in the EtherScope's web browser to create and manage your account.

Claiming the Unit

On Link-Live.com

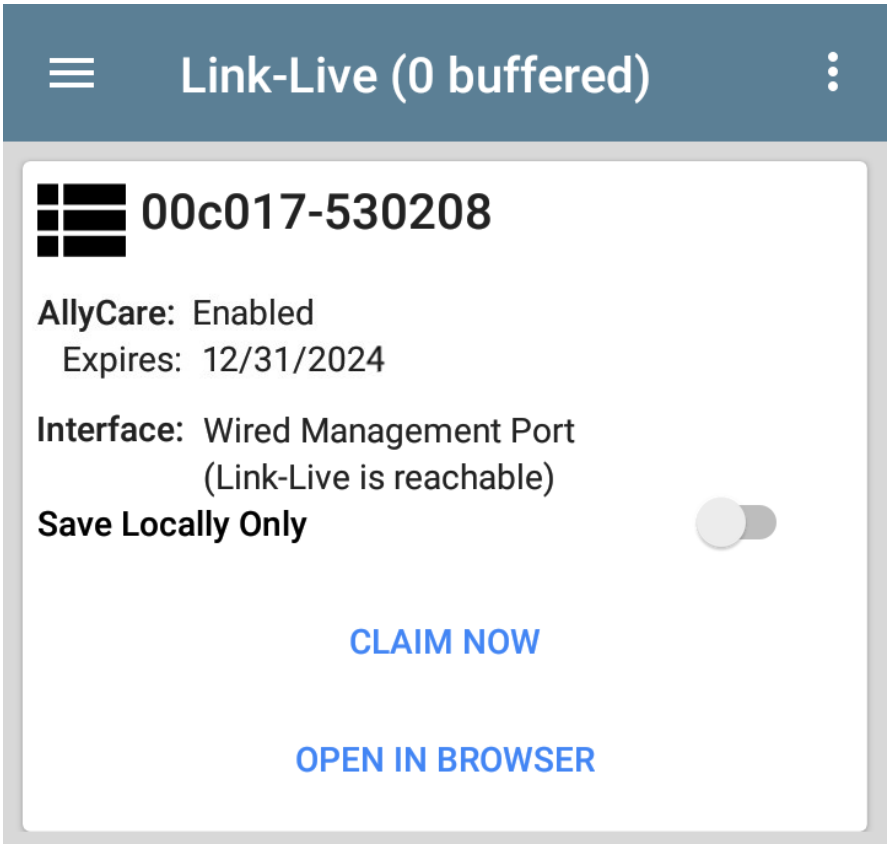
1. The first time you sign in to Link-Live.com, a pop-up window appears, prompting you to claim a device.

   If you already have a user account and other devices claimed to Link-Live, navigate to the **Units** page from the left side navigation drawer, and then click the **Claim Unit** button  at the lower right corner of the screen .

2. Then, select the EtherScope nXG image, and follow the claiming instructions on the Link-Live website.

On the EtherScope nXG Unit

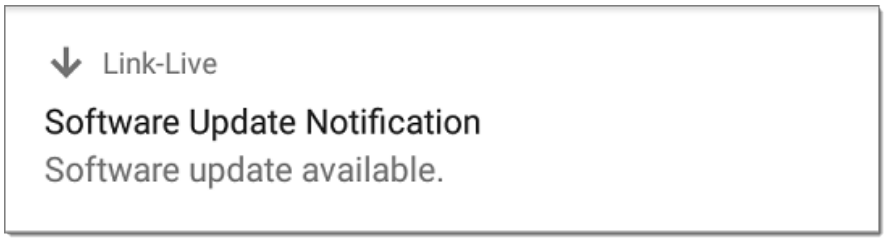
1. Open the Link-Live app. Your unit's MAC address is displayed.



2. Tap **CLAIM NOW** on the Link-Live app screen.
3. When prompted by the instructions on the Link-Live website, enter the MAC address.

After you claim your EtherScope nXG to Link-Live, a software update may be available. If so, a notification appears in the Status Bar . Open

the Top Notification Panel, and select the notification to update your unit.



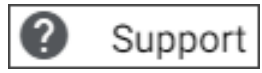
See Updating Software for more information.

After Claiming

Once your EtherScope is claimed to the Link-Live Cloud Service, it automatically uploads your AutoTest results each time you run AutoTest. You can also upload a test comment and a picture with your test results using the floating action buttons (FABs) for the Wired Test Results or Wi-Fi Test Results. You can automatically sort your results into folders in Link-Live using test and Job comments.

If your EtherScope is not connected to an active network, any test results, comments, or images are stored in memory (buffered) and uploaded once a connection is established.

For more information on how to the use the Link-Live.com website, click or tap the

navigation menu icon  at the top left of the Link-Live.com pages, and select 

.

Unclaiming

You may need to unclaim your unit from Link-Live to transfer it to another user or if you no longer want to send data to Link-Live.com.

To unclaim your EtherScope from Link-Live, tap the navigation drawer icon  in the Link-Live app, tap About, and then tap **UNCLAIM**.

AllyCare Code

The AllyCare Code button appears at the bottom of the About screen next to the Export Logs button if your unit is not claimed.

Tap **AllyCare Code** to open a dialog to enter an AllyCare Activation Code.

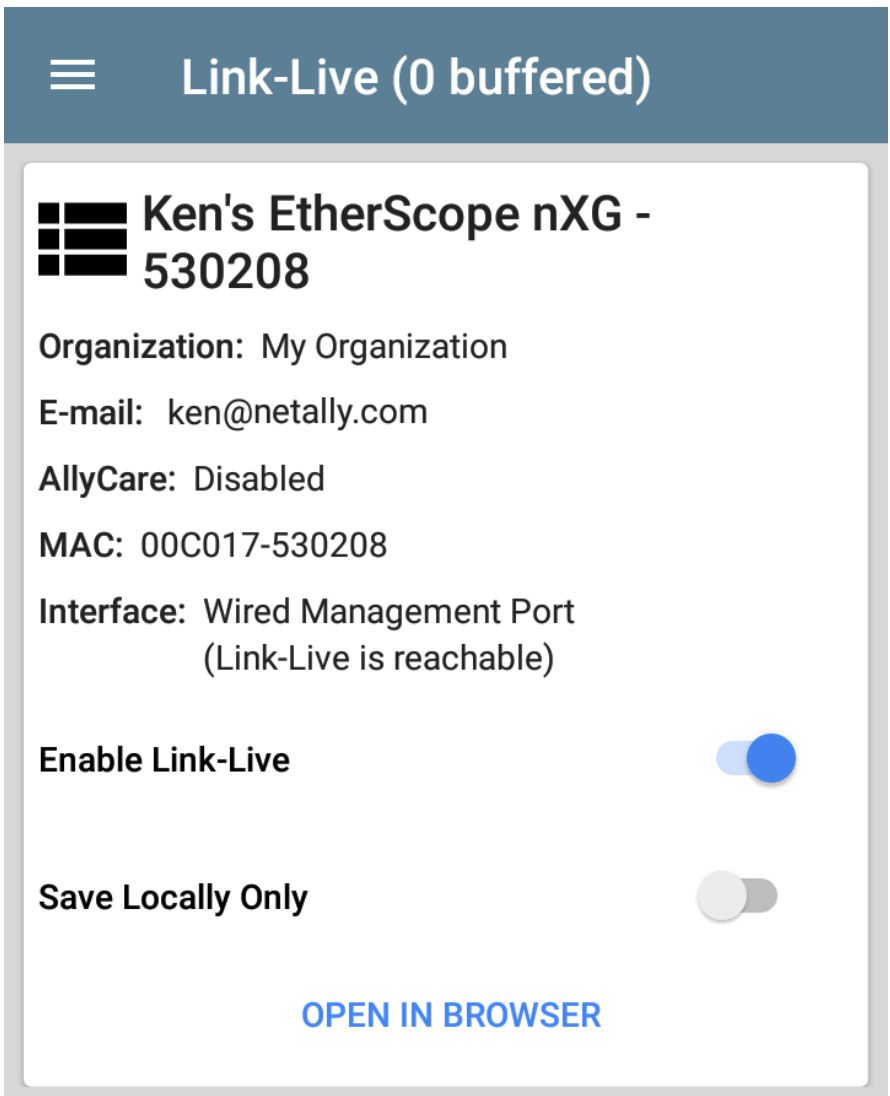
Private Link-Live Settings

Use these settings only when your organization has deployed a private instance of Link-Live. Consult your IT organization for setting details.

Link-Live App Features

The main Link-Live app screen on your EtherScope nXG facilitates the claiming process, displays Link-Live related information, and allows you to enable or disable Link-Live.com uploads as needed.

Link-Live App Screen



The EtherScope unit's name that displays on the Link-Live.com is shown to the right of the Link-Live icon  . You can change this name on the Link-Live.com **Units**  page.

Organization is the Link-Live organization where the unit is claimed.

E-mail is the first e-mail address assigned to the unit, which receives test result notification emails.

The Organization and Email address shown here are assigned on the Link-Live.com website. The fields displayed in EtherScope's Link-Live app are informational.

AllyCare indicates the status of NetAlly's optional AllyCare services. See NetAlly.-com/Support for more information.

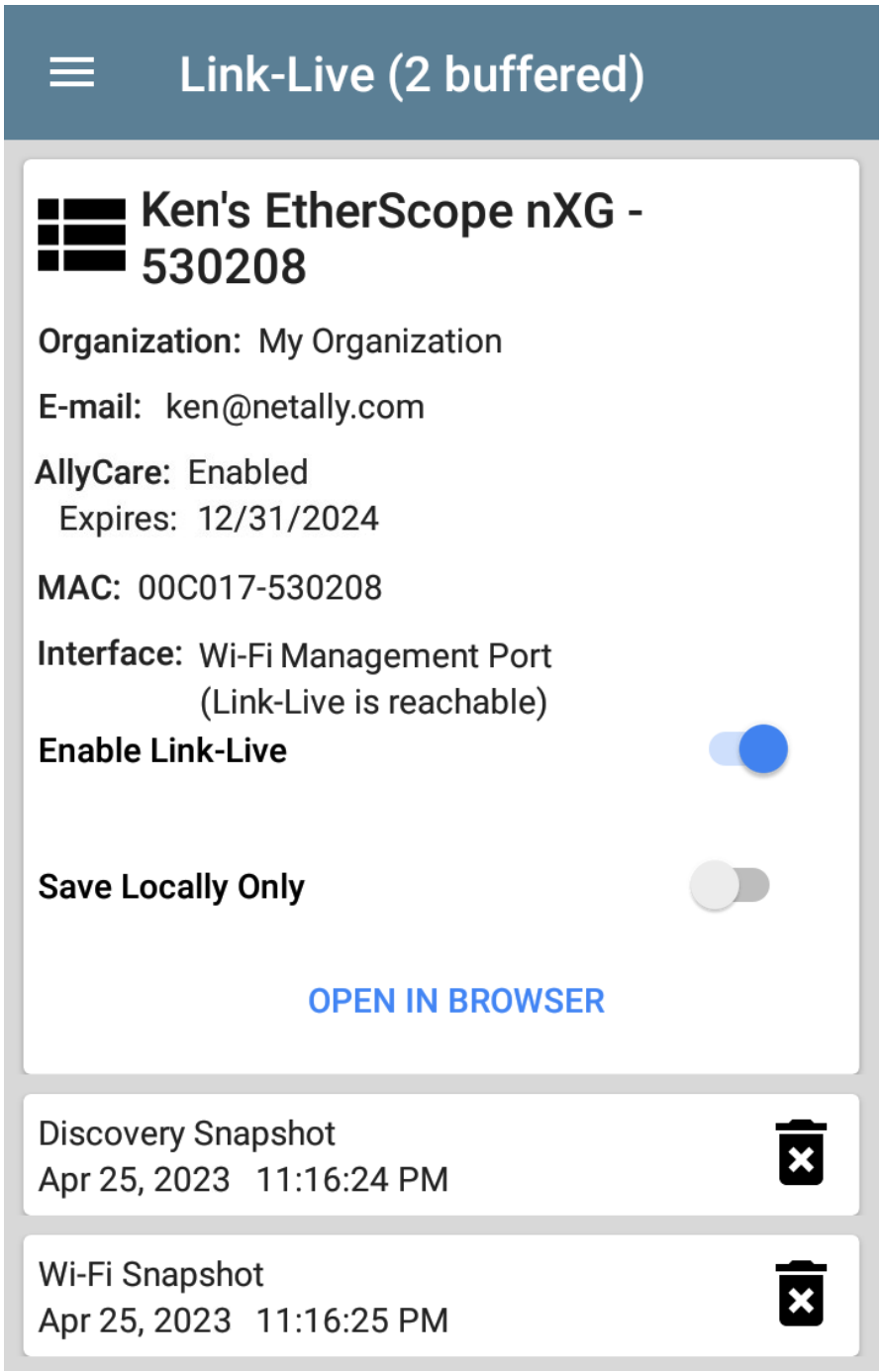
Interface shows which network interface is currently being used by Link-Live to post results and its status.

The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the EtherScope cannot upload test results or check for software updates. The

Upload to Link-Live options do not appear in the testing apps.

Tap the **OPEN IN BROWSER** link to open Link-Live.com on the EtherScope's web browser.

The "(# buffered)" in the Link-Live screen header indicates the number of files stored in the device memory when no active network connection is available. The buffered file types are listed below the main app card.

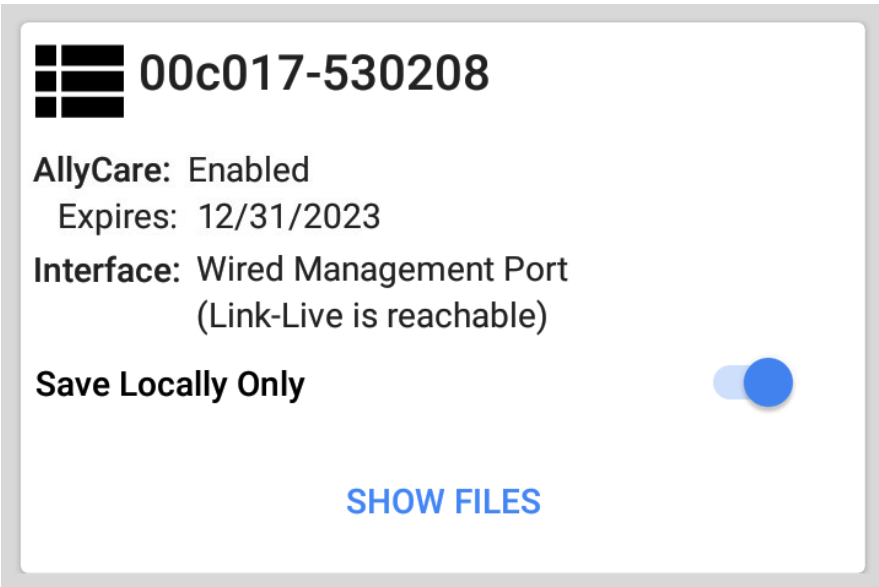


The buffered files displayed automatically upload to Link-Live.com once your EtherScope connects to an active network.

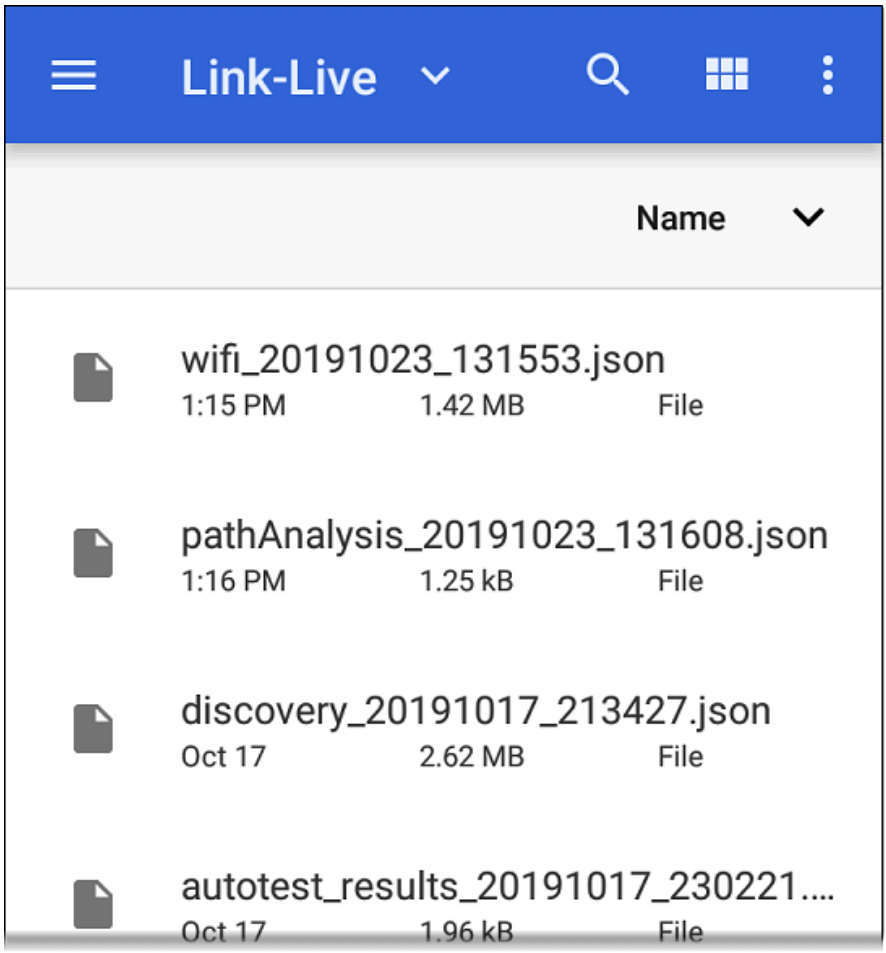
Saving Locally Only

If you do not want to send your results to the Link-Live website, you can still save results locally to your EtherScope as JSON files.

Tap the **Save Locally Only** toggle field in the Link-Live app to save the JSON files to your unit.



Select **SHOW FILES** to open the Files app. The .json files are saved in the **Downloads > TestResults** folder.



See the Managing Files topic for an overview of the Files app.

You can transfer the JSON files to a PC for analysis, or you can download a JSON viewer app from the App Store ▶ on your EtherScope.

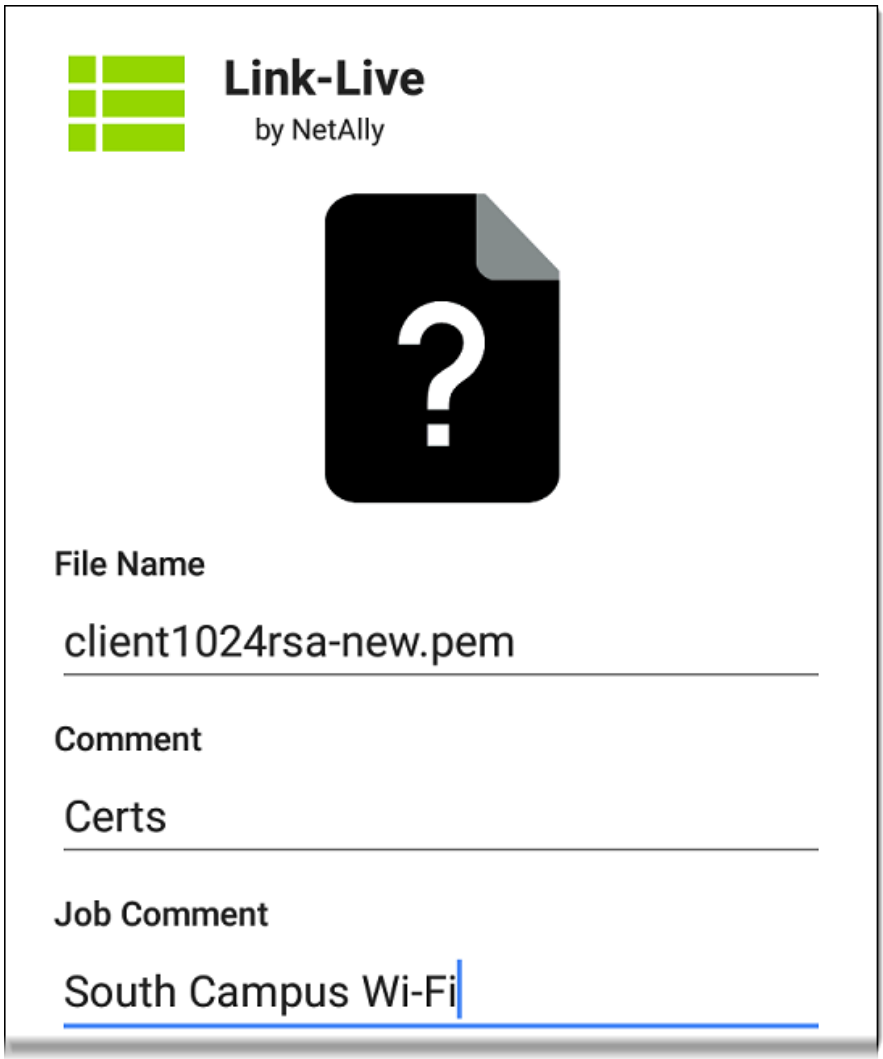
With **Save Locally Only** enabled, options for uploading or saving to Link-Live (described in the Link-Live and Testing Apps section below) still display in the NetAlly testing apps. However, the results are saved to the internal Link-Live

storage folder, and not uploaded to Link-Live.com.

Job Comment

The left-side navigation drawer for the Link-Live app lets you enter or change the Job Comment. The **Job Comment** attaches to all test results and files uploaded to Link-Live, until you change or delete it. In contrast, other **Comments**, like those attached to Wired or Wi-Fi AutoTest results or Discovery results, are only attached to one set of test results or uploaded file.

Both comment types appear on Link-Live sharing screens like the one below:



To enter or change the Job Comment in the Link-Live app:

1. With the Link-Live app open, tap the menu icon or swipe right from the left side of the screen.

2. Tap the **Job:** field.
3. Enter a comment in the dialog box.
4. Tap **SAVE**.

Note that the **Job Comment** field appears in other Link-Live sharing screens, allowing you to change it from multiple locations on the EtherScope. No matter where you change the Job Comment, it is updated everywhere on the unit.

Software Updates

The left-side navigation drawer for the Link-Live app also lets you check for and download any available software updates. See Updating Software in the Software Management chapter.

System Notifications

Link-Live can send messages to your test unit. They are displayed in the system Notification Panel.

Link-Live and Testing Apps

Once your unit is claimed, the Link-Live app works with several of the testing apps to upload test results, discovery and analysis data, comments, and images to the Link-Live website. Link-Live.com categorizes the uploads from different apps on corresponding webpages, as shown below:

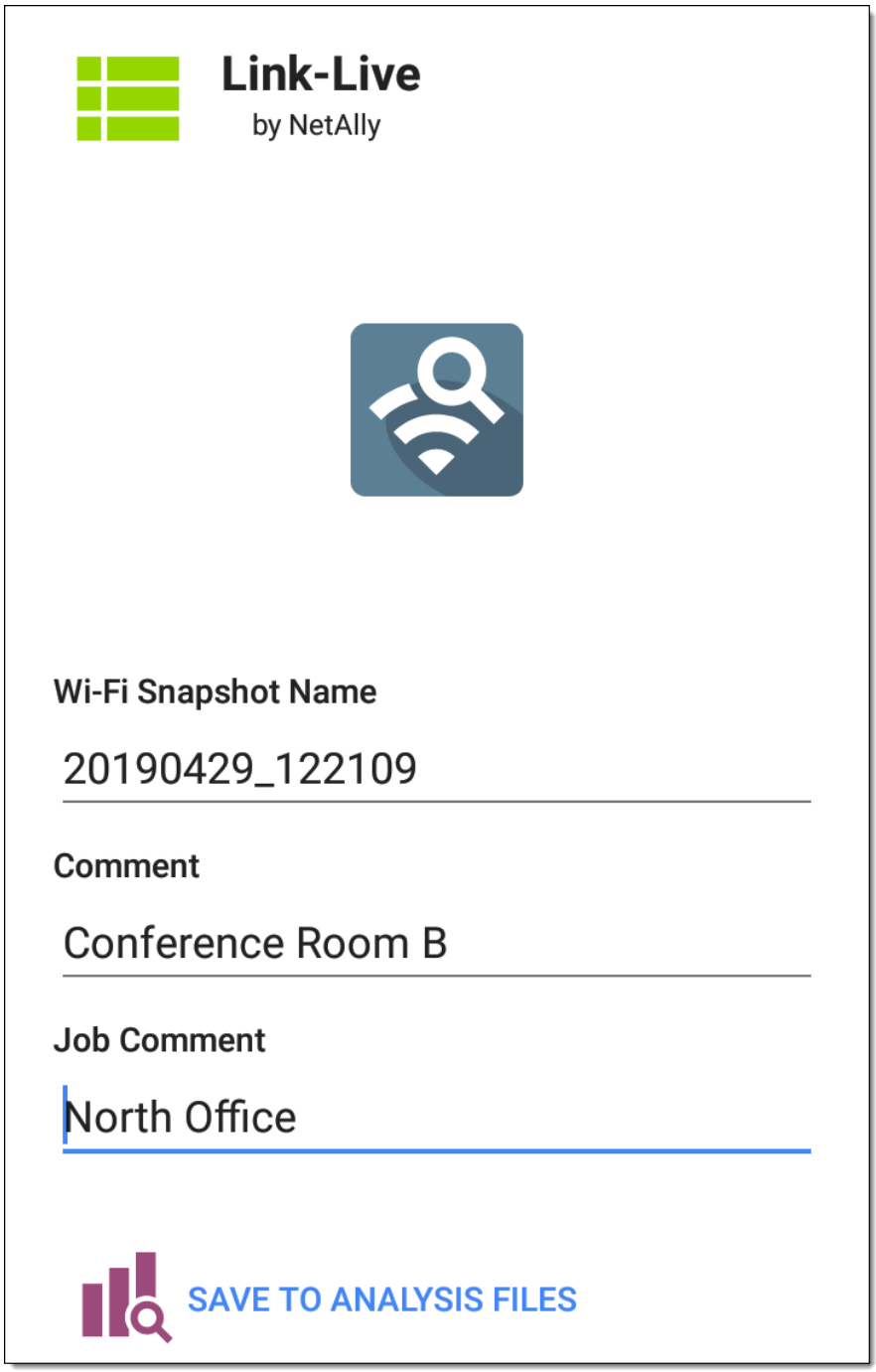
Link-Live Webpage	App Uploads
Results	AutoTest, Performance, iPerf, and Cable Test results Images, connect logs, and other files when saved to a test result
Uploaded Files	Captures, images, connect logs, and other file types
Analysis	Discovery, Wi-Fi, and Path Analysis results
AirMapper	**AirMapper Heatmaps**

If your unit is not claimed to Link-Live.com or if Link-Live is disabled on the app screen, the links and buttons for uploading to Link-Live in the testing apps do not appear.

Link-Live Sharing Screens

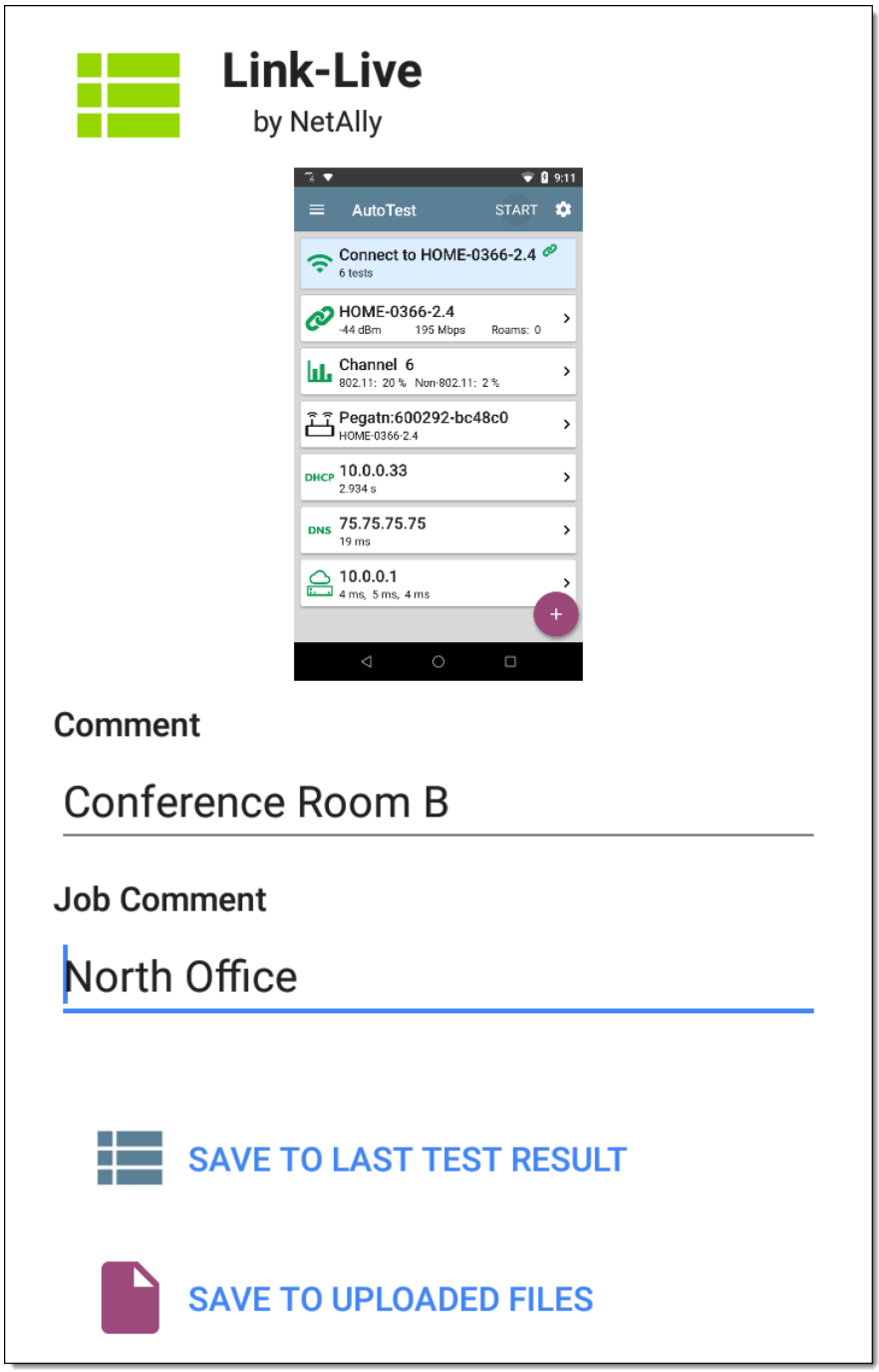
Whenever you select a button or link, like those above, to Upload, Save, or Share to Link-Live, a Link-Live sharing screen appears with the appropriate options for the data type.

For example, the Link-Live sharing screen for Discovery or Wi-Fi app data allows you to upload to the Analysis page on Link-Live.com.



The Link-Live sharing screen for a screenshot or other image allows you to attach it to the most recently run test result (AutoTest, Performance, iPerf, or Cable Test) (AutoTest or iPerf) on the

Results page, or to the Uploaded Files page on Link-Live.com.



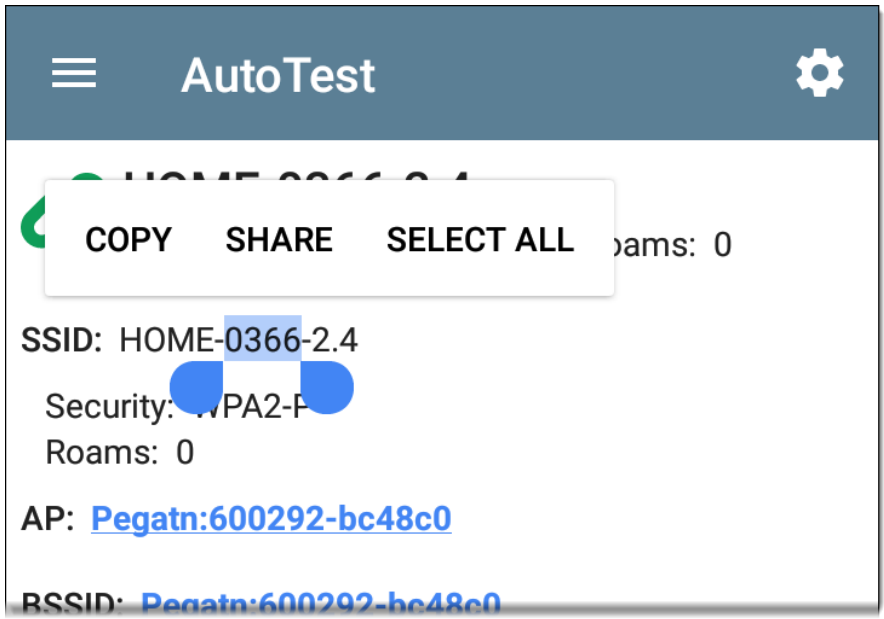
Remember, the regular **Comment** field uploads only to the current result or file, while the **Job**

Comment field uploads with all results and files until you change it.

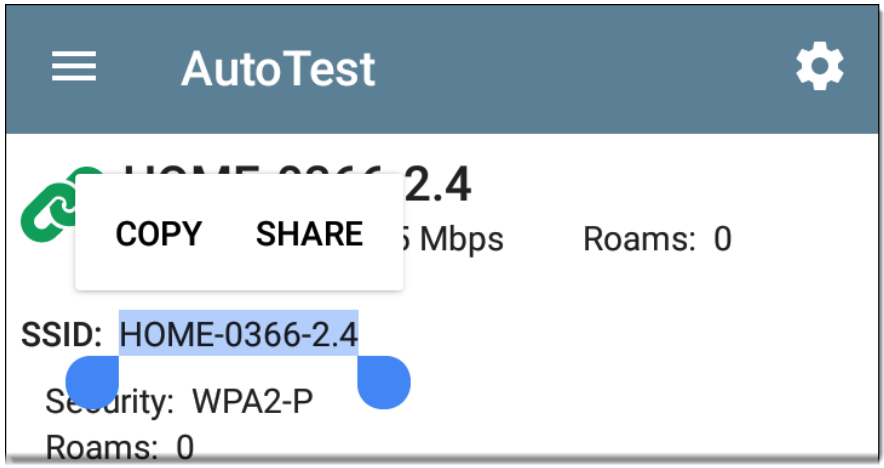
Sharing a Text File to Link-Live

You can also select and share text by long pressing text on the unit's screen. Text files are attached to the last test results on Link-Live.com.

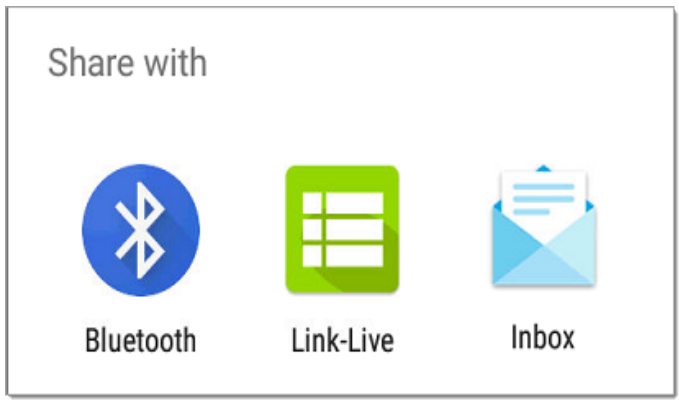
1. Long press a text string to select it.



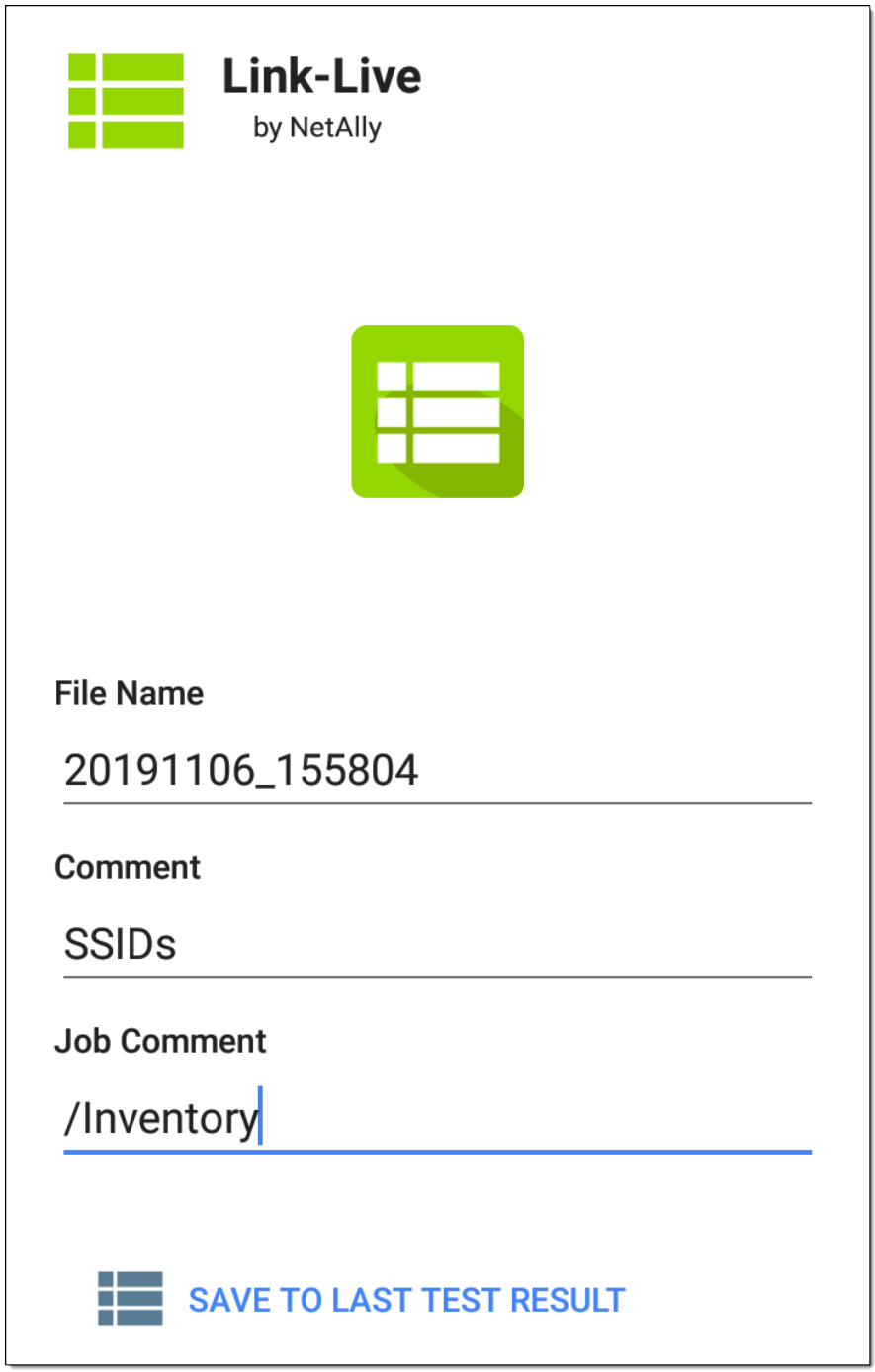
2. Tap **Select All** if needed.



3. Tap **SHARE**.



4. Select the Link-Live icon to open the Link-Live sharing screen.



5. Enter any comments as needed, and then tap **SAVE TO LAST TEST RESULT**.

Back to Title and Contents

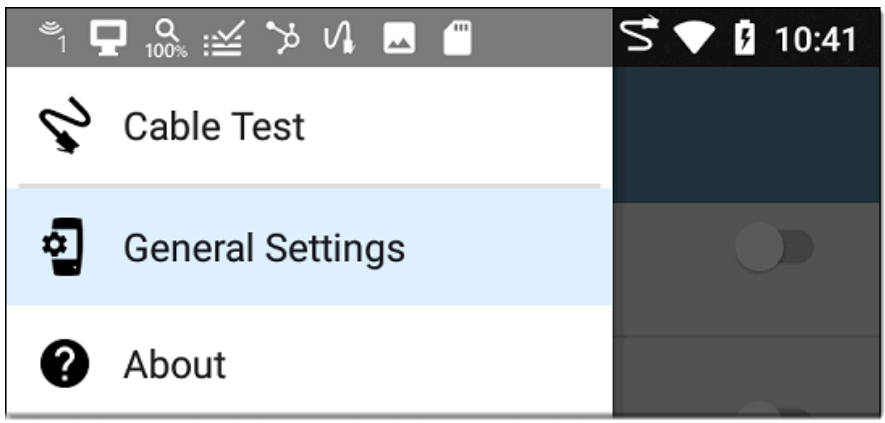
Cable Test App

EtherScope nXG's Cable Test can help you determine cable length and fault status, verify wiremapping of patch and structured cabling, and locate cable connections using toning. The cable testing port is the RJ-45 port on the left side of the EtherScope unit. Connect a cable to this port for testing and tracing with the tone function.

Cable Test Settings

The only setting that affects the Cable Test app is the **Distance Unit** setting, which designates Feet or Meters. This setting is contained in the General Settings menu.

1. To access General Settings, tap the menu icon on the Cable Test app screen, and select **General Settings**.

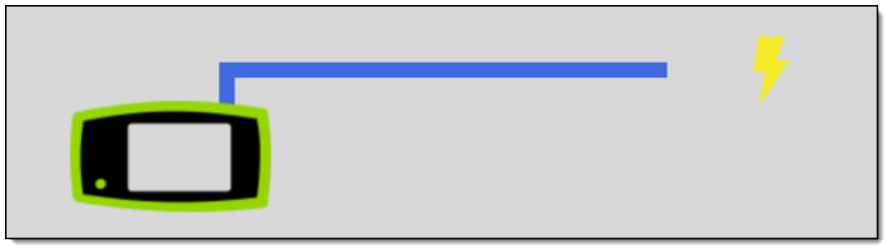


2. Scroll to the bottom of the Settings list under the **Preferences** heading.
3. Tap the **Distance Unit** field, and select either **Feet** or **Meters** as needed, then tap **OK**.

Running Cable Test

Refer to EtherScope nXG's Buttons and Ports as needed.

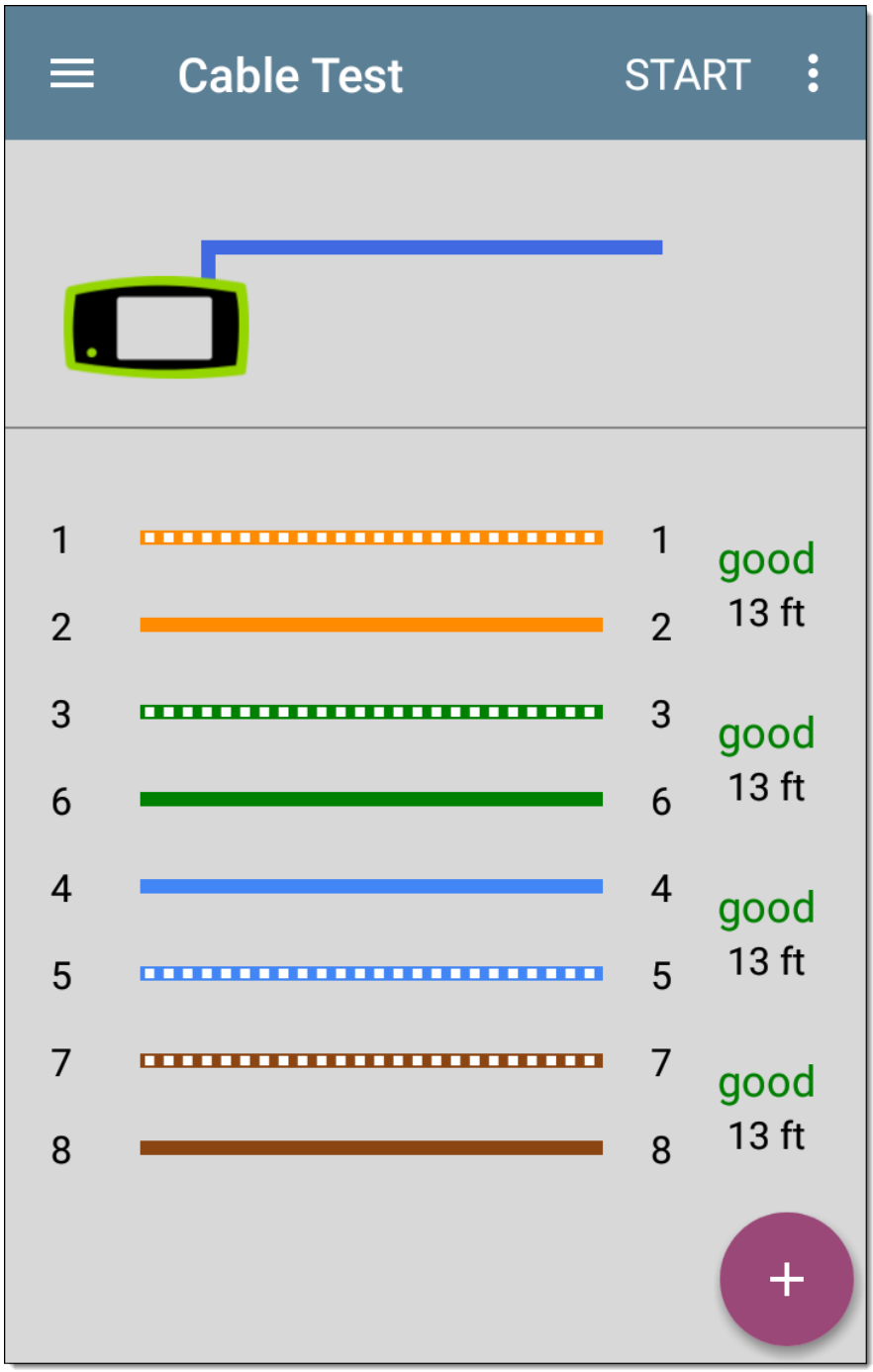
- With an open or unterminated cable connected to the RJ-45 cable test port (left side of the unit), you can measure length, identify shorts and splits, and locate opens.
- Using a cable terminated with a WireView Cable ID accessory, you can measure cable length and identify shorts, opens, split pairs, crossover cables, normal or negative pair polarity, and shielded cables.
- EtherScope nXG cannot perform a cable test on a cable that is connected to a switch; however, you can still use the toning function to trace the cable to the connected port.
- Additionally, you cannot run a cable test or use the toning feature if the unit detects voltage on the connected cable. The lightning bolt icon on the Cable Test screen indicates detected voltage.



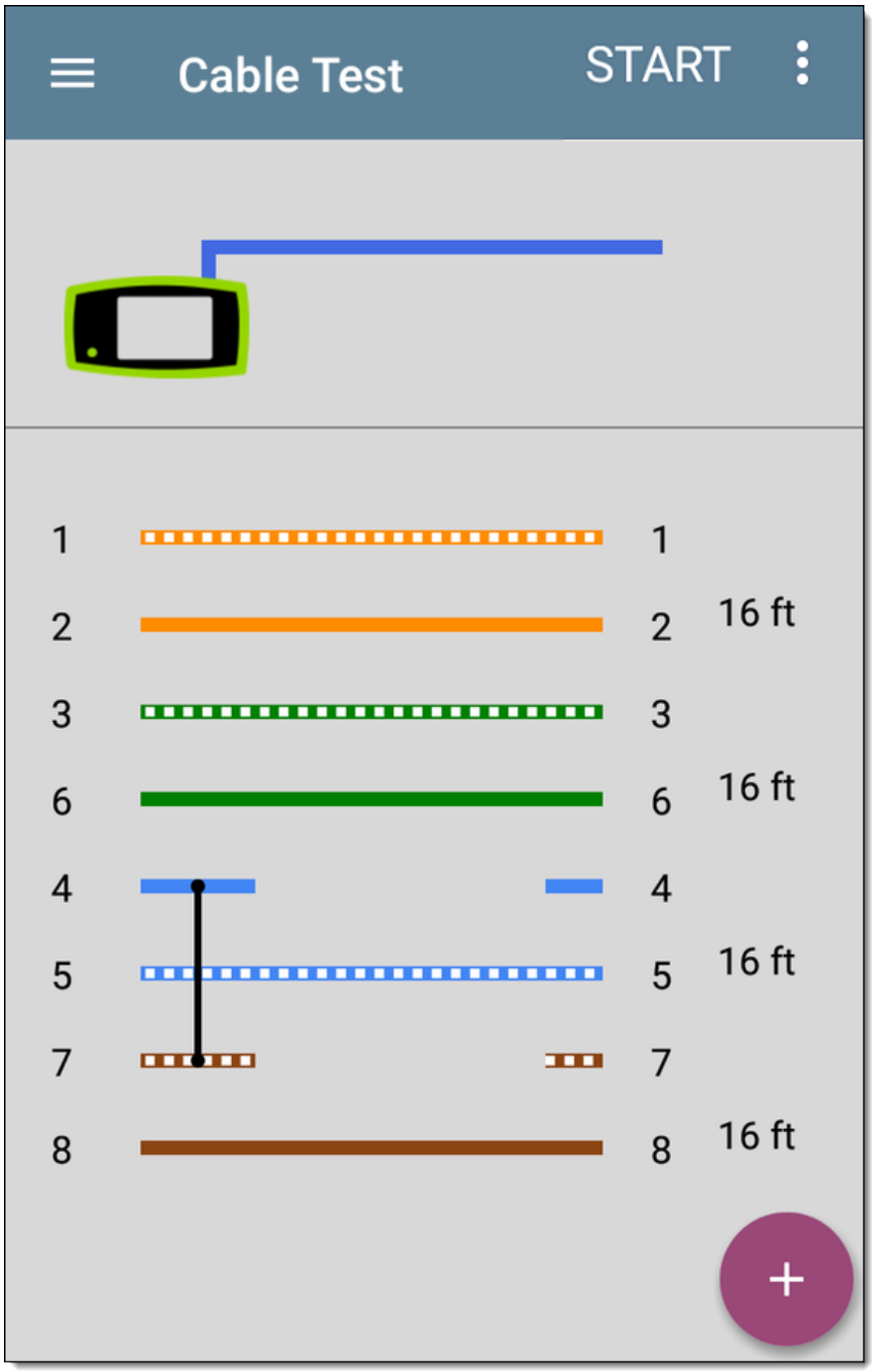
To start the cable test, tap **START** at the top right of the Cable Test app screen.

Open Cable TDR Testing

EtherScope nXG can measure the length of a cable and detect some faults by measuring the electrical reflections of the cable using Time Domain Reflectometry (TDR). Connect an open cable (unterminated) into the RJ-45 port on the left side of the EtherScope unit to measure its length and view any shorts, opens, or splits.



When a cable has no detected faults, "good" is shown next to each pair above the length measurement. Cable tests that detect a "split" or "open" in the cable also display the corresponding words.



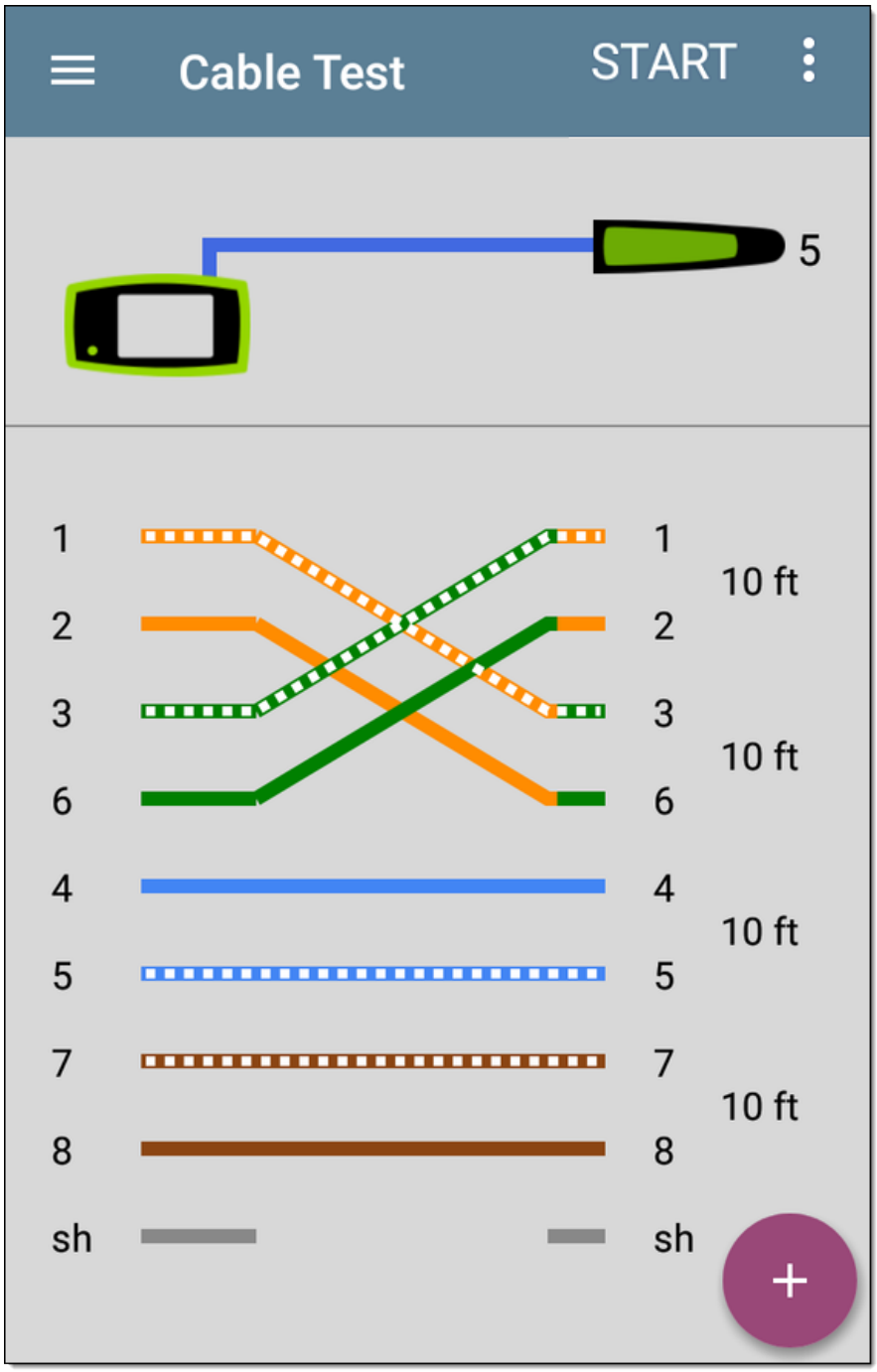
This unterminated cable test image shows a shorted cable between pins 4, 5, and 7.

Terminated WireView Testing

Using a WireView accessory provides more detailed, per-wire results. A WireView #1 is included with your EtherScope nXG. Additional WireViews 2-6 are available for purchase.

To run a terminated cable test, connect the left side RJ-45 port to a cable terminated with an external WireView Cable ID accessory.

The terminated cable test screen displays the number of the WireView attached, unless a cable fault prevents the EtherScope from detecting the WireView.



The image above indicates a crossover between pairs 1, 2 and 3, 6 and a WireView accessory number 5.

The last row of WireView results indicates whether the cable is shielded: an unbroken line between **sh** means a shielded cable is detected.

Toning Function

You can also trace a cable using a Fluke Networks* IntelliTone™ Probe, or any analog probe, and the Tone function.

Connect a cable into the left side RJ-45 port, and then tap the floating action button (FAB) . Select a Tone option from the menu. The EtherScope nXG emits the tone through the cable, and the probe detects it, allowing you to trace the wire or locate it in the switch closet.

* IntelliTone is a trademark of Fluke Networks.

Uploading Results to Link-Live

Tap the action overflow icon  at the top right of the Cable Test screen, and select **Upload to Link-Live** to send the current Cable Test result to the Results page  on Link-Live.com.

See the Link-Live chapter for more information.

Back to Title and Contents

Specifications and Compliance

This chapter contains device specifications and required compliance information.

EXG-200 Specifications

General

Dimensions	4.05 in x 7.67 in x 2.16 in (10.3 cm x 19.5 cm x 5.5 cm)
Weight	1.677 lbs (0.76 kg)
Battery	Rechargeable lithium-ion battery pack (7.2 V, 6.4 Ah, 46 Wh)
Battery Run Duration, Charge Time	Typical duration: 3-4 hours with all hardware powered on 8+ hours if wired test port is disabled Typical charge time: 2-4 hours
Display	5.0-inch color LCD with capacitive touchscreen (720 x 1280 pixels)
Host Interfaces	RJ-45 Cable Test and Management Port USB Type-A Port USB Type-C On-the-Go Port
SD Card Port	Supports Micro SD card storage
Memory	Approximately 8 GB available for storing test results and user applications

Charging	USB Type-C 45-W adapter: AC Input Power 100-240 V, 50-60 Hz; DC Output Power 15 V (3 A)
Media Access	Copper: 10M/100M/1G/2.5G/5G/10G Fiber SFP Adapters: 1G/10GBASE-X
Supported IEEE Standards	Wired: 802.3/ab/ae/an/bz/i/u/z Wi-Fi: 802.11a/b/g/n/ac PoE: 802.3af/at/bt, Class 0-8 and UPOE
Cable Test	Pair lengths, opens, shorts, splits, crossed, straight through, and WireView ID
Tone Generator	Digital tone: [455 KHz]; Analog tones: [400 Hz, 1 KHz]
LEDs	2 LEDs (Activity and Link Indicators)

Wireless

EtherScope nXG has two internal Wi-Fi Radios:

Wi-Fi Testing – 4x4 Dual-band 802.11ac Wave 2 wireless radio

System Wi-Fi, Bluetooth, and Management – 1x1 Dual-band 802.11ac Wave 2 + Bluetooth 5.0 and BLE wireless radio

Both are IEEE 802.11a/b/g/n/ac compliant.

4x4 Wi-Fi Radio for Testing

Applicant's Name	NetAlly
Model Number	BCM43465
Manufacturer	LITE-ON Technology Corporation
Manufacture Date	2017
Country of Origin	Taiwan
Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X (TKIP, AES)
Regulatory Domain	World Mode
Antenna Gain	1.1 dBi peak in the 2.4-GHz band; 3.2 dBi peak in the 5-GHz band

Data Rates

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11b**: 1, 2, 5.5, 11 Mbps
- **802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11n 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11n 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150 Mbps
- **802.11ac 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11ac 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 Mbps
- **802.11ac 80 MHz**: 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433 Mbps
- **802.11ac 160 MHz**: 65, 130, 260, 390, 520, 585, 650, 780, 867 Mbps

Operating Frequencies

The EtherScope nXG receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country.

These are the center frequencies of the channels that the Wi-Fi radio supports.

- **2.4-GHz band**: 2.412 – 2.484 GHz (channels 1 through 14)
- **5-GHz band**: 5.150 – 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)

Modulation

- **802.11b**: DBPSK (1 Mbps), DQPSK (2 Mbps), CCK (5.5 and 11 Mbps)
- **802.11g/n**: DBPSK, DQPSK, OFDM, BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM (proprietary)

Receive Sensitivity (Minimum)

- **6 Mbps**: -90 dBm
- **54 Mbps**: -71 dBm
- **802.11n 20 MHz**: -89 dBm (MSC 0/8)
- **802.11n 40 MHz**: -86 dBm (MSC 0/8)
- **VHT20 MCS 8**: -63 dBm
- **VHT40 MCS 9**: -60 dBm
- **VHT80 MCS 9**: -57 dBm

System 1x1 Wi-Fi/Bluetooth Adapter for Management

Applicant's Name	NetAlly
Model	Bluebean-A
Manufacturer	8devices
Manufacture Date	2019
Country of Origin	United States
Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X (TKIP, AES)
Regulatory Domain	World Mode
Antenna Peak Gain	+2.27 dBi in the 2.4-GHz band +5.18 dBi in the 5-GHz band

Data Rates

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11b**: 1, 2, 5.5, 11 Mbps
- **802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11n 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11n 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150 Mbps
- **802.11ac 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11ac 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 Mbps
- **802.11ac 80 MHz**: 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 Mbps

Operating Frequencies

The EtherScope nXG receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country.

These are the center frequencies of the channels that the Wi-Fi radio supports.

- **2.4-GHz band**: 2.412 – 2.484 GHz (channels 1 through 14)
- **5-GHz band**: 5.150 – 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)

Modulation

- **802.11a**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM
- **802.11n/ac**: BPSK (MCS0), QPSK (MCS1 and MCS2), 16 QAM (MCS3 and MCS4), 64 QAM (MCS5, 6, and 7), OFDM
- **802.11ac**: 256 QAM (MCS8 and MCS9), OFDM
- **802.11b**: DBPSK, BPSK (1 and 2 Mbps), QPSK (2 Mbps), CCK (5.5 and 11 Mbps)
- **802.11g**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM

Bluetooth v5 and BLE

- **Frequency Range**: 2.402 – 2.480 GHz
- **Max TX power**: 14 dBm (4 dBm BLE)

External Directional Antenna Accessory

Minimum gain: 5.0-dBi peak in the 2.4-GHz band and 7.0-dBi peak in the 5-GHz band

Reverse-polarity SMA plug

Antenna frequency range: 2.4 – 2.5 and 4.9 – 5.9 GHz

External antenna port is receive-only (no transmit).

Environmental Specifications

Operating Temperature	32°F to 113°F (0°C to +45°C) NOTE: The battery will not charge if the internal temperature of the unit is above 113°F (45°C).
Operating relative humidity (% RH without condensation)	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)
Storage Temperature	-4°F to 140°F (-20°C to +60°C)
Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	IEC 61010-1:2010: Pollution degree 2
Altitude	Operating: 4,000 m; Storage: 12,000 m

EXG-200 Certifications and Compliance

⚠ **CAUTION:** Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

CE	Conforms to relevant European Union directives.
	Conforms to relevant Australian Safety and EMC standards.
FC	Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.
C SA US	Listed by the Canadian Standards Association.

Industry Canada Class A emission compliance statement: This Class A digital apparatus complies with Canadian ICES-003. Avis de conformité à la réglementation d'Industrie Canada Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This device is not capable of transmitting in 5600-5650 MHz. This restriction is for the protection of Environment Canada’s weather radars operating in this band.

U-NII devices operating in the 5.25-5.35 GHz and 5.47-5.725 GHz band, without radar detection are restricted to use indoors.

Contains FCC IDs	WA7-43465, WA7-9377
Contains IC IDs	6627C-43465, 6627C-9377

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 contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s).

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : 1. L'appareil ne doit pas produire de brouillage; 2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Absorption Rate (SAR) information: This device meets the government's requirements for exposure to radio waves. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons regardless of age or health.

FCC RF Exposure Information and Statement: The SAR limit of USA (FCC) is 1.6 W/kg averaged over one gram of tissue. This device was tested for typical body-worn operations with the back of the handset kept 0 cm from the body. To maintain compliance with FCC RF exposure requirements, use accessories that maintain a 0 cm separation distance between the user's body and the back of the handset. The use of belt clips, holsters and similar accessories should not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

Body-worn Operation: This device was tested for typical body-worn operations. To comply with RF exposure requirements, a minimum separation distance of 0 cm must be maintained between the user's body and the handset, including the antenna. Third-party belt-clips, holsters, and similar accessories used by this device should not contain any metallic components. Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided. Use only the supplied or an approved antenna.

EMC	IEC 61326-1:2013: Basic Electromagnetic Environment; CISPR 11: Group 1, Class A

Group 1: Equipment has intentionally generated and/or uses conductively-coupled radio frequency energy that is necessary for the internal function of the equipment itself.

Class A: Equipment is suitable for use in all establishments other than domestic and those directly connected to a low-voltage power supply network that supplies buildings used for domestic purposes. There may be potential difficulties in ensuring electromagnetic compatibility in other environments due to conducted and radiated disturbances.

EU Compliance

This device complies with the following EU Directives: Directives 2014/53/EU, 2014/35/EU, and 2014/30/EU.

This device complies with RF specifications when the device is used at 0 mm from your body. Maximum measured SAR was 2.21 W/kg body; EU limit is 4.0 W/kg.

Accessory Information:

Adapter Model No.: FSP045-A1BR

Input: AC 100-240 V, 50/60 Hz 1.2 A

Output: DC 15 V, 3 A

Battery: 3250 mAh, 7.2 V 6.4 Ah

Wi-Fi: 2412 MHz-2472 MHz, 5180 MHz-5240 MHz, 5725 MHz - 5875 MHz

Bluetooth/BLE: 2402 MHz - 2480 MHz

เครื่องโทรคมนาคมและอุปกรณ์นี้ มีความสอดคล้องตามข้อกำหนดของ กสทช. (This telecommunication equipment conforms to the requirements of NBTC.)

EXG-300 Specifications

General

Dimensions	4.05 in x 7.67 in x 2.16 in (10.3 cm x 19.5 cm x 5.5 cm)
Weight	1.677 lbs (0.76 kg)
Battery	Rechargeable lithium-ion battery pack (7.2 V, 6.4 Ah, 46 Wh)
Battery Run Duration, Charge Time	Typical duration: 3-4 hours with all hardware powered on 8+ hours if wired test port is disabled Typical charge time: 2-4 hours
Display	5.0-inch color LCD with capacitive touchscreen (720 x 1280 pixels)
Host Interfaces	RJ-45 Cable Test and Management Port USB Type-A Port USB Type-C On-the-Go Port
SD Card Port	Supports Micro SD card storage
Memory	Approximately 8 GB available for storing test results and user applications

Charging Adapter	USB Type-C 45-W adapter: AC Input Power 100-240 V, 50-60 Hz; DC Output Power 15 V (3 A)
Supported IEEE Standards	Wired: 802.3/ab/ae/an/bz/i/u/z Wi-Fi: 802.11ax/ac/a/b/g/n PoE: 802.3af/at/bt, Class 0-8 and UPOE
Cable Test	Pair lengths, opens shorts, splits, crossed, straight through, and WireView ID
LEDs	2 LEDs (Activity and Link Indicators)

Wireless

EtherScope nXG has two internal Wi-Fi Radios:

- **Wi-Fi Testing** – Wi-Fi 6/6E 2x2 MU-MIMO wireless radio, IEEE 802.11 a/b/g/n/ac/ax compliant.
- **System Wi-Fi, Bluetooth, and Management** – 1x1 Dual-band, IEEE 802.11 a/b/g/n/ac compliant, Wave 2 + Bluetooth 5.0 and BLE wireless radio

WiFi 6/6E 2x2 MU-MIMO Radio for Testing

Applicant's Name	NetAlly
Model Number	WNFQ-268AXI(BT)
Manufacturer	SparkLAN Communications, Inc.
Manufacture Date	2021
Country of Origin	Taiwan
Security	64/128-bits WEP, WPA, WPA2, WPA3, 802.1x
Regulatory Domain	EXG-300 United States EXG-300C China EXG-300E World Mode
Internal Antenna Peak Gain (dBi, YZ plane)	+2.0 @ 2400-2500 GHz) +1.5 @ 4900-5850 GHz) +2.7 @ 5850-7200 GHz)

Data Rates

- **802.11a/g**: 54 Mbps
- **802.11ac**: MCS0~9
- **802.11ax**: HE0~11
- **802.11b**: 11 Mbps

- **802.11n**: MCS0~15
- **Bluetooth**: 1 Mbps, 2 Mbps, and up to 3 Mbps

Operating Frequencies (Test Wi-Fi, 3 Bands)

EXG-300/EXG-300E: The test unit receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country.

EXG-300C: The test unit receives and transmits only on the frequencies and channels allowed in the country.

Operating Frequencies (Management Wi-Fi, 2 Bands)

The test unit receives and transmits only on the frequencies and channels allowed in the country.

Modulation

Wi-Fi:

- **802.11a**: OFDM (BPSK, QPSK, 16-QAM, 64-QAM)

- **802.11ac**: OFDM (BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM)
- **802.11ax**: OFDMA (BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM)
- **802.11b**: DSSS (DBPSK, DQPSK, CCK)
- **802.11g**: OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
- **802.11n**: OFDM (BPSK, QPSK, 16-QAM, 64-QAM)

Bluetooth:

- **Header**: GFSK
- **Payload 2M**: π/4-DQPSK
- **Payload 3M**: 8-DPSK

Receive Sensitivity (Minimum)

- **802.11b, 11 Mbps**: -90 dBm
- **802.11g, 54 Mbps**: -76.5 dBm
- **802.11n / 2.4 GHz, HT20, MCS7**: -76 dBm
- **802.11n / 2.4 GHz, HT40, MCS7**: -73 dBm
- **802.11a 54 Mbps**: -97.5 dBm
- **802.11n / 5 GHz, HT20, MCS7**: -76.5 dBm
- **802.11n / 5 GHz, HT40, MCS7**: -76.5 dBm
- **802.11ac, VHT80, MCS9**: -62 dBm

- **802.11ac, VHT160, MCS9**: -62 dBm
- **802.11ax / 2.4 GHz, HE40, MCS 9**: -67 dBm
- **802.11ax / 5 GHz, HE20, HE11**: -64.5 dBm
- **802.11ax / 2.4 GHz, HE40, HE11**: -63.5 dBm
- **802.11ax / 2.4 GHz, HE80, HE11**: -59 dBm
- **802.11ax / 2.4 GHz, HE160, HE11**: -56.5 dBm
- **802.11ax / 6 GHz, HE20, HE11**: -63 dBm
- **802.11ax / 6 GHz, HE40, HE11**: -61 dBm
- **802.11ax / 6 GHz, HE80, HE11**: -58 dBm
- **802.11ax / 6 GHz, HE160, HE11**: -55 dBm
- **Bluetooth, 3 Mbps**: 0.1% BR, BER at -70 dBm

System 1x1 Wi-Fi/Bluetooth Adapter for Management

Applicant's Name	NetAlly
Model	Bluebean-A
Manufacturer	8devices
Manufacture Date	2019
Country of Origin	United States
Security	64/128-Bit WEP Key, WPA, WPA2, 802.1X (TKIP, AES)
Regulatory Domain	EXG-300 United States EXG-300C China EXG-300E World Mode
Antenna Peak Gain	+2.27 dBi in the 2.4-GHz band +5.18 dBi in the 5-GHz band

Data Rates

- **802.11a**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11b**: 1, 2, 5.5, 11 Mbps
- **802.11g**: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- **802.11n 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11n 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150 Mbps

- **802.11ac 20 MHz**: 7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7 Mbps
- **802.11ac 40 MHz**: 15, 30, 45, 60, 90, 120, 135, 150, 180, 200 Mbps
- **802.11ac 80 MHz**: 32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 Mbps

Operating Frequencies

The EtherScope nXG receives on all of the frequencies in every country, but transmits only on the frequencies and channels allowed in the country or if the unit detects the AP 802.11d domain.

The following channels are supported in each band:

- **2.4-GHz band**: 2.412 – 2.484 GHz (channels 1 through 14)
- **5-GHz band**: 5.150 – 5.825 GHz (channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165)
- **6-GHz band**:
    - 5.925 – 6.425 GHz (Channels 1E, 5E, 9E, 13E, 17E, 21E, 25E, 29E, 33E, 37E, 41E, 45E, 49E, 53E, 57E, 61E, 65E, 69E, 73E, 77E, 81E, 85E, 89E, 93E)

- 6.425 – 6.525 GHz (Channels 97E, 101E, 105E, 109E, 113E)
- 6.525 – 6.825 GHz (Channels 117E, 121E, 125E, 129E, 133E, 137E, 141E, 145E, 149E, 153E, 157E, 161E, 165E, 169E, 173E, 177E, 181E, 185E)
- 6.825 – 7.125 GHz (Channels 189E, 193E, 197E, 201E, 205E, 209E, 213E, 217E, 221E, 225E, 229E, 233E)

Modulation

- **802.11a**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM
- **802.11n/ac**: BPSK (MCS0), QPSK (MCS1 and MCS2), 16 QAM (MCS3 and MCS4), 64 QAM (MCS5, 6, and 7), OFDM
- **802.11ac**: 256 QAM (MCS8 and MCS9), OFDM
- **802.11b**: DBPSK, BPSK (1 and 2 Mbps), QPSK (2 Mbps), CCK (5.5 and 11 Mbps)
- **802.11g**: BPSK (6 and 9 Mbps), QPSK (12 and 18 Mbps), 16 QAM (24 and 36 Mbps), 64 QAM (48 and 54 Mbps), OFDM

Bluetooth v5 and BLE

- **Frequency Range**: 2.402 – 2.480 GHz
- **Max TX power**: 14 dBm (4 dBm BLE)

External Directional Antenna Accessory

- Antenna type: patch directional
- Average gain: 2.4 GHz: +6.4 dBi, 5 GHz: +8.9 dBi, 6 GHz: +8.6 dBi
- RP-SMA connector
- Frequency range: 2400-2500, 4900-5925, 6000-7125 (MHz)
- Receive only antenna (no transmit allowed)

Environmental Specifications

Operating Temperature	32°F to 113°F (0°C to +45°C) NOTE: The battery will not charge if the internal temperature of the unit is above 113°F (45°C).
Operating relative humidity (% RH without condensation)	90% (50°F to 95°F; 10°C to 35°C) 75% (95°F to 113°F; 35°C to 45°C)
Storage Temperature	-4°F to 140°F (-20°C to +60°C)

Shock and vibration	Meets the requirements of MIL-PRF-28800F for Class 3 Equipment
Safety	IEC 61010-1:2010: Pollution degree 2
Altitude	Operating: 4,000 m; Storage: 12,000 m

EXG-300 Certifications and Compliance

⚠ **CAUTION:** Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FC	Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.
	Conforms to relevant Australian Safety and EMC standards.
C SA ® US	Listed by the Canadian Standards Association.
CE	Conforms to relevant European Union directives.
UK CA	Complies with United Kingdom and European Economic Area radiation

	exposure limits.

Also includes Japan Indoor Use Statement and Taiwan Regulatory Statement

	FCC Notices
Contains FCC IDs	RYK-WNFQ268AXBT, WA7-9377
Contains IC IDs	6158A-WNFQ268AXBT, 6627C-9377

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.

Caution: Any changes or modifications made to the equipment without the approval of manufacturer could void the user's authority to operate this equipment.

The device is for indoor use. This equipment may only be operated indoors. Operation outdoors is in violation of 47 U.S.C. 301 and could subject the operator to serious legal penalties.

The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

Warning: FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 25 cm between the radiator and your body.

	**Australian IEC 61326-1:2013: Basic Electromagnetic Environment; CISPR 11: Group 1, Class A**

Group 1: Equipment has intentionally generated and/or uses conductively-coupled radio frequency energy that is necessary for

the internal function of the equipment itself.

Class A: Equipment is suitable for use in all establishments other than domestic and those directly connected to a low-voltage power supply network that supplies buildings used for domestic purposes. There may be potential difficulties in ensuring electromagnetic compatibility in other environments due to conducted and radiated disturbances.

Innovation, Science and Economic Development Canada

Innovation, Sciences et Développement économique Canada

Warning: For indoor use only. Pour une utilisation en intérieur uniquement. This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est

autorisée aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compirs un brouillage brouillage susceptible de provoquer un fonctionnement indésirable.

Warning: IC Radiation Exposure Statement: This equipment complies with RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 27 cm between the radiator & your body.

Avertissement: Cet équipement est conforme aux limites d'exposition aux rayonnements RSS-102 établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

Caution: The device for operation in the band 5150-5530 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Avertissement: les dispositifs fonctionnant dans la bande 5150-5530 MHz sont réservés uniquement pour une utilisation à l’intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêemes canaux.

This radio transmitter has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in the SparkLAN WNFQ-268AXI(BT) Datasheet, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Cet émetteur radio a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antennes répertoriés dans la fiche technique SparkLAN WNFQ-268AXI(BT), avec le gain maximal autorisé indiqué. Les types d'antenne non inclus dans cette liste qui ont

un gain supérieur au gain maximum indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.

CE European Union (EU) Radiation Warning Statement and Conformance Notices

Warning: This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

Selling Countries:

Restrictions or requirements in the UK

AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK (NI)

This device complies with the following EU

Directives: Directives 2014/53/EU, 2014/35/EU, and 2014/30/EU.

Accessory Information:

Adapter Model No.: FSP045-A1BR

Input: AC 100-240 V, 50/60 Hz 1.2 A

Output: DC 15 V, 3 A

Battery: 3250 mAh, 7.2 V 6.4 Ah

Japan Indoor Use Statement

For Japan, the EXG-300E is restricted for indoor use in the 5150-5530 MHz band only.

Taiwan Regulatory Statement

Article 12: For low-power RF motors that have passed the type certification, companies, firms or users are not allowed to change the frequency, increase the power, or change the features and functions of the original design without permission.

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不

得擅自變更頻率、加大功率或變更原設計之特性及功能。

Article 14: The use of low-power radio frequency motors shall not affect flight safety or interfere with legal communications; if any interference is found, it shall be stopped immediately, and it shall be continued to be used until there is no interference. The legal communication referred to in the preceding paragraph refers to the radio communication operated in accordance with the provisions of the Telecommunications Law. Low power radio frequency motors are subject to interference from legal communications or radio wave radiating electrical equipment for industrial, scientific and medical use.

第十四條低功率射頻電機之使用不得影響飛航安全及干擾合法通信;經發現有干擾現象時,應立即停用,並改善至無干擾時方得繼續使用。前項合法通信,指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Wireless information transmission equipment operating in the 5.25-5.35 kHz frequency band is limited to indoor use.

在5.25-5.35 秭赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

Complies with United Kingdom and European Economic Area radiation exposure limits

This equipment complies with the UK and EEA radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body. The frequency and the maximum transmitted power in the UK and European Conformity are listed below:

2402-2480 MHz (LE) 9.63 dBm

2405-2480 MHz 9.81 dBm

2412-2472 MHz 19.96 dBm

5180-5240 MHz 22.95 dBm

5260-5320 MHz 22.98 dBm

5500-5700 MHz 22.98 dBm

5745-5825 MHz 22.98 dBm

5955-5825 MHz 22.98 dBm

5955-6415 MHz 22.97 dBm

6489-7987.2 MHz -41.58 dBm/RBW

The device is restricted to indoor use only when operating in the 5295 to 6425 MHz frequency range.

Hereby, NetAlly declares that the radio equipment EtherScope is in compliance with Radio Equipment Regulations 2017.

Back to Title and Contents