



CYBERSCOPE™

User Guide

Tap a [link](#) to go directly to the app's chapter.
Scroll down to view the full list of Contents.

[NetAlly Network Testing Apps](#)



[AutoTest](#)



[Nmap](#)



[Discovery](#)



[Wi-Fi](#)



[AirMapper™](#)



[Path Analysis](#)



[Spectrum](#)



[Ping/TCP](#)



[Capture](#)



[Performance](#)



[iPerf](#)



[LANBERT™](#)



[Cable Test](#)



[Link-Live](#)

Software v2.6. Published September 19, 2024

Contents

Contact Us	16
Introduction	17
How to Use this Guide	18
Differences Between Models	22
Differences Between Models	24
Buttons and Ports	26
Charging and Power	31
PoE Charging	31
Safety and Maintenance	34
Legal Notification	37
Home and System Interface	38
Home Screen	39
Navigating the System	41
System Status Bar and Notifications ...	45
Notification Panel	45
Apps Screen and Store	48
Device Settings	52
Quick Settings Panel	53
Connecting to Wi-Fi	57
Captive Portals	60
Configuring for Enterprise Security ...	61

Sharing	70
Sharing a Screenshot	73
Changing the Device Language	75
CyberScope Settings and Tools	77
Navigation Drawer	78
About Screen	80
Exporting Logs	81
Import/Export for All Apps	81
Restarting the Test Unit	82
Test and Management Ports	83
Test Ports	84
Selecting Ports	89
CyberScope General Settings	92
Wi-Fi General Settings	93
Wired General Settings	97
Management	101
Preferences	104
Trending Graphs	105
Common Icons	109
Floating Action Button (FAB) and Menu	110
Common Tools	113
Web Browser/Chromium	113

Telnet/SSH	113
Camera and Flashlight	115
Software Management	116
Managing Files	117
Files Application	117
How to Move or Copy a File	120
Using a Micro SD Card	121
Using a USB Drive	122
Ejecting Storage Media	124
Using a USB Type-C to USB Cable	124
Updating Software	127
Remote Access	132
Using VNC	134
Using Link-Live Remote	135
Managing NetAlly App Settings	137
Resetting Testing App Defaults	137
Saving App Settings and Configurations	141
Import/Export Settings	145
Import/Export Settings for All Apps ..	155
Resetting CyberScope Factory Defaults	157
CyberScope Feature Access	160

Introduction to Feature Access	161
Controlling Feature Access	169
Permanently Disabling Features	175
Changing the Administrative Password	181
CyberScope Testing Applications ..	184
AutoTest App and Profiles	185
AutoTest Overview	187
Managing Profiles and Profile Groups ..	190
Factory Default Profiles	190
Adding New Profiles	192
Profile Groups	198
Creating New Profile Groups	203
Import/Export AutoTest Profiles	206
Main AutoTest Screen	207
Periodic AutoTest	209
Periodic AutoTest Settings	209
Running Periodic AutoTest	211
Wired AutoTest Profiles	214
Wired Profile Settings	218
PoE Test Settings	219
Wired Connection Settings	222
VLAN Settings	229

Stop After	231
HTTP Proxy	232
Wired Profile Test Results	234
PoE Test Results	236
Wired Link Test Results	239
802.1X Test Results	245
VLAN Test Results	247
Switch Test Results	250
Wired Profile FAB	257
Wi-Fi AutoTest Profiles	261
Wi-Fi Profile Settings	265
Wi-Fi Connection Settings	267
Advanced (Wi-Fi Connection) Settings	278
Channel Test Settings	282
HTTP Proxy	285
Wi-Fi Profile Test Results	287
Wi-Fi Link Test Results	290
Connect Log	300
Channel Test Results	301
Other Actions (Wi-Fi Profile FAB)	307
DHCP, DNS, and Gateway Tests	311
DHCP or Static IP Test	312
DNS Test	326

Test Targets for Wired and Wi-Fi

AutoTest	337
Adding and Managing Test Targets ...	338
AutoTest TCP Connect Test	351
FTP Test	368
Nmap Test	378
Air Quality AutoTest Profiles	385
Air Quality Profile Results	387
Viewing and Saving Results	391
Air Quality Profile Settings	393

Nmap App

399

Nmap Tests	403
Editing Nmap Test Parameters	410
Running Nmap Tests	417
Nmap Runner Settings	419
Nmap Output	423

Discovery App

431

Introduction to Discovery	433
Main Discovery List Screen	435
Searching the Discovery List	439
Filtering the Discovery List	441
Sorting the Discovery List	444

Security Auditing – Batch	
Authorization	446
Refreshing Discovery	451
Uploading Results to Link-Live	452
Discovery Details Screens	454
Top Details Card	456
Lower Cards in Device Details	462
Problems	464
Addresses	465
TCP Port Scan	467
VLANs	469
Interfaces	470
SNMP	476
Connected Devices	477
Resources	478
SSIDs	479
Discovery App Floating Action Menu .	481
Device Types	488
Routers	489
Switches	490
Unknown Switches	491
Network Servers	492
Hypervisors	493

Virtual Machines	494
Wi-Fi Controllers	495
Access Points (APs)	496
Wi-Fi Clients	497
VoIP Phones	498
Printers	499
SNMP Agents	500
Network Tools	501
Hosts/Clients	502
Device Names and Authorization	505
Assigning a Name and Authorization to a Device	505
Discovery Settings	518
Active Discovery Ports	521
Extended Ranges	522
ARP Sweep Rate	526
Refresh Interval	526
SNMP Configuration	527
Nmap Tests	538
Auto AP Grouping Rules	539
Problem Settings	547
TCP Port Scan Settings	550
Wi-Fi Analysis App	553

Wi-Fi Analysis and Discovery	555
Wi-Fi App Screens	556
Wi-Fi App List Screens	557
Filtering in the Wi-Fi App	561
Sorting in the Wi-Fi App	566
Clearing All Problems	568
Setting Authorization	569
Uploading Results to Link-Live	570
Wi-Fi Details Screens	572
Wi-Fi Problems Screen	575
RF and Traffic Statistics Overview	577
Locating Wi-Fi Devices	582
Channels Map	593
Map and Map 6E Tabs	594
Channels	602
SSIDs	607
APs	612
BSSIDs	616
Clients	629
Bluetooth	638
AirMapper™ App	643
AirMapper Settings	644

Configuring an AirMapper Survey	645
Collecting AirMapper Data	655
Path Analysis App	672
Introduction to Path Analysis	673
Path Analysis Settings	674
Populating Path Analysis from Another App	674
Configuring Path Analysis Manually ..	674
Running Path Analysis	677
Path Analysis Results and Source CyberScope Cards	678
Layer 3 Hops	681
Layer 2 Devices	686
Uploading Results to Link-Live	692
Spectrum Test App	694
Using the Spectrum Views	695
Uploading Results to Link-Live	703
Spectrum Settings	705
Changing Spectrum Views	705
Saving Settings	705
Changing Spectrum Settings	706
Ping/TCP Test App	709

Ping/TCP Settings	710
Populating Ping/TCP from Another App	710
Configuring Ping/TCP Settings Manually	712
Running Ping/TCP Tests	715
Capture App	719
Capture Settings	720
Running and Viewing Captures	725
Link-Live Cloud Service	731
Getting Started in Link-Live Cloud Service	733
Claiming the Unit	733
After Claiming	735
Unclaiming	736
AllyCare Code	737
Private Link-Live Settings	738
Link-Live App Features	739
Saving Locally Only	743
Job Comment	745
Link-Live and Testing Apps	748
Link-Live Sharing Screens	749

Sharing a Text File to Link-Live	752
Performance Test App	761
Introduction to Performance Testing .	763
Performance Test Settings	765
Saving Custom Performance Tests ...	766
Configuring the Source CyberScope ..	771
Configuring Performance Endpoints ..	788
OneTouch 10G Performance Peer	789
LinkRunner G2 Reflector	791
LinkRunner AT Reflector	793
NPT Reflector Software	795
Running a Performance Test	797
Performance Test Results	798
Performance Service Detailed Results	800
Uploading Results to Link-Live	808
Running CyberScope as a Performance	
Peer	812
iPerf Test App	816
iPerf Settings	818
Saving Custom iPerf Settings	818
Test Accessories in Discovery	819
Configuring iPerf Settings	822

Running an iPerf Test	827
Uploading Results to Link-Live	831
LANBERT™ Test App	833
LANBERT Settings	834
Configuring LANBERT Generator Settings	834
Configuring LANBERT Loopback Settings	839
Running a LANBERT Test	840
Uploading Results to Link-Live	847
Cable Test App	850
Cable Test Settings	851
Running Cable Test	853
Uploading Results to Link-Live	863
Switch App	864
Running Switch	865
Specifications and Compliance	868
CyberScope Specifications	869
General	869
Wireless	870
Environmental Specifications	878

CyberScope Certifications and Compliance	880
Index	892

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:
Cyberscope.netally.com/

For customer support, visit:
NetAlly.com/Support

Register your CyberScope

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 CyberScope is a rugged, handheld cyber security analyzer. The multi-function tools and various applications allow comprehensive site security surveying, analysis and reporting for your on-premises site 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 CyberScope to access these features.


How to Use this Guide

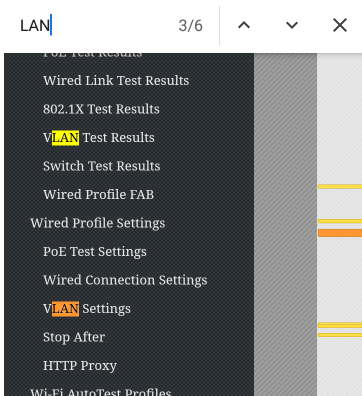
This user guide describes the CyberScope's testing functionality and basic elements of the system interface.

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

The CyberScope is also referred to as just CyberScope 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 CyberScope, 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](#), 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 CyberScope user guide is available if you [change the device language](#) to one of those languages. The English user manual is used if you change the language to German, Japanese, or Korean.

Differences Between Models

The Model number of your CyberScope 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:

CYBERSCOPE-CE, CYBERSCOPE-CE-E, CYBERSCOPE-CE-C, CYBERSCOPE-XRF

- CYBERSCOPE-CE: Supports 2.4 GHz, 5 GHz, and 6 GHz frequency bands; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.
- CyberScope-CE-E: 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.
- CyberScope-CE-C: Supports 2.4 GHz and 5 GHz frequency bands, limited by 802.11d regional domain specification; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.

- CyberScope-XRF: Identical to CYBERSCOPE-CE but does not support wireless features and apps.

For more information, see [CyberScope Specifications](#).

Differences Between Models

The Model number of your CyberScope 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:

CYBERSCOPE-CE, CYBERSCOPE-CE-E, CYBERSCOPE-CE-C, CYBERSCOPE-XRF

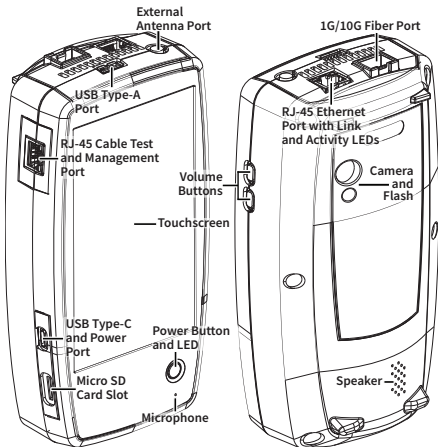
- CYBERSCOPE-CE: Supports 2.4 GHz, 5 GHz, and 6 GHz frequency bands; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.
- CyberScope-CE-E: Supports 2.4 GHz, 5 GHz, and 6 GHz frequency bands, limited by 802.11d regional domain specification; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.
- CyberScope-CE-C: Supports 2.4 GHz and 5 GHz frequency bands, limited by 802.11d regional domain specification; supports 802.11a/b/g/n/ac/ax Wi-Fi standards.

- CyberScope-XRF: Identical to CYBERSCOPE-CE but does not support wireless features and apps.

For more information, see [CyberScope Specifications](#).

Buttons and Ports

Button and port functions on your CyberScope 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 Flashlight	Captures images and acts as a flashlight
Micro SD Card Slot	Used for removable storage expansion (See Inserting a Micro SD Card below.)

FEATURE	DESCRIPTION
Volume Buttons	Increase or decrease the audio volume
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

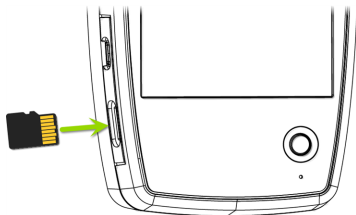
See [Test and Management Ports](#) for detailed explanations of the port functions.

See [Updating Software](#) for requirements on updating system software.

Refer to the product [Specifications](#) if needed.

Inserting a Micro SD Card

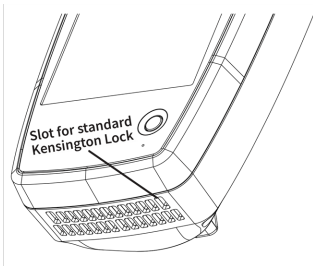
A Micro SD card must be inserted with the *metal contacts facing the front* (towards the touchscreen) of the unit, as shown below.



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 slot for a standard Kensington lock is the right front vent hole on the bottom of the unit, as shown below.



Charging and Power

Your CyberScope 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 CyberScope detects a new copper link in the top [Wired Test Port](#).

See [Buttons and Ports](#) for port locations and descriptions.

Powering On

- To start 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.


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.

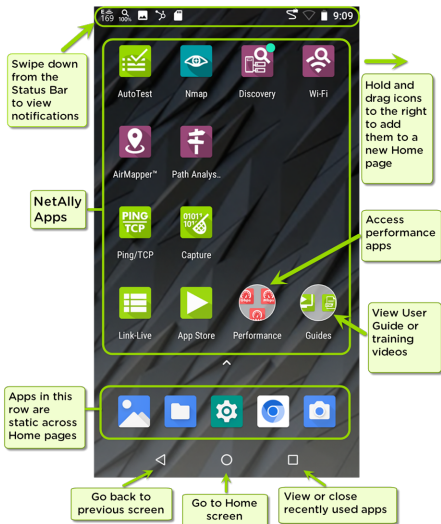
© 2019-2024 NetAlly

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 CyberScope 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



Like other hand-held devices, your CyberScope 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 CyberScope 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 them. 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).

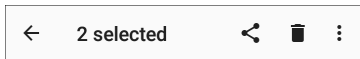
Swiping


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.

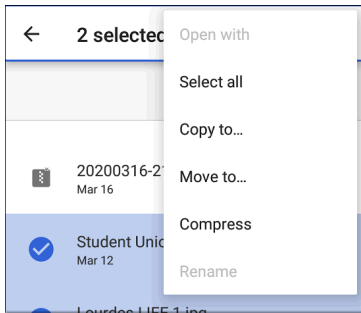
Long Pressing

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.





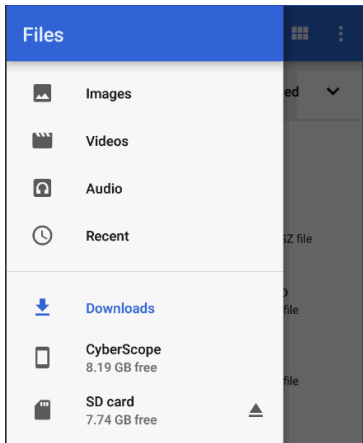
Additional options often appear in an overflow menu, designated by the action overflow icon .




You can also long press on text on most screens to open options for copying and [sharing](#) the text.

Left-Side Navigation Drawer

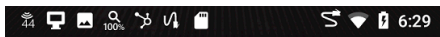
In the [Files](#)  app, tap the Menu icon  or or swipe right to open the navigation drawer. It displays the folders in your file system.



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 **CyberScope CyberScope Airfolder** and sub-folders, as shown above.

See the [Navigation Drawer](#) topic for additional information.

System Status Bar and Notifications



The Status Bar across the top of the screen displays notification icons from the system as well as CyberScope-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 CyberScope 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.



NetAlly ^

Mode: Scanning Channel: 85E

Channel Width: 160 MHz

Tester System • 31m ▾

Screenshot captured.

Tap to view your screenshot.



Discovery

Discovery Status: 100%

NetAlly

Wired Management Port

IP Address: 192.168.0.106

Tester System ▾


SD card

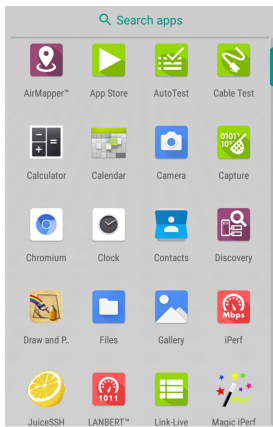
For transferring photos and media

- 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 CyberScope 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 .

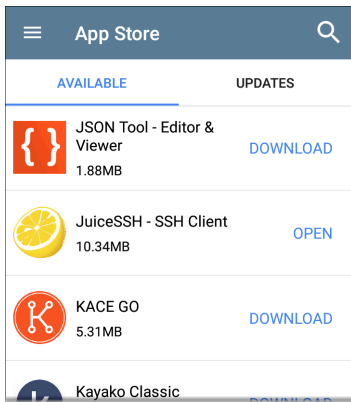


The Apps screen displays all the apps on your device. The image above is an example. Your Apps screen may contain different third-party apps.


- 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 CyberScope.




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

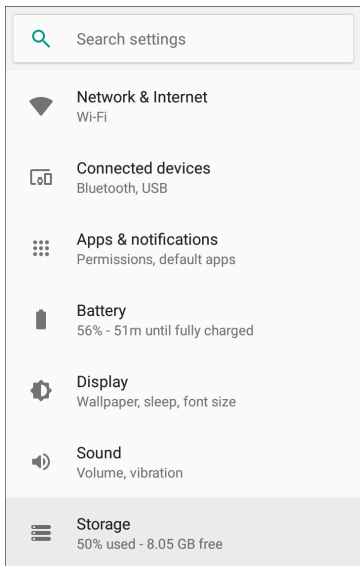
- Tap the search icon to search for an App.
- Tap **UPDATES** to view available updates of installed apps.
- To request that an App be added to the App Store, visit the Apps  page at [Link-](#)

[Live.com](https://www.live.com), and select the floating action button (FAB) at the lower right corner to

▶ **Request or Upload an App.**

Device Settings

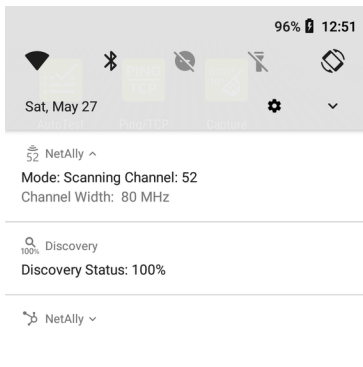
To access the system device settings, tap the Settings  icon at the bottom of the [Home screen](#).



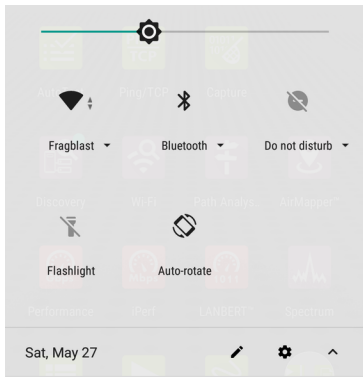
The device settings screen lets you adjust the display; adjust sound (including volume for external Bluetooth or USB speakers or headsets); set date and time; view installed applications and memory devices; [connect to Wi-Fi](#); or [reset to factory defaults](#).


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 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 Chinese, English, German, Japanese, and Korean language displays. See [Changing the Device Language](#) for information on changing the device interface language. The user guide is available in Chinese and English. See [How to Use this Guide](#).

Connecting to Wi-Fi

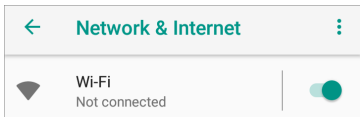
Basic connectivity to Wi-Fi is done using the Wi-Fi Management Port (configured in the system network settings). The [Wi-Fi Management Port](#) is separate from the Wi-Fi test ports. It can access the internet, be used by other system applications, upload test results to the Link-Live web site, and be 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.

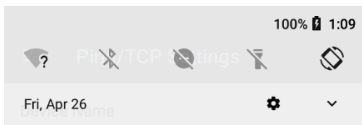
To connect your CyberScope to a Wi-Fi network:

1. Open the system Wi-Fi Device Settings using either method below:
 - Open the device Wi-Fi settings from the main [Device Settings](#) screen by tapping

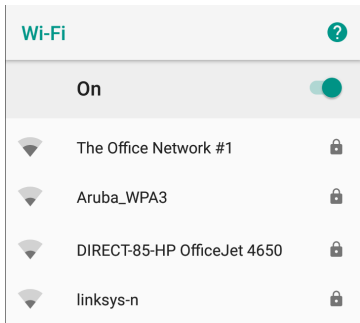
the Settings icon  and selecting **Network & Internet > Wi-Fi**.



- 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 method opens the Wi-Fi settings screen:




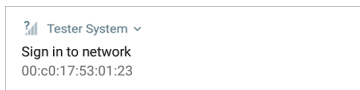
2. Ensure the Wi-Fi feature is **On**.
3. Tap an available Wi-Fi network in the list.
4. Enter the network's security credentials. (Most networks only require a password, but depending on the security settings, some may also require a company username, EAP type, authentication type, certificate, or other credentials.)
5. 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.

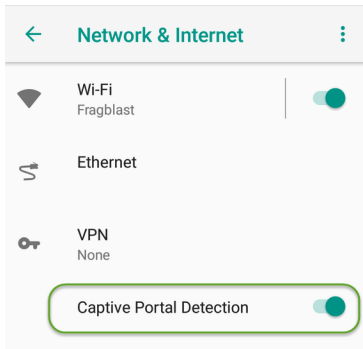
Captive Portals

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
- Clients:certificates 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 CyberScope, 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 CyberScope, 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.

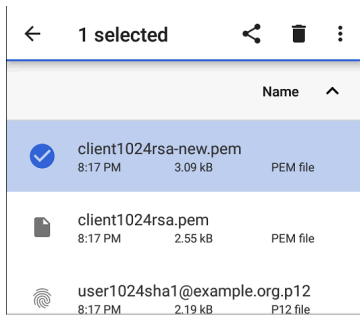
10. (Optional) Verify the client certificate installed correctly:
 - a. Tap the system **BACK** button to return to Encryption & credentials.
 - b. Tap **User credentials**.
 - c. Verify that the name of your client certificate file (for example, **FreeRadius client**) is displayed.
11. Press the system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


Sharing

The system **Files**  app lets you share files from internal or external storage 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 the Navigation menu  or the [left-side navigation drawer](#).
3. Long-press on one or multiple files to select.



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

Share via




Link-Live




Bluetooth

5. Tap to choose a sharing method and follow the system prompts to share the file or files.
6. (Optional) If uploading to [Link-Live](#):

- a. Tap the  **Link-Live** option.

**Link-Live**
by NetAlly



File Name


client1024rsa-new.pem


Comment

Certs

Job Comment

South Campus Wi-Fi

 **SAVE TO LAST TEST RESULT**

 **SAVE TO UPLOADED FILES**

- 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.)
- d. See the [Link-Live](#) chapter for more information on using Link-Live with your CyberScope.

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 [Sharing procedure](#) to share the image using Link-Live, Bluetooth, or another configured application.

Changing the Device Language

The CyberScope supports Chinese, English, German, Japanese, and Korean 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 CyberScope displays the chosen languages, as available, in the priority order shown on the Language preferences screen.



NOTE: This user guide supports Chinese and English. If you choose German, Japanese, or Korean 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/>

CyberScope Settings and Tools

The CyberScope 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 CyberScope*.


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

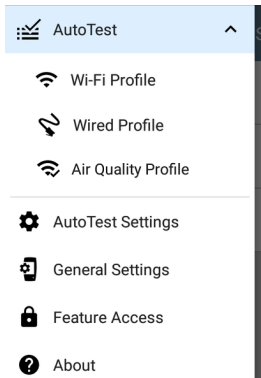
Access common settings and informational screens for the NetAlly testing apps (like AutoTest or Capture) by opening the left-side Navigation Drawers  or Settings .

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

**About**

CyberScope Analyzer

Model: CYBERSCOPE-CE

Serial: 2314182ES3CE

MAC Addresses

Wired: 00c017-570048

Wired Management: 00c017-570049

Wi-Fi: 00c017-57004a

Wi-Fi Management: 00c017-57004b

System Version: 2.5.0.102

AllyCare: Enabled

Expires: 4/6/2024

SFP Details

Type: 1000BASE-SX (850 nm)

Vendor: AVAGO

Version: --

Model: AFBR-57M5APZ

Rx Power: --

[EXPORT LOGS](#)

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


You can enable a **User-Defined MAC** in the application [General Settings](#), in the [Wired](#) profile settings, or in the [Wi-Fi](#) profile settings. (**User-defined**) then appears next to the MAC address on the About screen and in relevant test screens.

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](#).)

Import/Export for All Apps

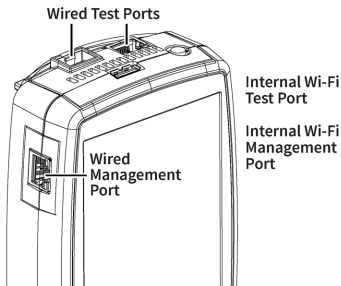
Tap the action overflow icon  on the About Screen to display a menu for importing or exporting of settings for *all* applications that allow import/export. See [Import/Export Settings](#) for details.

Restarting the Test Unit

To restart your test unit, tap the action overflow icon  on the About Screen and select the **Restart Tester** option.) (This functions the same as holding down the power button and then tapping the **Restart Tester** option.)

Test and Management Ports

The CyberScope 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.



Either the top copper port or fiber port can act as the Wired Test Port, so in total, the CyberScope 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](#) below for more information.

See the sections below for more information on the ports. Also see [Buttons and Ports](#) and the technical [Specifications](#) as 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.



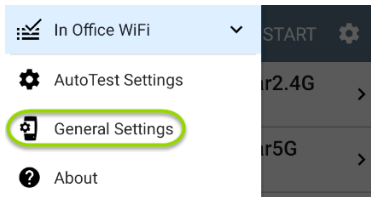
Wi-Fi Test Port: The internal Wi-Fi test adapter is a 4x4 Dual-band 802.11ac wireless radio. To disable, see [General Settings](#) in the testing apps' left-side [navigation drawer](#).

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

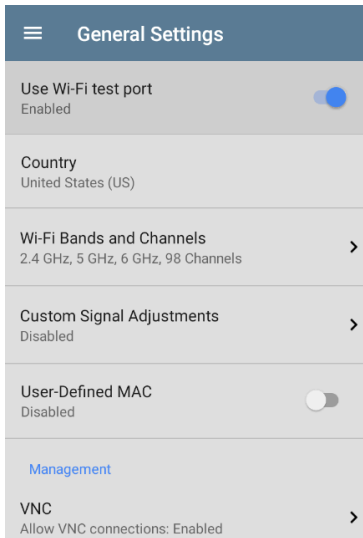
CyberScope runs Wired and Wi-Fi AutoTests, Captures, Discovery, and other comprehensive network analysis apps over the test ports. The Wi-Fi test radio is primarily controlled by the settings in applications, especially AutoTest.

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 CyberScope 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](#) to configure this connection.

The Wi-Fi management radio is set up by the system network settings. The radio provides full Internet access and a more stable network

connection than the Test Ports, which may frequently drop links and reconnect or resume scanning.

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


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

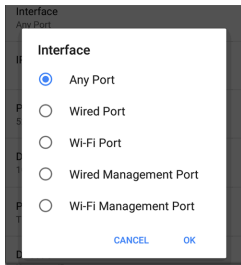
Selecting Ports

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

- 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 from a dialog.




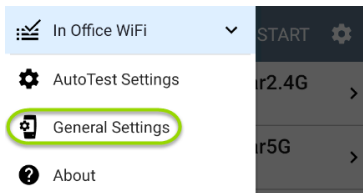
- The top two Wired and Wi-Fi Ports refer to the Test ports.
- An AutoTest [Wired](#) or [Wi-Fi Profile](#) must run to establish test port links.

- The last listed [Wired Profile](#) runs automatically when you start up the CyberScope if a connection is available.

CyberScope General Settings

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

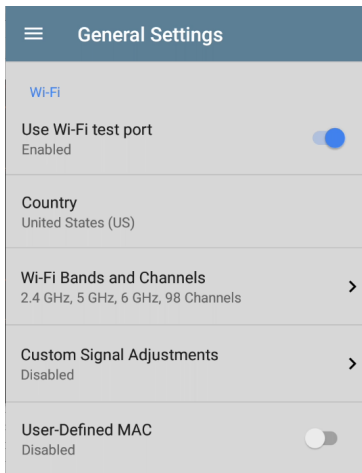
Access the General Settings from the [left-side navigation drawer](#)  in the NetAlly testing apps, such as AutoTest, Discovery, Capture, iPerf, etc.



See also [Test and Management Ports](#) and [Test and Port Status Notifications](#) for related information on port functionality and status icons.

6 **Wi-Fi General Settings** 1

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.

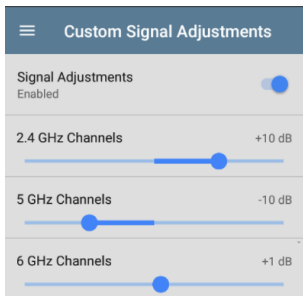
Tap each band or channel setting to open a selection dialog.

- 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 CyberScope stays on each channel to gather data.

Wi-Fi Bands and Channels	
Wi-Fi Band(s)	2.4 GHz, 5 GHz, 6 GHz
2.4 GHz Channels	All
5 GHz Channels	All
6 GHz Channels	All
Dwell Time	210 ms

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.



User-Defined MAC: This setting affects the [Wi-Fi Test Port](#) only.

1. Tap the toggle field to enable a user-defined MAC for the CyberScope. This displays the current user-defined MAC definition. (If you have not previously provided a definition, the field shows the factory default

MAC address.)



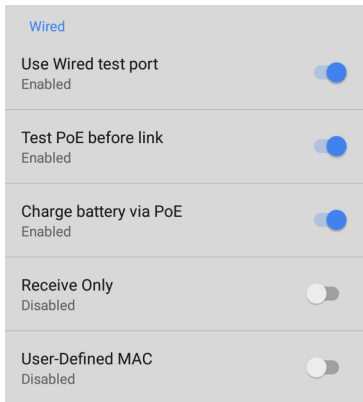
2. To enter a new definition, tap the User-Defined MAC definition field, enter a new definition, and then tap **OK**. When enabled, **(User-defined)** appears next to the MAC address on the [About](#) screen and on relevant test result screens.

NOTE: This definition can be overridden by a profile-based user-defined MAC. See [Wi-Fi Profile Settings](#) for more information.



Wired General Settings

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 CyberScope 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 CyberScope 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: Enable this setting to prevent the CyberScope 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.

1. Tap the toggle field to enable a user-defined MAC for the CyberScope. This displays the current user-defined MAC definition. (If you have not previously provided a definition, the field shows the factory default MAC address.)



2. To enter a new definition, tap the User-Defined MAC definition field, enter a new definition, and then tap **OK**. When 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](#) for more information.



Management

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

Management

VNC >
Allow VNC connections: Enabled

Link-Live Remote
Enabled

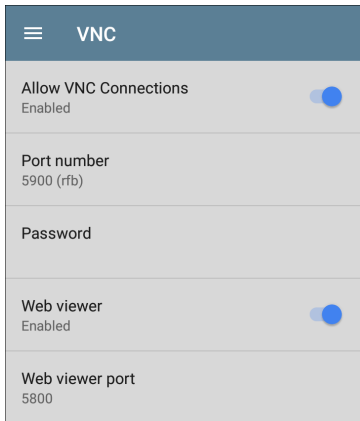
Wired Management Port >
DHCP: Enabled



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 CyberScope 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 CyberScope'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 CyberScope 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 CyberScope.



Wired Management Port

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

Preferences

Preferences

Distance Unit

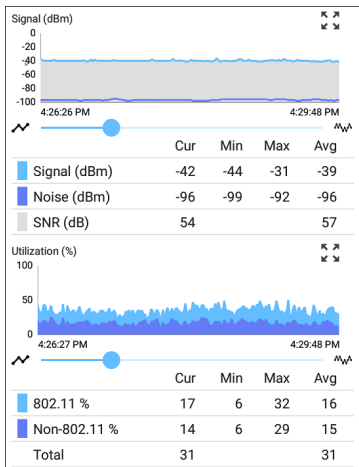
Feet

Distance Unit: This is the unit CyberScope 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 saving files. (The default is to give you the option to save to [Link-Live](#) or locally.)

Trending Graphs

Many of the CyberScope 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](#).

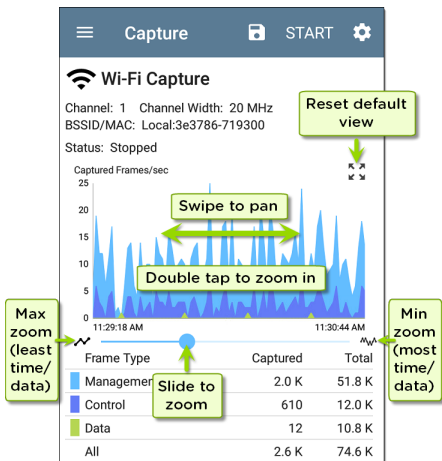



d

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



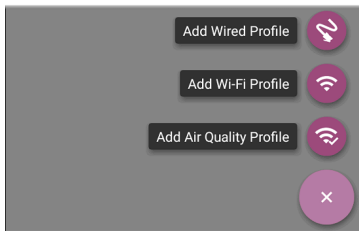
Directional Arrows (or Carets) - indicate the ability to "drill in," open a screen, or expand a panel for more detailed information, or to change the order of a list

For explanations of the CyberScope 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.


☰ **Discovery**

GS510TP - Office Switch **Path Analysis** 


Switch

Name **Ping/TCP** **PING TCP**
SNMP: GS510TP - Office Switch


Address **TCP Port Scan** 
IPv4: 192.168.1.5 (Reachable)
MAC: Netgear:2cb05d-9cab7e

Capture (Wired) 


Attributes: Discovered via SNMP, Transparent Switch


VLANs **Browse** 

1, 2, 3, 10


Interfaces **Add Test Target** 

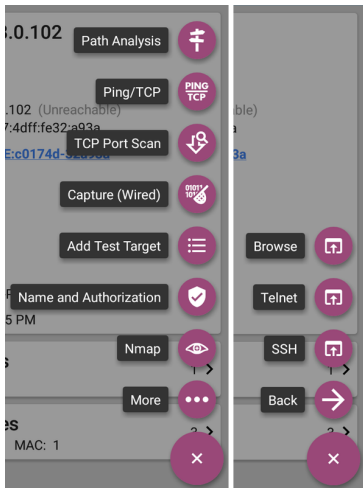
Up: 7 Down: 8 15 >

Name and Authorization 

MIB **SNMP** **More** 

Uptime: 1 week 6 days 9 hours 16 min






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. CyberScope has the Chromium browser pre-installed.

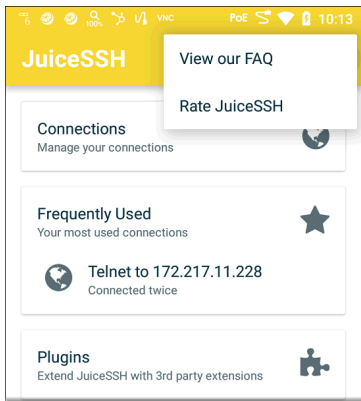
Telnet/SSH

The JuiceSSH  application pre-installed. Both the AutoTest and Discovery apps provide links 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](#).

Flashlight

The flashlight is located on the back of the unit. (See [Buttons and Ports](#).)

Access the Flashlight feature from the [Quick Settings Panel](#) by swiping down twice from the top of the screen.

Software Management

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

Tap a link below to skip to a topic:

[Managing Files](#)

[Updating Software](#)

[Remote Access](#)

[Resetting App Defaults](#)


[Restoring Factory Defaults](#)


Managing Files

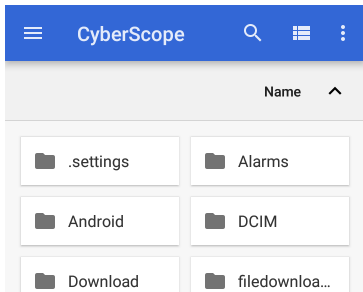
The CyberScope operating system, images, documents, and other files reside in a folder system, where you can copy, move, and paste them between folders or to external storage locations.


See also [Sharing](#).

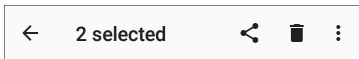
Files Application


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

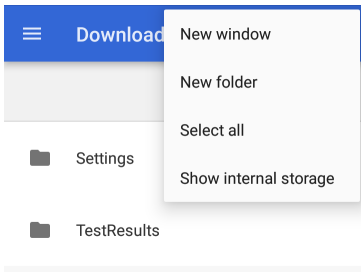
NOTE: To select the device sub-folders in the Files app as shown below, you may need to open the [navigation drawer](#) by swiping from the left side of the screen or by tapping the navigation icon  at the top left and then tapping the **CyberScope** folder.




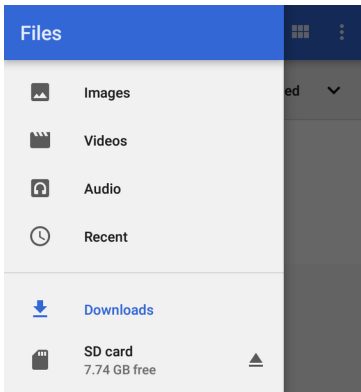
- Tap a folder or file to open it.
- **Long press** on folders or files to select multiple and to view additional file management operations in the top toolbar, including the **Share**  and Delete buttons.



- 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.



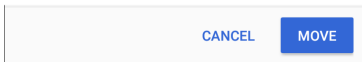
How to Move or Copy a File

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 CyberScope. See [Inserting a Micro SD card](#).

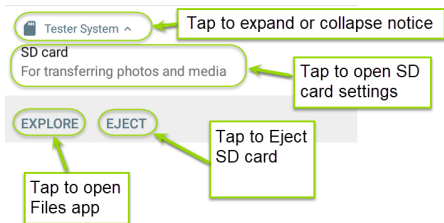
A Micro SD card icon  appears in the Status Bar at the top of the screen. Pull down the top [Notification Panel](#) to reveal the SD card notification.


 Tester System ▾

SD card

For transferring photos and media

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




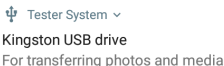
The **SD card** storage location is also available from the [Files](#)  application.

⚠ 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.

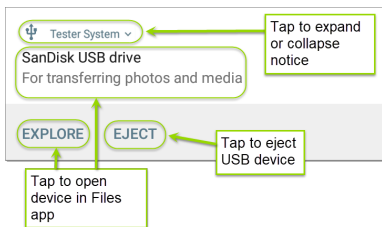
Using a USB Drive


Insert a USB flash drive into the [USB port](#) on the top of the CyberScope.

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:



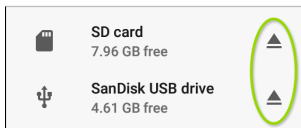
The **USB storage** location is now available from the **Files**  application.

⚠ 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.

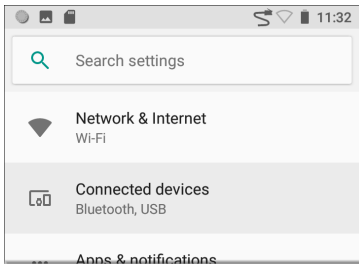
Ejecting Storage Media

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).

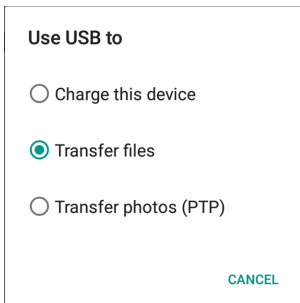


Using a USB Type-C to USB Cable

1. Plug a USB-C cable into the [USB-C](#) port on the left side of the CyberScope, and connect to a PC or tablet.
2. On the CyberScope 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: CyberScope does not charge through a USB cable connected to a PC.

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


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

Updating Software

Your CyberScope 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 CyberScope unit at [Link-Live.com](https://link-live.com). Then your CyberScope can find and download software updates. See [Getting Started in Link-Live](#).

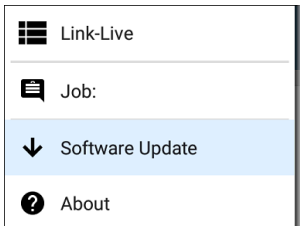
The first time you claim your CyberScope to Link-Live, a software update may be available. If so, an update icon  appears in the Status Bar. Slide down the [Top Notification Panel](#), and then select the notification to update your unit.

 Link-Live

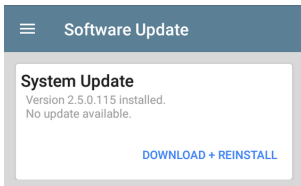
Software Update Notification

Software update available.

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 get 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. The file name is in the format: **<product name abbreviation>-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 or a FAT32-formatted Type A **USB drive**, and then insert the card or drive into your CyberScope.
2. Power off your CyberScope 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** or **apply update from USB drive**.
5. Press the **Power** button to confirm the selection.
6. Use the volume buttons to highlight the correct update file on the Micro SD card or USB drive.
7. Press the **Power** button to confirm. The CyberScope 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.' or 'Install from USB drive completed with status 0.' should show on the install line.
8. Use the volume keys and **Power** button to select **reboot system now**. Your unit should boot normally.

Remote Access

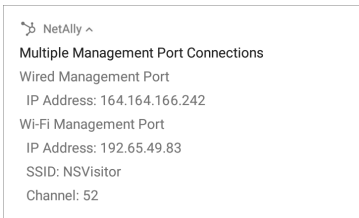
CyberScope supports remote access and control using either a standalone VNC client or the Link-Live Remote feature, which uses a VNC client through the Link-Live website.

NOTE: The Link-Live Remote feature is only available to customers with an active **AllyCare** subscription. Your CyberScope 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](#).

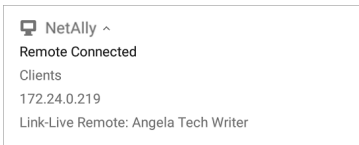
The top [notifications](#) are the quickest way to find assigned IP addresses for your CyberScope ports. Swipe down from the [Status Bar](#) to view them.



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 CyberScope using a peer-to-peer VNC client installed on a PC or other machine.

See [General Settings > VNC](#) to enable and configure VNC connections.

NOTE: By default, VNC is disabled for CyberScope. See [General Settings > VNC](#) to enable and configure VNC connections.

To connect to CyberScope 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 CyberScope.

On your CyberScope, 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](https://link-live.com) to access the Link-Live Remote feature. Your CyberScope must be [claimed](#).
2. Navigate to the **Units**  page at Link-Live.com.
3. Select the CyberScope 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 CyberScope interface.

5. If necessary, at the top of the window, enter the Password set in **General Settings > Management > VNC** on the CyberScope unit.

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


Managing NetAlly App Settings

This topic explains how to reset, [load](#), [save](#), [import](#), and [export](#) the test settings for NetAlly testing apps.

For instructions on restoring factory defaults to the entire test unit, see [Restoring CyberScope Factory Defaults](#).

Resetting Testing App Defaults

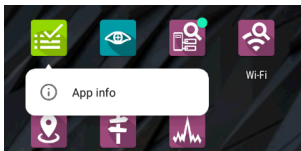
After you adjust settings in the NetAlly apps, you may need to reset an app's settings to the defaults. The following process resets all app-specific settings to the factory defaults.

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

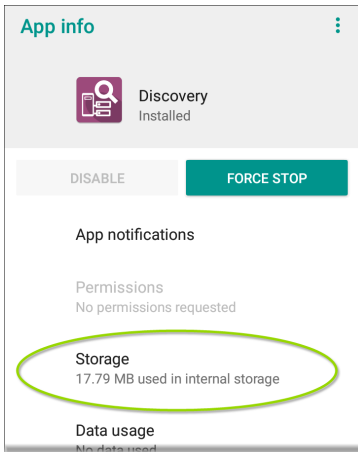
The Discovery app is used as an example in the following steps:


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

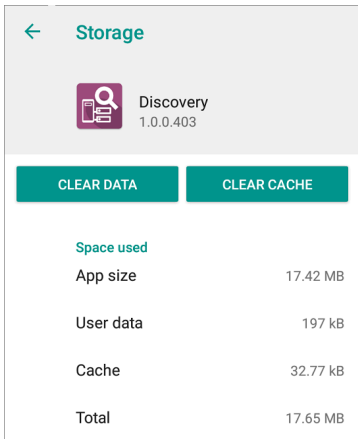
Home or Apps screen.




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**.



← Storage

 Discovery
1.0.0.403

CLEAR DATA CLEAR CACHE


Space used

App size	17.42 MB
User data	197 kB
Cache	32.77 kB
Total	17.65 MB

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

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

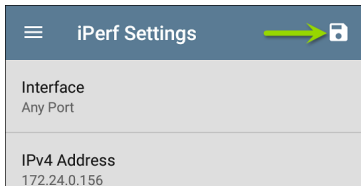
Saving App Settings and Configurations

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.

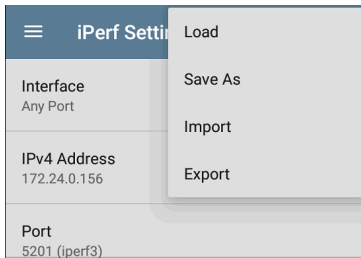
The following apps allow you to save and load settings configurations:

- [AutoTest, including Profile Groups](#)
- [Discovery](#)
- [Discovery Problem Settings](#)
- [Nmap](#)
- [Performance](#)
- [iPerf](#)
- [Spectrum](#)

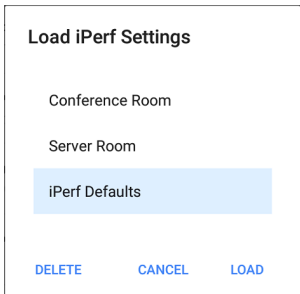
The iPerf app is shown below as an example.



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.

Save iPerf Settings

Conference Room

Server Room

iPerf Defaults


Server Room



CANCEL SAVE

- **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/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.

Import/Export Settings

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

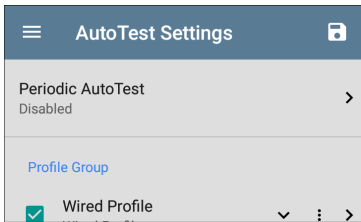
NOTE: You can import and export settings only between the same kind of NetAlly products. For example, both units must be CyberScopes for a transfer to work.


The exception to this rule is that you can export Nmap tests or settings to Link-Live and then push the them to either CyberScope or CyberScope Air units.

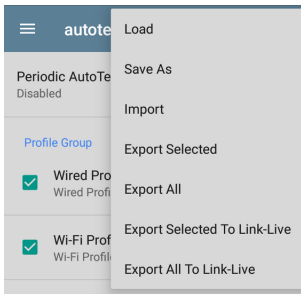
The following apps enable you to import and export settings and configurations:

- [AutoTest Settings, including Profile Groups](#)
- [Discovery Settings](#)
- [Discovery > Problem Settings](#)
- [Nmap Settings](#)
- [Performance Settings](#)
- [iPerf Settings](#)

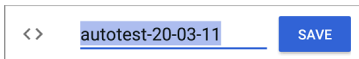
The AutoTest Settings are shown as an example in the images below.



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

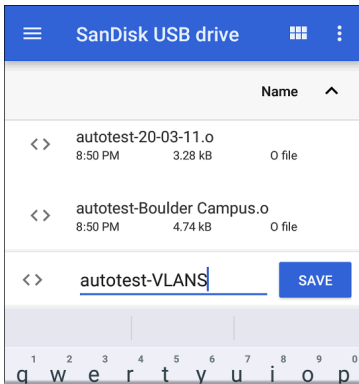


- Selected (checked) items in shared lists of configurations are the only ones exported when you choose **Export Selected**. This can include any checked items in submenus (such as AutoTest Test Targets or Community Strings in [Discovery Settings](#)). You can also select **Export All** to export all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

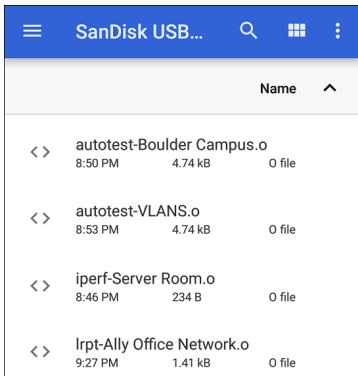


The image shows a screenshot of a configuration name field. On the left, there are angle brackets '< >'. To their right is a text input field containing the text 'autotest-20-03-11'. The text is highlighted with a blue selection bar. To the right of the input field is a blue button with the word 'SAVE' in white capital letters.

- 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.



SanDisk USB...			
Name ^			
<>	autotest-Boulder Campus.o	8:50 PM	4.74 kB
			0 file
<>	autotest-VLANS.o	8:53 PM	4.74 kB
			0 file
<>	iperf-Server Room.o	8:46 PM	234 B
			0 file
<>	lrpt-Ally Office Network.o	9:27 PM	1.41 kB
			0 file

- 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

CyberScope 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.

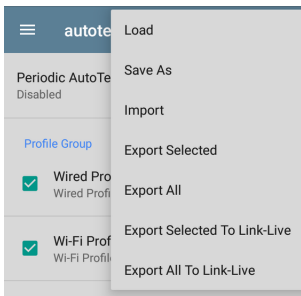
Before You Begin

- 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 CyberScope 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](#) 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.

**Link-Live**
by NetAlly

Settings File Name


autotest-shared settings

Comment

Update for all units

Job Comment


New profiles

 **EXPORT TO 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. Tap the main menu icon .
3. Click on **Settings** to open the settings menu.
4. Select **CyberScope** 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.
-

 AutoTest

New settings from Link-Live
autotest-autotest trial.o

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.

Import/Export Settings for All Apps

Your CyberScope 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 CyberScopes for a transfer to work.


To perform a group export or import:

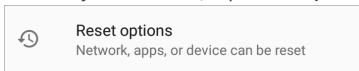
1. Open the About Screen by tapping the navigation menu icon  in any NetAlly application and then tapping **About**.
2. Tap the action overflow icon  to display the export or import menu.
3. To import settings:

- a. Tap **Import CyberScope 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 **Import CyberScope 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 CyberScope 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 CyberScope 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 again before resetting. If so, tap the final confirmation button to reset your CyberScope'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.)

CyberScope Feature Access

This chapter explains how to semi-permanently and permanently control the availability of features on your CyberScope.

Tap a link below to skip to your desired topic:

[Introduction to CyberScope](#)

[Controlling Feature Availability](#)

[Permanently Disabling Features](#)

[Changing the Admin Password](#)

Introduction to Feature Access

The CyberScope provides the ability to semi-permanently and permanently disable certain features to meet a variety of security needs. These features are referred to as controlled features.

Controlled features have categories to help you identify which features can be disabled.

Removable Storage

- USB Access
- Micro SD Access

Connectivity Apps

- Browser App
- Telnet/SSH App

Remote Control

- VNC

Wireless

- Management Wi-Fi
- Bluetooth

Documenting

- Nmap
- Packet Capture
- Network Discovery
- Camera
- Microphone

Link-Live Cloud Service

- Link-Live Access
- Download from App Store

Removable Storage

USB Access

Both the USB Type-A port on the top of the unit and the Type-C port on the left side of the unit are deactivated when the USB Access feature is disabled. This means that there can be no data transfer in either direction via these ports and that external devices cannot receive power from these ports.

NOTE: The USB Type-C port continues to function to support powering the unit using the AC adapter.

Micro SD Access

The Micro SD card slot on the left side of the unit is deactivated when the Micro SD Access feature is disabled. The operating system no longer recognizes an inserted Micro SD card and no data transfer in either direction is possible.

NOTE: The Micro SD card slot is temporarily re-activated for recovery mode operation. See [Manual Updates](#) for a description of updating the software using recovery mode.

Connectivity Apps

Browser App

The Chromium browser is removed if you disable the Browser App feature. All NetAlly apps that normally provide access to the Chromium browser remove that option. Other apps cannot access the browser.

NOTE: If you re-enable the Browser App feature, the Chromium browser, User Guide,

and Video apps are restored but do not appear on the Home screen. See [Apps](#) for more information about the Apps screen.

Telnet/SSH App

The JuiceSSH app, which provides Telnet and SSH client services, is removed when the Telnet/SSH App feature is disabled. All NetAlly apps that normally provide access to this app remove this option.

Remote Control

VNC

The ability to remotely access and control the product UI using a standalone VNC client is deactivated when the VNC feature is disabled. See [Remote Access](#) for more information about this capability.

NOTE: The Link-Live Remote feature remains active when VNC is disabled. To deactivate Link-Live Remote, Link-Live Access must be disabled.

Wireless

Management Wi-Fi

The internal Wi-Fi Management Port, which runs on the main system's 1x1 Dual-band 802.11ac + Bluetooth 5.0 wireless adapter and external Wi-Fi adapters, is deactivated when the Management Wi-Fi feature is disabled. All NetAlly apps that normally provide access to the Wi-Fi management port will remove access to the port.

NOTE: See [Test and Management Ports](#) for more information.

Bluetooth

The internal Bluetooth Port, which runs on the main system's 1x1 Dual-band 802.11ac + Bluetooth 5.0 wireless adapter, is deactivated when the Bluetooth feature is disabled. Peripheral access and data transfer over Bluetooth is not possible.

Documenting

Nmap

The Nmap app is disabled when the Nmap feature is disabled. All NetAlly apps that normally provide access to the Nmap app will remove this option.

NOTE: See [Nmap](#) for more information.

Packet Capture

The Capture app is disabled when the Packet Capture feature is disabled. All NetAlly apps that normally provide access to the Capture app will remove this option.

NOTE: See [Capture](#) for more information.

Network Discovery

The Upload to Link-Live or Save Locally function in the Discovery and Wi-Fi apps are disabled.

NOTE: See [Discovery](#) for more information.

Camera

The built-in camera on your unit is deactivated when the Camera feature is disabled.

NOTE: To provide additional security control, your CyberScope ships with a decal that you can use to cover the camera lens.

Microphone

The built-in microphone on your unit is deactivated when the Microphone feature is disabled.

Link-Live Cloud Service

Link-Live Access

The [Link-Live](#) app is disabled when the Link-Live Access feature is disabled. All NetAlly apps and services that provide an interface to Link-Live will remove access.

NOTE: The Link-Live Remote feature and the App Store app are also disabled when Link-Live Access is disabled.

Download from App Store

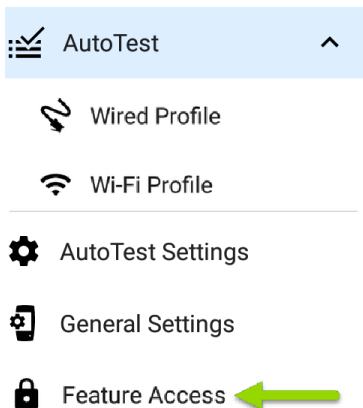
The App Store app is disabled when the Download from App Store feature is disabled. Adding additional apps to the product is not possible.

NOTE: Disabling Link-Live Access also disables the App Store app.


Controlling Feature Access


The CyberScope supports disabling (and re-enabling) certain features to meet a variety of security needs. These features are referred to as controlled features.

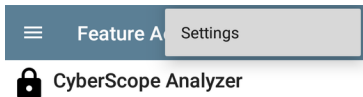
Use the **Feature Access** selection to manage feature access. It is accessible from the left-side [navigation drawer](#) in NetAlly apps, such as AutoTest and Ping/TCP.



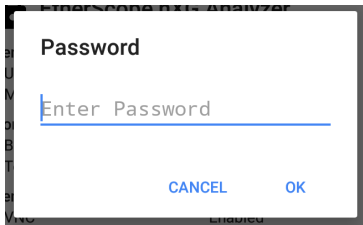
Select **Feature Access** to view the **Feature Access** status screen. This screen shows the current state of the controlled features.

Feature Access	
 CyberScope Analyzer	
Removable Storage	
USB Access	Enabled
MicroSD Access	Enabled
Connectivity Apps	
Browser App	Enabled
Telnet/SSH App	Enabled
Remote Control	
VNC	Enabled
Wireless	
Management Wi-Fi	Enabled
Bluetooth	Enabled
Test Wi-Fi	Enabled
Documenting	
Nmap	Enabled
Packet Capture	Enabled
Network Discovery	Enabled
Camera	Enabled
Microphone	Enabled
Link-Live Cloud Service	
Link-Live Access	Enabled
Download from App Store	Enabled

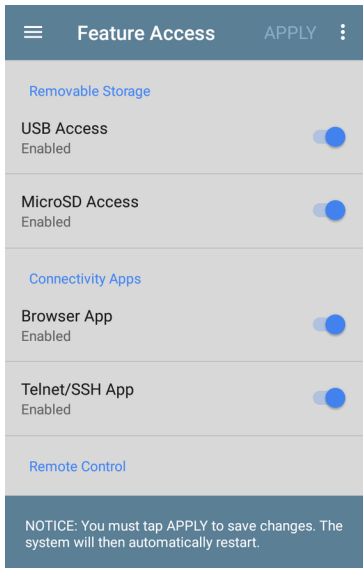
To change access to a controlled feature, tap the action overflow icon , and then tap the **Settings** option.



When prompted, enter the admin password, and then tap the **OK** button.



The **Feature Access** screen shows the current state of the controlled features and lets you turn features off or on using the toggle. Note that the state of **permanently disabled controlled features** cannot be changed.



Feature Access

APPLY

Removable Storage

USB Access
Enabled

MicroSD Access
Enabled

Connectivity Apps

Browser App
Enabled

Telnet/SSH App
Enabled

Remote Control

NOTICE: You must tap APPLY to save changes. The system will then automatically restart.

If you make changes, the **Apply** button at the top of the screen becomes active.

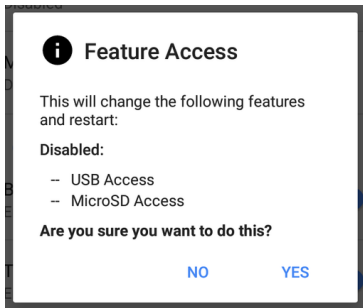


Feature Access

APPLY

Tap **Apply** as the first step in completing the changes.

A message lists the pending feature changes.



- Select **Yes** to make the pending changes
- Select **No** to cancel the pending changes and return to the Settings screen

After the changes are applied, the unit automatically restarts.

To view the state of the controlled features, visit the **Feature Access** status screen.



Feature Access



CyberScope Analyzer

Removable Storage

USB Access	Disabled
------------	----------

Connectivity Apps

Browser App	Disabled
-------------	----------

Telnet/SSH App	Disabled
----------------	----------

Remote Control

VNC	Disabled
-----	----------

Wireless

Management Wi-Fi	Enabled
------------------	---------

Bluetooth	Enabled
-----------	---------

Documenting

Nmap	Disabled
------	----------

Packet Capture	Enabled
----------------	---------

Network Discovery	Enabled
-------------------	---------

Link-Live Cloud Service

Link-Live Access	Enabled
------------------	---------

Download from App Store	Enabled
-------------------------	---------

Permanently Disabling Features

The CyberScope supports permanently disabling controlled features to meet a variety of security needs.


When controlled features are permanently disabled, internal hardware modifications are made that prevent the disabled controlled features from operating. Please note that NetAlly does not accept product return requests from customers who want to re-enable permanently disabled controlled features.

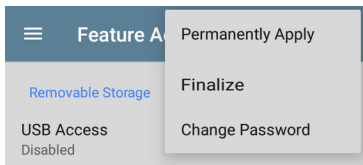
CAUTION:

- **NetAlly does not accept product return requests from customers who want to re-enable permanently disabled controlled features.**
- **NetAlly does not accept product return requests from customers who want to make controlled feature changes after the changes to the unit have been finalized.**

In addition, the product supports finalizing the state of controlled features. When controlled features are finalized, hardware modifications are made that prevent any future changes to the state of the controlled features.

To permanently disable controlled features, follow the instructions in [Controlling Feature Availability](#) to select the features you want to permanently disable or to finalize.

After selecting features on the Settings screen, tap the action overflow icon  at the top of the screen.



Select one of the following options:

- **Permanently Apply**
- **Finalize**

NOTE: the **Finalize** option only becomes active when at least one controlled feature has been permanently disabled and there are no semi-permanently disabled controlled features.

If you select **Permanently Apply**, a message identifies the pending actions:

Warning

This will permanently disable the following features and restart:

- USB Access
- MicroSD Access
- Link-Live Access
- Download from App Store

I agree selecting Change Permanently will irreversibly disable these features.

CANCEL **CHANGE PERMANENTLY**

Select one of the following options:

- **CHANGE PERMANENTLY** to *irreversibly* apply the pending changes
Note that these changes are *permanent* and cannot be undone.

- **CANCEL** discards the pending changes and returns to the Settings screen

After the changes are applied, the unit automatically restarts.

If the **Finalize** option is selected, a message identifies the pending actions:

Warning

This will permanently disable the following features and restart:

- USB Access
- MicroSD Access
- Link-Live Access
- Download from App Store

No additional changes will be possible.

I agree selecting Change Permanently will irreversibly disable these features and disable future changes.

CANCEL **CHANGE PERMANENTLY**

Select one of the following options:

- **CHANGE PERMANENTLY** to *irreversibly* apply the pending changes. Note that these changes are *permanent* and cannot be undone. In addition, the state of all the controlled features is *permanently locked*.
- **CANCEL** to discard the pending changes and return to the Settings screen

After the changes are applied, the unit automatically restarts.

To view the new status of the controlled features, visit the Feature Access Status screen. (This example assumes the Browser App and Telnet/SSH App were previously disabled but not permanently disabled.)



Feature Access

**CyberScope Analyzer****Removable Storage**

USB Access Permanently Disabled

MicroSD Access Permanently Disabled

Connectivity Apps

Browser App Disabled

Telnet/SSH App Disabled

Remote Control

VNC Enabled

Wireless

Management Wi-Fi Enabled

Bluetooth Enabled

Test Wi-Fi Enabled

Documenting

Nmap Enabled

Packet Capture Enabled

Network Discovery Enabled

Camera Enabled

Microphone Enabled

Link-Live Cloud Service


Link-Live Access Permanently Disabled

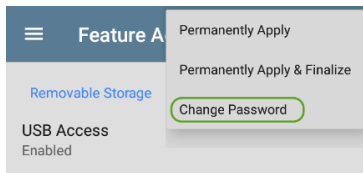
Download from App Store Permanently Disabled

Changing the Administrative Password

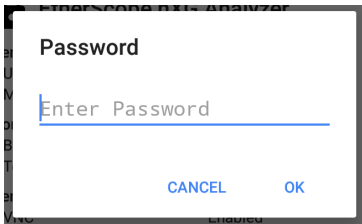
NetAlly recommends that you change the factory-set admin password when you configure **Feature Access** to prevent non-administrative users from gaining access to the **Feature Access** screen.

To change the admin password:

1. Follow the procedure in [Controlling Feature Availability](#) to access the **Feature Access** selection screen.
2. From the selection screen, tap the action overflow icon  at the top of the screen to display the overflow menu.



3. Select **Change Password** to display the Current Password entry screen.



4. Enter the current admin password and tap **OK** to continue. (Select **CANCEL** to return to the **Feature Access** selection screen without making any changes.)

Note: The factory-set administrative password is: **admin**

5. Wait for the New Password entry screen to display, enter the new password in both fields, and then tap **OK** to complete the admin password change. (Select **CANCEL** to return to the **Feature Access** selection screen without changing the current admin

password.)

Note that you cannot complete the admin password change until the new password fields contain matching entries.

New Password

Enter new password

Confirm new password

CANCEL **OK**



CyberScope 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 CyberScope. 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 CyberScope.

AutoTest Chapter Contents

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

[AutoTest Overview](#)

[Managing Profiles and Profile Groups](#)

[Main AutoTest Screen](#)

[Periodic AutoTest](#)

[Wired AutoTest Profiles](#)

[Wi-Fi AutoTest Profiles](#)

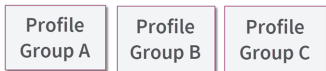
[DHCP, DNS, and Gateway Tests](#)

[Test Targets](#)

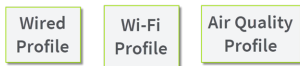
AutoTest Overview

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.

Profile Groups



Profiles



Test Targets



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.

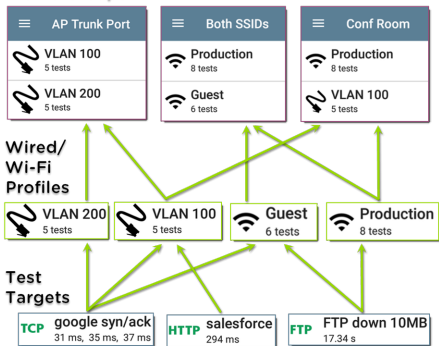
A Test Target can be in any number of Profiles, and a Profile can be in any number of Profile Groups.

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.

Profile Groups



Managing Profiles and Profile Groups

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

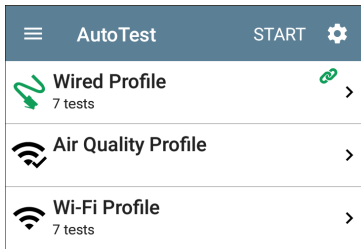
Wired Profiles to test copper and fiber connections.


Wi-Fi Profiles to test wireless connections.

Air Quality Profiles to measure channel utilization and interference.

Factory Default Profiles

The CyberScope 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.

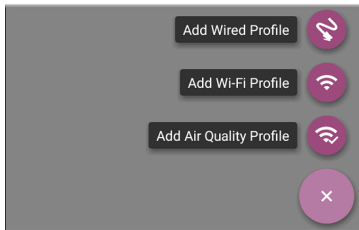
- The default **Air Quality Profile** runs when you tap **START** on the main AutoTest screen or the Air Quality screen.
- For the default **Wi-Fi Profile** to run successfully, you must select an SSID and enter security credentials before the CyberScope can connect to a network.




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.





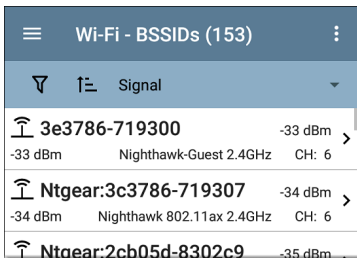
The profile's configuration screen appears after you select the type of profile you want to add. See the topic for each profile type for a description of its settings.


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.

1. Open the **Wi-Fi app**  from the Home screen.
2. Tap the menu button  to select the **SSIDs or BSSIDs** list screen.



3. Tap an SSID or BSSID's card to open its Details screen.
4. Tap the FAB (floating action button)  to open the floating action menu.

Wi-Fi - BSSID

 **Ntgear:3c3786-719307**
BSSID

SSID: **Nighthawk 802.11ax**

AP: **192.168.1.1**

BSSID: 3c3786-719307

802.11

Channel: 1


Types: ax, n, g, b


Signal: -30 dBm


SNR: 64 dB



Security Type: WPA2-E



Last Seen: 11:38:24 PM

Locate 

Connect 

↑↓ Rates and Capabilities 

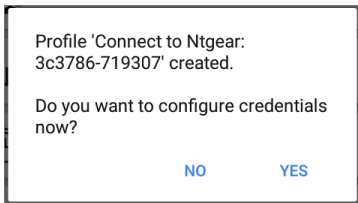
 Clients 

 RF and Traffic Statistics 

CH: 1 Utilization: 7%

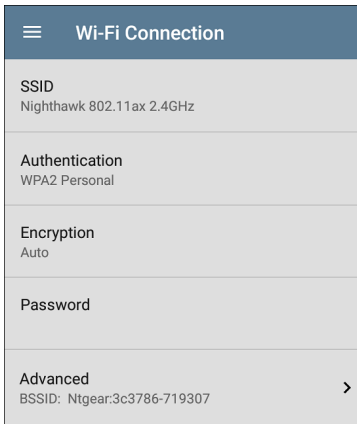
5. In the floating action menu, tap **Connect**.


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.


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

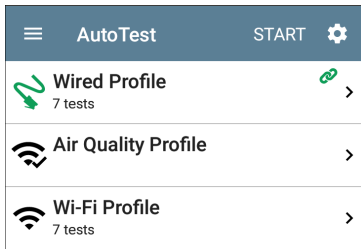


7. Enter any additional credentials, like the network Password.
8. After configuring, tap the back button  to return to and run the new Profile.

Profile Groups

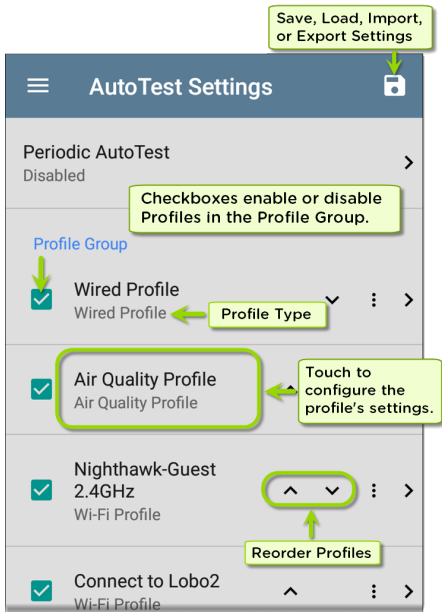
CyberScope also allows you to save Profile Groups. Profile Groups are simply **the included list of test Profiles and the order in which they run** when you start an AutoTest. (See [AutoTest Overview](#) for more explanation of Profile Groups.) You can configure and select Profiles and Profile Groups 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.

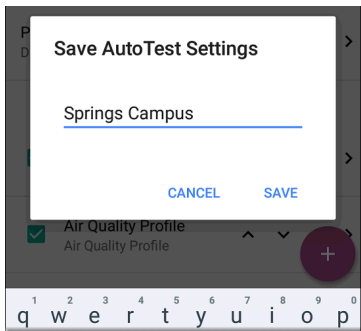
Each Profile Group can run one or many instances of the profile types. Saved Profiles are available across all of your Profile Groups.

Custom AutoTest Settings/Profile Group Names

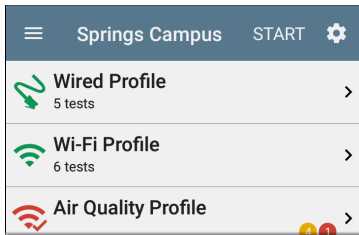
By default, the AutoTest app screen shows "AutoTest" in the header, and the AutoTest Settings screen header is "AutoTest Settings." Once you save a custom name, the name

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.




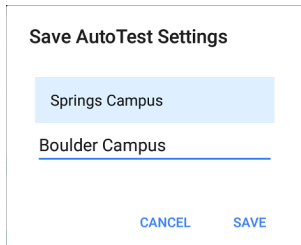
Creating New Profile Groups

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 CyberScope 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 802.11 ax 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, then scans the wireless channels for Air Quality results, and then connects to "The Office Network #1" and remains connected to that network. This Profile Group will *not* connect to or test the "Nighthawk..." or "LRC" networks.

Import/Export AutoTest Profiles

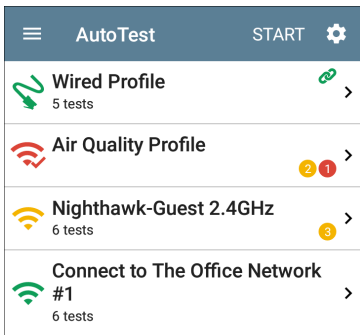
In addition to creating new profiles or using defaults, you can also:

- Import and export profile settings to any connected external or internal storage. See [Import/Export Settings](#).
- 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](#).

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 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.

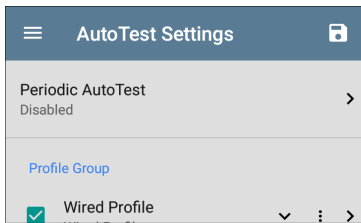
Each profile and test is summarized on a card. Tap a profile's or individual test's card to open and view test result details, including the causes of any Warnings or Failures.

Periodic AutoTest

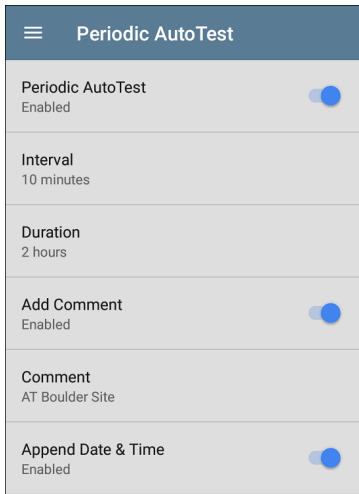
The Periodic AutoTest feature allows you to run AutoTests at set time intervals.

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 the following options:



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](https://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. AutoTest continues to run at the set Interval for the selected Duration or until you tap **STOP** in AutoTest.

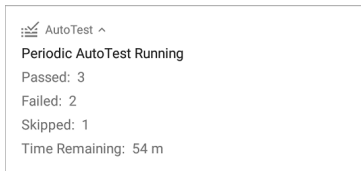
AutoTest Settings STOP

- Wired Profile**
7 tests
- Air Quality Profile**
9 1
- CiscoE4200-5G**
6 tests

Periodic AutoTest Status
Passed: 11
Failed: 25
Skipped: 3
Time Remaining: 21 m
Next: 2 s

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.

☰
AutoTest
START

Wired Profile

8 tests

50.6 V
>

Class: 3 13.0 W

100M/1G/2.5G/5G/10G
>

RJ-45 HDx/FDx

EXTREME_48
>

Port: 1/37

DHCP
10.250.3.161
>

31 ms

DNS
Compass.netally.eng
>

6 ms

COS_DEV_SW1
>

8 ms, 7 ms, 2 ms

HTTP
google
>


+

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

	Wired Profile 9 tests	
	56.23 V Class: 0 13.00 W	>
	100M/1G/2.5G/5G RJ-45 HDx/FDx	>
802.1X	PEAP MSCHAP V2 User: qatest1	>
VLAN	Untagged Top: Untagged, 508, 560, 2510, 525, 526, 1	>
	COS-DEV-SW1.NetAlly.com Port: FiveGigabitEthernet1/0/19	>


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

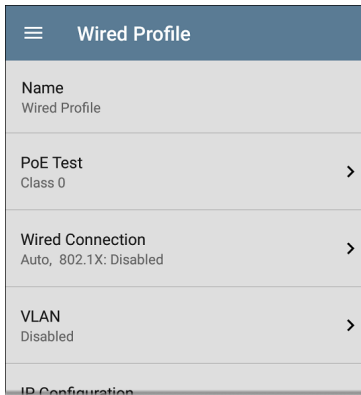
The VLAN test card appears if the **VLAN** setting is enabled or if VLAN-tagged traffic is detected during the AutoTest.


- Skip to [Wired Profile Settings](#).
- Skip to [Wired Profile Results](#).
- Skip to [DHCP, DNS, and Gateway Tests](#).
- Skip to [Test Targets](#).

Wired Profile Settings

These settings control the wired test port connection, PoE tests, 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.



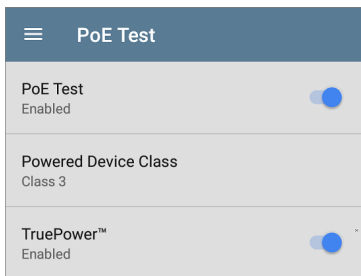
On the **Wired Profile** settings screen, tap each field described below as needed to configure the profile. Changed settings are automatically applied. When you finish configuring, tap the back button  to return to the profile.

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	
PoE Test Enabled	<input checked="" type="checkbox"/>
Powered Device Class Class 3	
TruePower™ Enabled	<input checked="" type="checkbox"/>

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.

CyberScope 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: CyberScope may not receive the total wattage advertised by your switch or injector because of power loss over the cable.

NOTE: CyberScope 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 CyberScope but LLDP is not

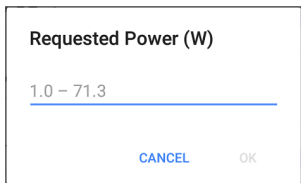
enabled on your Cisco switch, negotiation fails.

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.

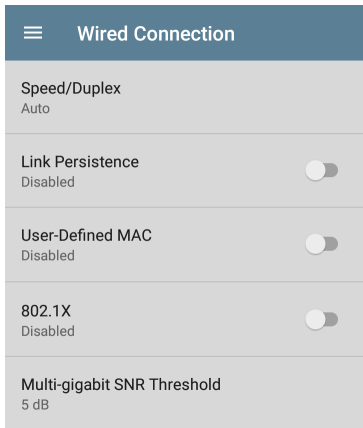
General Settings that Affect PoE

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.



Wired Connection	
Speed/Duplex Auto	
Link Persistence Disabled	<input type="checkbox"/>
User-Defined MAC Disabled	<input type="checkbox"/>
802.1X Disabled	<input type="checkbox"/>
Multi-gigabit SNR Threshold 5 dB	

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, CyberScope 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. The default setting for Link Persistence is disabled.

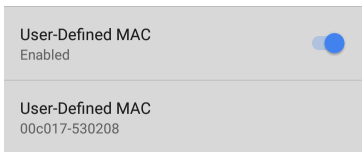
Link Persistence and Establishing Link: When enabled there is no timeout on how long to wait for link to be established. When disabled, the link step fail if not successful in 25 to 30 seconds.

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.

User-Defined MAC

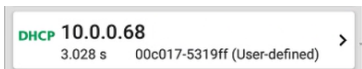
This feature can help with tasks such as testing ACL lists (for example, finding out if specific MAC addresses are allowed on the network) or determining if specific IPv4 addresses should be assigned to specific MAC addresses.

1. Tap the toggle field to enable a user-defined MAC for the CyberScope. This displays the current user-defined MAC definition. (If you have not previously provided a definition, the field shows the factory default MAC address.)



2. To enter a new definition, tap the User-Defined MAC definition field, enter a new definition, and then tap **OK**. When enabled, **(User-defined)** appears next to the MAC address on the [About](#) screen and on

relevant test result screens.



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.

802.1X Enabled	<input checked="" type="checkbox"/>
EAP Type PEAP MSCHAP V2	
Username	
Password	
Alternate ID	

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.

Wired Profile

- Wait For Network Traffic**
Enabled 
- IP Configuration**
DHCP: Enabled >
- DNS Test**
www.google.com >
- Gateway Test**
Timeout Threshold: 100 ms >
- Test Targets**
1 target(s) >
- Stop After**
All
- HTTP Proxy**
Disabled >

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, you may choose to disable this delay. The maximum time to delay is 45 seconds.

DHCP, DNS, and Gateway Settings

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, FTP, or Nmap tests to your AutoTest profile.

See [Test Targets for Wired and Wi-Fi Profiles](#).

Stop After

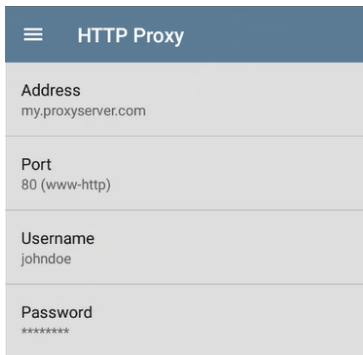
This setting directs the Wired Profile to stop testing after the selected test step (**Link, Switch, DHCP, DNS, Gateway, or All**). The excluded test cards do not appear on the Profile results screen.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the CyberScope 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.

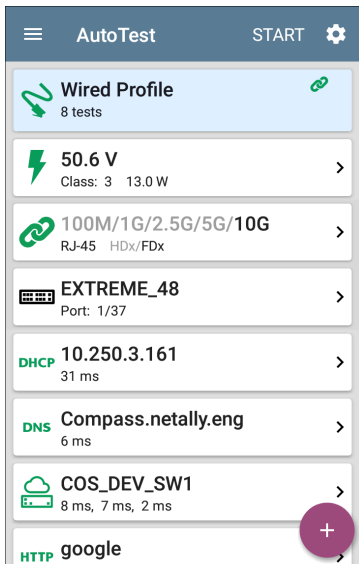


HTTP Proxy	
Address	my.proxyserver.com
Port	80 (www-http)
Username	johndoe
Password	*****

Tap each field to open a pop-up keyboard and enter the appropriate **Address** (you can enter a proxy name or an IPv4 address), **Port** (set to match the proxy port), **Username**, and **Password**. Tap **OK** to save your entries.

Wired Profile Test Results





The image below shows a completed AutoTest Wired Profile.




The screenshot displays the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" and a gear icon on the right. Below the header is a list of test results for a "Wired Profile" (8 tests). Each result is shown in a white card with a green icon on the left and a right-pointing chevron on the right. A purple circular button with a white plus sign is overlaid on the bottom right of the list.

- Wired Profile** (8 tests)
- 50.6 V** (Class: 3 13.0 W)
- 100M/1G/2.5G/5G/10G** (RJ-45 HDx/FDx)
- EXTREME_48** (Port: 1/37)
- DHCP 10.250.3.161** (31 ms)
- DNS Compass.netally.eng** (6 ms)
- COS_DEV_SW1** (8 ms, 7 ms, 2 ms)
- HTTP google**

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

A rectangular card with a light gray border. On the left side, there is a green lightning bolt icon. To its right, the text "53.1 V" is displayed in a large, bold font. Below this, the text "Class: 0 13.0 W" is shown in a smaller font. On the far right side of the card, there is a right-pointing chevron symbol (>).

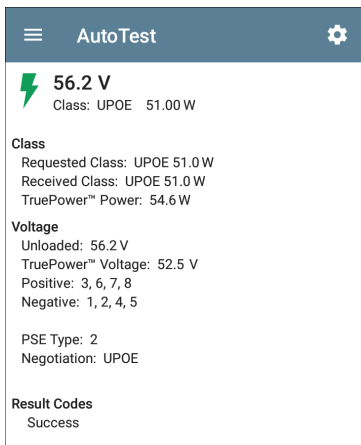
	53.1 V	>
	Class: 0 13.0 W	

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



☰ AutoTest ⚙️

 **56.2 V**
Class: UPOE 51.00 W

Class
Requested Class: UPOE 51.0 W
Received Class: UPOE 51.0 W
TruePower™ Power: 54.6 W

Voltage
Unloaded: 56.2 V
TruePower™ Voltage: 52.5 V
Positive: 3, 6, 7, 8
Negative: 1, 2, 4, 5

PSE Type: 2
Negotiation: UPOE

Result Codes
Success

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

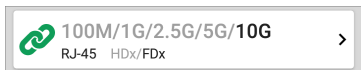
PSE Type: Switch's advertised Power Sourcing Equipment (PSE) type. Recognized types are 1 – 4, LTPoE++, Cisco UPOE, and PoE Injectors. PSE supporting UPOE are classified under Type 2. If the type cannot be determined, "1/2" is displayed.

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**.

CyberScope 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:

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

Tap the card to open the Link test screen.

Wired Link Test Screen



AutoTest



100M/1G/2.5G/5G/10G

RJ-45 FDX

Speed

Advertised Speeds: 100M/1G/2.5G/5G/10G

Actual Speed: 10G

Duplex

Advertised Duplex: FDX

Actual Duplex: FDX

RJ-45 Details

Rx Pair: All

Multi-Gigabit Details

Channel	Delay Skew	SNR	Avg SNR
A	REF	8.8 dB	8.7 dB
B	-1.25 ns	6.7 dB	6.8 dB
C	-3.75 ns	5.9 dB	5.9 dB
D	-1.25 ns	8.9 dB	8.7 dB
Threshold			1 dB

Result Codes

Success

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 CyberScope

Duplex

Advertised Duplex: Duplex capabilities reported by the switch

Actual Duplex: Duplex in use as detected by CyberScope

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)

**1G**

SFP FDx

Speed

Advertised Speeds: 1G

Actual Speed: 1G

Duplex

Advertised Duplex: FDx

Actual Duplex: FDx

SFP Details

Wavelength: 850 nm

Temperature: 42 C

Voltage: 3.29 V

Tx Bias Current: 5.99 mA

Tx Power: -4.42 dBm

Rx Power: -7.67 dBm

Reference Power: -7.67 dBm

Power Difference: 0 dB

Result Codes

Success

[SET REFERENCE](#)[CLEAR REFERENCE](#)

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. (The value 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)

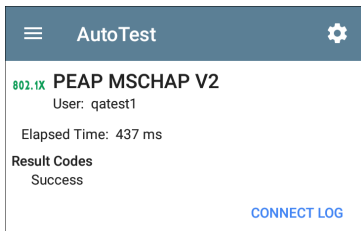
802.1X Test Results

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.

Connect Log		Save to Link-Live
3:59:45.654 PM	Supplicant: PEAP_MSCHAP_V2	
3:59:45.775 PM	Received EAP Fail	
3:59:45.777 PM	Identity: qatest1	
3:59:45.781 PM	Identity: qatest1	
3:59:45.808 PM	NAK: GOT (4) EAP-MD5 WANT (25) EAP-Peap	
3:59:45.822 PM	PEAP: Selecting Version: 0	
3:59:45.824 PM	PEAP: Received EAP Start request, sending Client Hello	
3:59:45.851 PM	PEAP: Received Server Hello	
3:59:45.923 PM	PEAP: Server Certificate unverified:	

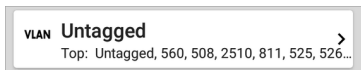
Select the action overflow icon  at the top right on the Connect Log screen to attach the log to its associated AutoTest result on the [Link-Live](#) website. You can also attach the Connect Log from the [floating action menu](#)  on the main Wired Profile screen.

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.

VLAN 508, Best Effort (0)	
Top: Untagged	

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.

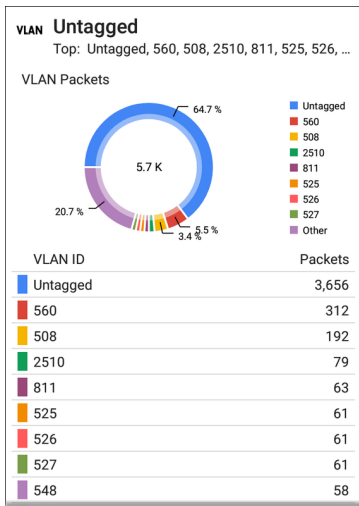


Untagged indicates that no VLAN tag is present in either received or transmitted frames, also referred to as the Native VLAN.

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



The CyberScope 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.

**COS-DEV-SW1.NetAlly.com**

Port: Fi1/0/42

Status:

Network traffic seen in 196 ms from
NetAlly:00c017-53009d

Nearest Switch: [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42

Description: Test Port

VLAN ID: 500

Voice VLAN ID: 3333

IP Address: 10.250.0.2

MAC Address: Cisco:7802b1-b0caaa

Location: COS-DEV Lab Rack S2

Contact: Erik

Model: cisco C9300-48UN

Type: CDP (First Seen)

Last Seen: 3:39:11 PM

Switch: [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42

Description: Test Port

VLAN ID: 500

IP Address: 10.250.0.2

MAC Address: Cisco:7802b1-b0ca80

Model: Cisco IOS Software [Fuji], Catalyst L3 Switch
Software (CAT9K_IOSXE), Version 16.9.3,

Type: LLDP

Last Seen: 3:39:12 PM

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 CyberScope

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 CyberScope has SNMP access to the Nearest Switch.

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

CyberScope 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 CyberScope.

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

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.

Software (CAT9K_IOSXE), Version 16.9.3,
Type: LLDP
Last Seen: 3:39:12 PM

Switch: [COS-DEV-SW1.NetAlly.com](#)

Port: Fi1/0/42
Description: Test Port
VLAN ID: 500
IP Address: 10.250.0.1
MAC Address: Cisco:00000c-07ac01
Model: CAT9K_IOSXE
Type: SNMP
Last Updated: 3:39:05 PM

[INTERFACE DETAILS](#) [BROWSE](#) ...

Switch: The Nearest Switch is listed at the top of this section. Other switches seen via advertisements or SNMP are listed below.

Additional Actions

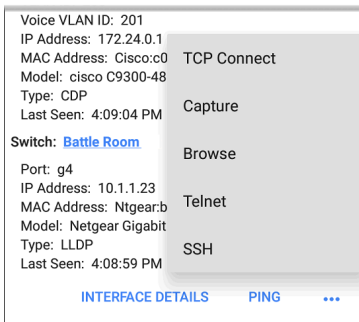
Tap the blue links at the bottom of the switch test results screen to open other apps or tools for the target.

- Tap [INTERFACE DETAILS](#) to open 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

CyberScope has current **Discovery** data, and AutoTest identified the nearest switch and connected interface.

- Tap **PING** to open the Ping test screen for the switch.
- Tap the action overflow menu icon **...** to open an additional menu:



- Tap **TCP Connect** to open the corresponding NetAlly apps, populated with the switch's address.

- Tap **Capture** to open the [Capture](#) app to run a packet capture on the target.
- Tap **Browse** to open the Chromium browser pointed to the switch IP address.
- Tap **Telnet** to open a [Telnet](#) session for the switch IP address.
- Tap **SSH** to open a [SSH](#) session for the switch 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](#)

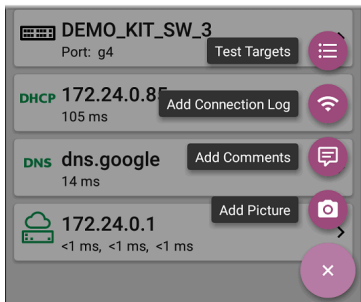
PING FTP TCP HTTP Target Tests

See the [Test Targets](#) topic for information on target test results.


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.



Connection Log Name
20191022_122355

 **SAVE TO 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.

Comment

Conference Room

Job Comment

North Office

 **SAVE TO TEST RESULT**

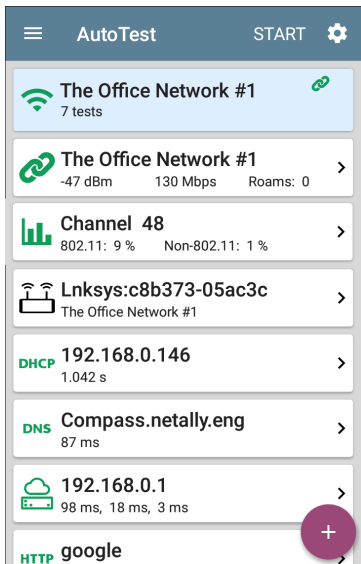
Tap the fields to enter your desired comments, and tap **SAVE TO LAST TEST RESULT** to upload them.

- 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.

Wi-Fi AutoTest Profiles

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



The screenshot shows the AutoTest app interface. At the top, there is a blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" and a gear icon on the right. Below the header is a list of items:

- The Office Network #1** (7 tests) - includes a chain link icon.
- The Office Network #1** - includes a chain link icon, signal strength (-47 dBm), speed (130 Mbps), and Roams: 0.
- Channel 48** - includes a bar chart icon, 802.11: 9 %, and Non-802.11: 1 %.
- Lnksys:c8b373-05ac3c** (The Office Network #1) - includes a Wi-Fi router icon.
- DHCP 192.168.0.146** (1.042 s)
- DNS Compass.netally.eng** (87 ms)
- 192.168.0.1** (98 ms, 18 ms, 3 ms)
- HTTP google**

Each item has a right-pointing chevron icon. A purple circular button with a white plus sign is located at the bottom right of the list.

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.

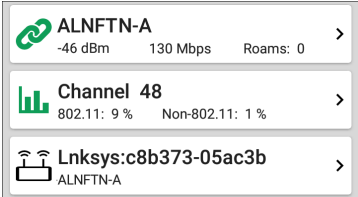
After connecting to a network during a Wi-Fi connection test, CyberScope remains connected until you run another Wi-Fi or [Air Quality](#) Profile or open the [Wi-Fi app](#). Wi-Fi Test Port linkage is

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 screenshot shows three stacked cards for Wi-Fi profile tests:

- ALNFTN-A**: Shows a green link icon, signal strength of -46 dBm, speed of 130 Mbps, and Roams: 0.
- Channel 48**: Shows a green bar chart icon, 802.11: 9 %, and Non-802.11: 1 %.
- Lnksys:c8b373-05ac3b**: Shows a Wi-Fi router icon and the profile name ALNFTN-A.


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

long as CyberScope remains connected to the wireless network.

- Skip to [Wi-Fi Profile Settings](#).
- Skip to [Wi-Fi Profile Results](#).
- Skip to [DHCP, DNS, and Gateway Tests](#).
- Skip to [Test Targets](#).

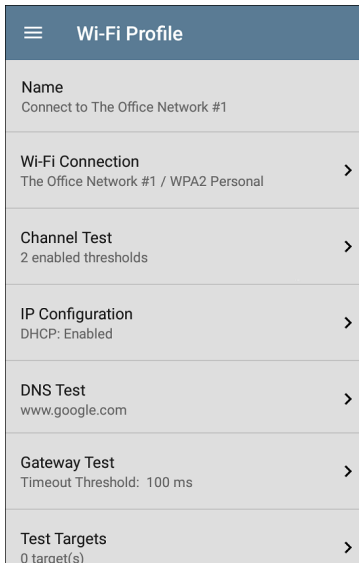
Wi-Fi Profile Settings

These settings control which network is tested, how the CyberScope 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:

- [Wi-Fi Connection Settings](#)
- [Certificates](#)
- [Advanced Wi-Fi Connection Settings](#)
- [Channel Test Settings](#)



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.

Wi-Fi Connection	
SSID	The Office Network #1
Authentication	WPA2 Personal
Encryption	Auto
Password	*****
Advanced	BSSID: Any >

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.

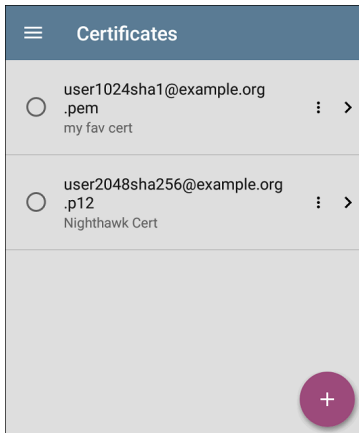
Username

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.

CyberScope 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 CyberScope supports 1-way client authentication only; mutual authentication, Server, and CA/Root certificates are not supported. While CyberScope 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:

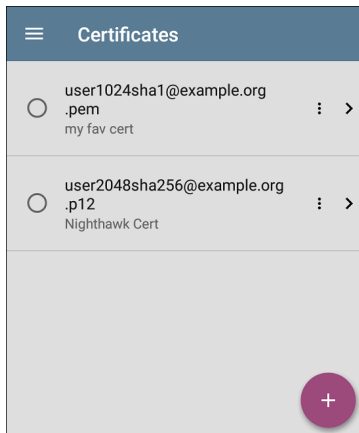
Certificate files can be imported from either an inserted storage device (USB or Micro SD) or the


CyberScope's internal file system.

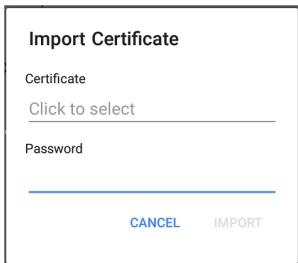
1. Make the certificate file available on your CyberScope unit by saving it to a USB drive or Micro SD card inserted into your unit or by transferring to the file system using a USB-C cable or email. (See [Managing Files](#) for help.)
2. To run an [AutoTest Wi-Fi Profile](#) using certificate authentication, 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:

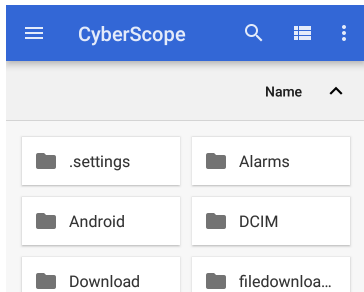
- a. 802.1X: **Enabled**
 - b. EAP Type: **EAP TLS, PEAP TLS, or TTLS EAP TLS**
3. In **AutoTest > Wi-Fi Connection** or **Wired Connection** settings, tap the **Certificate** setting to open the Certificates screen.




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.
7. Tap the menu button  to open the left-side [navigation drawer](#).
8. 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.

9. Enter the certificate's password if it is password protected.

10. Tap **IMPORT**.
11. If desired, tap the fields to edit the **Name** and **Description** of the certificate. The name defaults to the certificate file name.
12. Tap the back button  to return to the Certificates list screen. The newly added certificate appears selected in the list.
13. 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

Advanced	
BSSID	Any
Wi-Fi Band	Auto
Roam Threshold	-70 dBm
Link Test Thresholds	4 enabled thresholds >
Alternate ID	
User-Defined MAC	<input type="checkbox"/>
Disabled	

BSSID

Enter or select a specific BSSID for the Wi-Fi Profile to prevent the CyberScope 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 CyberScope stays connected and looks for another AP on the network with a stronger signal. If found, it disconnects from the current AP and connects 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.

Link Test Thresholds

Signal Level Thresholds

Enabled

Warning
-70 dBm

Failure
-85 dBm

Signal-to-Noise (SNR) Thresholds

Enabled

Warning
25 dB

Failure
10 dB

Retries Thresholds

Enabled

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

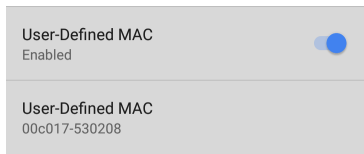
Enter an Alternate ID if necessary. This is an Advanced Authentication setting.

User-Defined MAC

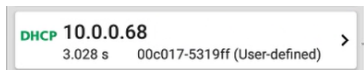
This feature can help with tasks such as testing ACL lists (for example, finding out if specific MAC addresses are allowed on the network) or determining if specific IPv4 addresses should be assigned to specific MAC addresses.

1. Tap the toggle field to enable a user-defined MAC for the CyberScope. This displays the

current user-defined MAC definition. (If you have not previously provided a definition, the field shows the factory default MAC address.)



- To enter a new definition, tap the User-Defined MAC definition, enter a new definition, and then tap **OK**. When enabled, **(User-defined)** appears next to the MAC address on the [About](#) screen and on relevant test result screens.



Channel Test Settings

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

Channel Test	
802.11 Utilization Threshold (%) Enabled	<input checked="" type="checkbox"/>
Warning 35 %	
Failure 75 %	
Non-802.11 Utilization Threshold (%) Enabled	<input checked="" type="checkbox"/>
Warning 30 %	
Failure 50 %	

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

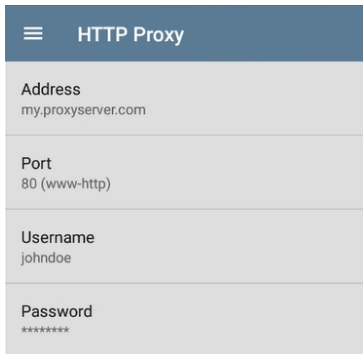
Tap the **Test Targets** field to open the Test Targets screen and add custom Ping, TCP Connect, HTTP, FTP, or Nmap tests to your AutoTest profile. See [Test Targets](#) to learn more.

HTTP Proxy

The Proxy control lets you specify a proxy server through which the CyberScope 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.



HTTP Proxy	
Address	my.proxyserver.com
Port	80 (www-http)
Username	johndoe
Password	*****

Tap each field to open a pop-up keyboard and enter the appropriate **Address** (you can enter a proxy name or an address), **Port** (set to match the proxy port), **Username**, and **Password**. Tap **OK** to save your entries.

Wi-Fi Profile Test Results

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






The screenshot displays the AutoTest application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text "AutoTest" in the center, and "START" and a gear icon on the right. Below the header, the main content area shows a list of test results for a Wi-Fi profile named "Connect to The Office Network #1".

- Connect to The Office Network #1**: 7 tests. A green link icon is on the right, and a yellow circle with the number "1" is in the bottom right corner of the card.
- The Office Network #1**: -42 dBm, 130 Mbps, Roams: 0. A green link icon is on the left, and a right-pointing chevron is on the right.
- Channel 6**: 802.11: 36 %, Non-802.11: 5 %. A green bar chart icon is on the left, and a right-pointing chevron is on the right.
- Lnksys:c8b373-05ac3b**: The Office Network #1. A Wi-Fi router icon is on the left, and a right-pointing chevron is on the right.
- DHCP 192.168.0.140**: <1 ms. A green "DHCP" label is on the left, and a right-pointing chevron is on the right.
- DNS cosopendns1.net.com**: 34 ms. A green "DNS" label is on the left, and a right-pointing chevron is on the right.
- 192.168.0.1**: 23 ms, -, 18 ms. A yellow cloud and server icon is on the left, and a right-pointing chevron is on the right.
- PING google**: A green "PING" label is on the left, and a right-pointing chevron is on the right.

A purple circular button with a white plus sign is located in the bottom right corner of the test results list.

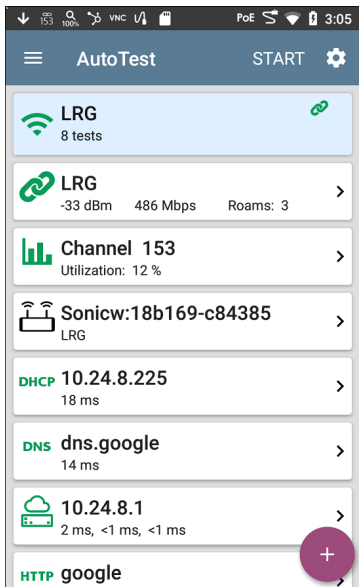
This Profile connects to SSID "The Office Network #1." The Profile is displaying one **Warning** condition from a timeout of the second Gateway ping.

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.

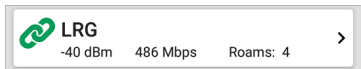
NOTE: Blue links and action icons do not appear on every test screen. If the network connection is dropped, you may need to rerun the Profile to re-establish link and enable additional actions.

The individual test cards and screens using the Wi-Fi Profile results for the "LRG" SSID are 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



CoFC-GuestNet

-47 dBm

130 Mbps

Roams: 4

SSID: [CoFC-GuestNet](#)


Security: Open

 Roams: 4

AP: [10.10.0.5](#)

BSSID: [RuckusWi:543d37-299cb8](#)

Channel: 11


 Roam Scans: 1

Last Roam From

AP: [543d372c7ed8](#)

BSSID: [RuckusWi:543d37-2c7ed8](#)

Channel: 11

 Roam Scans: 3

Results

Signal (dBm)



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 CyberScope 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

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

AP: AP from which the AP last roamed

BSSID: BSSID of the access point

Channel: Channel number on which the AP is operating

Wi-Fi Link Trending Graphs

CyberScope'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.

Results

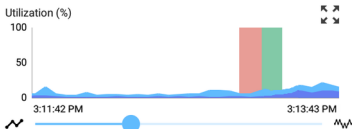


	Cur	Min	Max	Avg
--	-----	-----	-----	-----

Signal (dBm)	-38	-79	-23	-48
--------------	-----	-----	-----	-----

Noise (dBm)	-92	-98	-89	-92
-------------	-----	-----	-----	-----

SNR (dB)	54			44
----------	----	--	--	----



	Cur	Min	Max	Avg
--	-----	-----	-----	-----

802.11 %	7	1	29	7
----------	---	---	----	---

Non-802.11 %	2	0	21	3
--------------	---	---	----	---

Total	9			10
-------	---	--	--	----

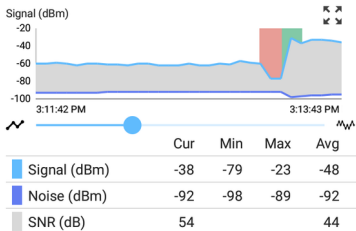
The Wi-Fi Link Test graphs save and display data for up to 24 hours in the past if the unit stays linked. The default time interval shown is 2 minutes.

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.
- 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).

Results

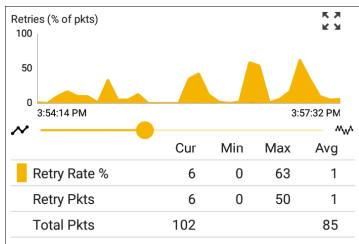


Utilization (%) graph: Plots percentage of the connected channel's capacity being used by 802.11 devices and by non-802.11 interference.

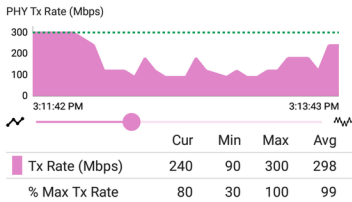
- Green vertical bars - The tester roamed to a new AP.

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.

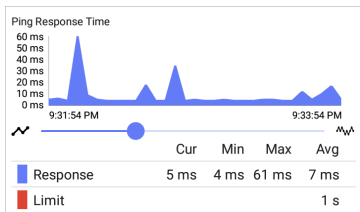


PHY TX Rate (Mbps) graph: Plots the physical transmission rate. The green horizontal dotted line shows the AP's maximum TX rate.




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.




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)

Other Actions


Scroll to the bottom of the link test screen to access action links (in blue):

- Tap **PING** to open the **Ping/TCP** app.
- Tap **CONNECT LOG** to view the **Wi-Fi connection log**.
- Tap the action overflow menu icon **•••** to open an additional menu:
 - Tap **Capture** to open the **Capture** app to run a Wi-Fi packet capture on the connected channel and AP.
 - Tap **Upload graphs to Link-Live** upload graphic results to Link-Live. This opens the Link-Live sharing screen.
 1. Use the default file name (which has a <DATE-TIME> format) or tap the Graphs Image Name field to open a touch keyboard to type a custom name.
 2. Tap **SAVE TO UPLOADED FILES** to upload to the Results page  on Link-Live.com.

Connect Log

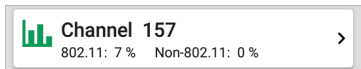
Connect Log	
4:52:26.734 PM	Wireless: SSID LRG
4:52:27.100 PM	WPA2 Personal
4:52:29.892 PM	Link Down
4:52:29.892 PM	Connecting to AP: 18:b1:69:c8:43:8d Chan 1
4:52:29.893 PM	Send Open Authentication Request
4:52:30.317 PM	Authentication Timeout
4:52:30.319 PM	Connecting to AP: 18:b1:69:c8:43:8d Chan 1
4:52:30.319 PM	Send Open Authentication Request
4:52:30.320 PM	Receive Open Authentication Success
4:52:30.320 PM	Send Association Request
4:52:30.320 PM	Wireless: WPA2 Info Element: Mcast=([4] AES-CCMP) Ucast=([4] AES-CCMP) Auth=([2] PSK)
4:52:30.321 PM	Receive Association Success

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.

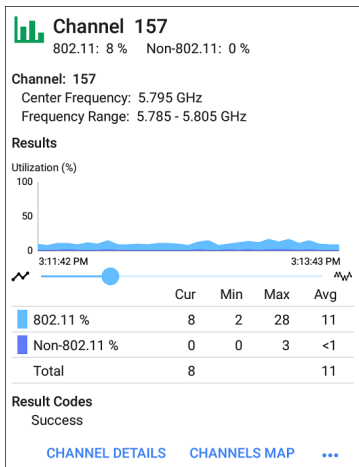
Channel Test Results



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

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
- **Total:** Total percentage of both 802.11 and non-802.11 channel utilization

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

Other Actions

Scroll to the bottom of the link test screen to access action links (in blue):

- Tap **CHANNEL DETAILS** to open the Wi-Fi app's **Channels** display.
- Tap **CHANNELS MAP** to open the Wi-Fi app's **Channels Map** display.
- Tap **CAPTURE** to open the **Capture** app to run a Wi-Fi packet capture.



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 CyberScope 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.

AP Test Screen

AutoTest

10.24.8.29
LRG

Device Name: [10.24.8.29](#)

IP Address: 10.24.8.29
MAC Address: Sonicw:18b169-c84603

SSID: [LRG](#)

Security: WPA2-P
Roams: 0

802.11
Channels: **157**, 159
Type: n
Supported Types: b, g, n

Client Associations: 3
Roam Scans: 3

[CONNECT LOG](#) [PATH ANALYSIS](#) ...

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

Other Actions

Scroll to the bottom of the link test screen to access action links (in blue):

- Tap **CONNECT LOG** to view the [Wi-Fi connection log](#).
- Tap **CAPTURE** to open the [Capture](#) app to run a Wi-Fi packet capture.

DHCP, DNS, and Gateway Results

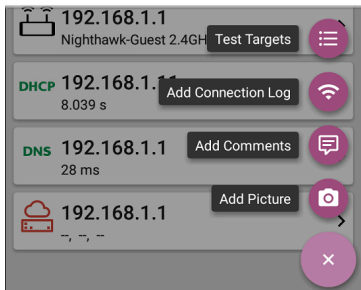
See [DHCP, DNS, and Gateway Tests](#).

PING FTP TCP HTTP Target Tests

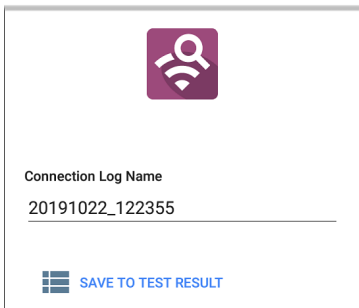
See the [Test Targets](#) topic for information on target test results.

Other Actions (Wi-Fi Profile FAB)

Tap the floating action button (FAB) on the Wi-Fi Profile AutoTest Profile screen to open a floating menu for additional actions:





- Tap **Test Targets** to open the [Test Targets](#) screen. You can add Ping, TCP Connect, HTTP, FTP, and Nmap target tests to the current profile.
- Tap **Add Connection Log** to open a Link-Live sharing screen that allows you to give a custom name to the log file.




1. Use the default file name (which has a <DATE-TIME> format) or tap the text field to enter your desired log name.
 2. Tap **SAVE TO TEST RESULT** to upload the named log file.
- Tap **Add Comments** to open a Link-Live sharing screen where you can add enter comments for the results.
 1. Use the default file name (which has a <DATE-TIME> format) or tap the text field to open a touch keyboard to type a

comment.


2. Tap **SAVE TO LAST TEST RESULT** to upload to the Results page  on Link-Live.com.
- Tap **Add Picture** to open the **Gallery** or **Camera** app to select or take a photo that is then uploaded and attached to your test result.
 1. Use the default file name (which has a <DATE-TIME> format) or tap the Graphs Image Name field to open a touch keyboard to type a custom name.
 2. Tap **SAVE TO UPLOADED FILES** to upload to the Results page  on Link-Live.com.
 - Tap **Add Picture** to 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 more about Link-Live and uploading.

DHCP, DNS, and Gateway Tests

DHCP	10.250.2.168	>
	<1 ms	
DNS	Compass	>
	16 ms	
	10.250.0.1	>
	2 ms, 2 ms, 4 ms	

These tests are included in both [Wired](#) and [Wi-Fi](#) AutoTest Profiles. The settings and results fields are the same for each Profile type.

Access AutoTest's DHCP, DNS, and Gateway tests 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.

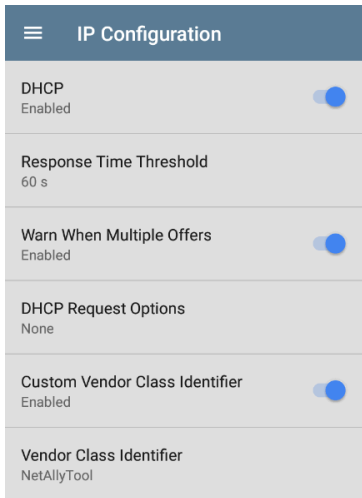
DHCP or Static IP Test

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

DHCP Settings – IP Configuration

To open the IP Configuration screen, either:

- Open a Wired or Wi-Fi Profile, tap the DHCP summary card, and then tap the settings button  on the DHCP test results screen.
- Tap the main menu icon , select **AutoTest Settings**, open a Wired or Wi-Fi Profile, and then tap **IP Configuration**.



DHCP

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

Response Time Threshold

(Appears only if DHCP is enabled.) Tap this field to select a value or enter a custom value to set how long the CyberScope waits for a DHCP server response before failing the DHCP test.

Warn When Multiple Offers

(Appears only if DHCP is enabled.) Depending on how your network is configured, multiple DHCP offers may or may not be a problem. Tap this field to toggle whether AutoTest creates a warning if multiple offers are received.

DHCP Request Options

(Appears only if DHCP is enabled.) Tap this field to open a dialog to select one or more DHCP request options.

Custom Vendor Class Identifier

Custom Vendor Class Identifier is disabled by default. Tap the toggle button to enable the Vendor Class Identifier field, as described below.

Vendor Class Identifier

(Appears only if Custom Vendor Class Identifier is enabled.) Tap this field to type the vendor class identifier.

Static IP Address

IP Configuration	
DHCP Disabled	<input type="checkbox"/>
Static IP Address	
Subnet Mask 255.255.255.0 /24	
Default Gateway 192.168.1.1	
Primary DNS Server 8.8.8.8	
Secondary DNS Server	

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: (User-defined) appears next to the MAC address beneath the DHCP IP address on the results screen when a User-Defined MAC is enabled for this connection in [General Settings](#) or in the AutoTest profile.

☰ AutoTest ⚙️

DHCP 192.168.1.32
736 ms 60c017-530234 (User-defined)

Device Name: [Mike's home AP](#)

IPv4 Address: 192.168.1.1

DHCP Test Results Screen

DHCP 10.250.2.168

<1 ms

Device Name: [COS_DEV_SW1](#)

IPv4 Address: 10.250.0.2

MAC Address: Cisco:001cb1-da2cc6

Results

Offered: 10.250.2.168

Accepted: 10.250.2.168

Subnet Mask: 255.255.252.0

Subnet: 10.250.0.0/22

Lease Time: 1 day 0 seconds

Expires: 4/26 2:39 PM

Relay Agent: --

Metric	Result
 Offer	<1 ms
 Acknowledge	<1 ms
Total Time	<1 ms
Threshold	60 s

End User Response Time

50.0 %  Offer Acknowledge

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 CyberScope

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

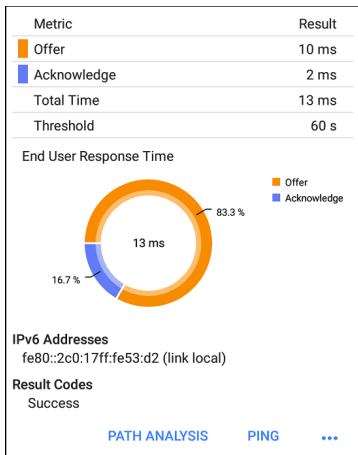
Lease Time: The amount of time the IP address is leased to the CyberScope by the DHCP server

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 CyberScope sent the discovery and received an address offer from the DHCP server

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

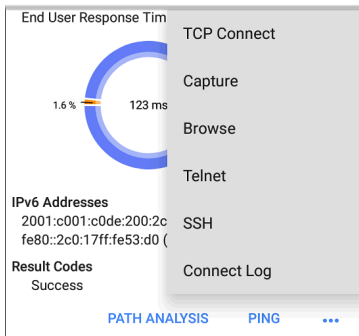
Total Time: Total amount of time consumed by the DHCP process

Threshold: The DHCP Response Time Threshold from the DHCP test settings, which controls how long the CyberScope 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

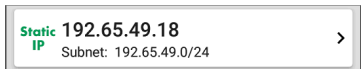
Results Codes: Final status of the test (Success or Failure)



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](#).

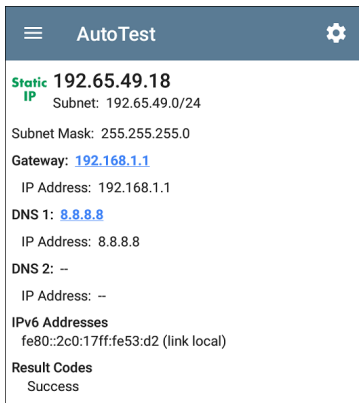
Static IP Test Results

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: [BRW2C6FC94A974E](#)

MAC Address: HonHai:2c6fc9-4a974e

IPv6 Addresses

fe80::2c0:17ff:fe53:d2 (link local)

Result Codes

IP address already in use (11)

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 CyberScope obtains DNS addresses through DHCP or static address configuration.

DNS Test Settings

☰ DNS Test

DNS Test
Enabled

Lookup Name
www.google.com

IP Protocol Version
IPv4

Lookup Time Threshold
1 s

Reverse Grading
Disabled

DNS Test

To disable the DNS test in your current AutoTest, tap the top field on the this screen to set it to Disabled. The DNS card still appears on the main AutoTest results screen so that you can still see the addresses of the DNS servers. However, the

following lookup values are set to "--", and the Result Code is set to "Test is disabled".

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

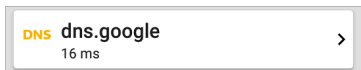
This threshold controls how long the CyberScope waits for a response from the DNS server(s) before the test is failed. The default is 1 second. Tap the field to select or enter a new threshold.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

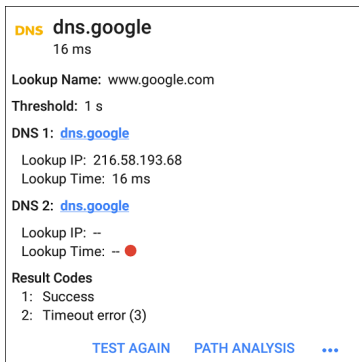
DNS Test Results

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

A screenshot of the full DNS test results screen, enclosed in a black border. At the top, it shows 'DNS dns.google' in bold black with '16 ms' below it. The 'Lookup Name' is 'www.google.com'. The 'Threshold' is '1 s'. 'DNS 1' is listed as '[dns.google](#)' with 'Lookup IP: 216.58.193.68' and 'Lookup Time: 16 ms'. 'DNS 2' is also '[dns.google](#)' but with 'Lookup IP: --' and 'Lookup Time: --' followed by a red circle. Under 'Result Codes', it lists '1: Success' and '2: Timeout error (3)'. At the bottom, there are three blue buttons: 'TEST AGAIN', 'PATH ANALYSIS', and a three-dot menu icon.

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

14 ms

Lookup Name: www.goo

Threshold: 1 s

DNS 1: [dns.google](#)

Lookup IP: 172.217.11.

Lookup Time: 14 ms

DNS 2: [dns.google](#)

Lookup IP: 172.217.11.

Lookup Time: 14 ms

Result Codes

1: Success

2: Success

Ping

TCP Connect

Capture

Browse

Telnet

SSH

TEST AGAIN PATH ANALYSIS ...

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.

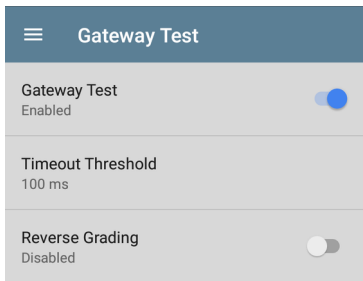


Gateway Test

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	
Gateway Test Enabled	<input checked="" type="checkbox"/>
Timeout Threshold 100 ms	
Reverse Grading Disabled	<input type="checkbox"/>

Gateway Test

To disable the Gateway test in your current AutoTest, tap the top field on the this screen to set it to Disabled. The Gateway card still appears on the main AutoTest results screen so that you can still see the addresses of the Gateway servers. However, the following lookup values are set to "--", and the Result Code is set to "Test is disabled".

Timeout Threshold

Indicates how long the CyberScope 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.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

Gateway Test Results

CyberScope 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 CyberScope'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



The screenshot shows the 'AutoTest' application interface. At the top, there is a dark blue header with a hamburger menu icon on the left, the text 'AutoTest' in the center, and a gear icon on the right. Below the header, the main content area has a white background. It starts with a green cloud icon and a server rack icon, followed by the text 'COS_DEV_SW1' and '2 ms, 2 ms, 3 ms'. Below this, there are several sections: 'IPv4 Gateway Name: COS_DEV_SW1', 'IPv4 Address: 10.250.0.1', 'MAC Address: Cisco:00000c-07ac01', 'IPv6 Gateway Name: Andromeda Automation Procurve', 'Protocols: RIP, OSPF, HSRP, Statically Configured Router, Proxy ARP Agent, Virtual Router (HSRP)', 'Ping Results' with 'Response Times: 2 ms, 2 ms, 3 ms' and 'Threshold: 100 ms', and 'Result Codes' with a list: '1: Success', '2: Success', '3: Success'. At the bottom of the screen, there are three blue buttons: 'TEST AGAIN', 'PATH ANALYSIS', and '...'.

AutoTest

 **COS_DEV_SW1**
2 ms, 2 ms, 3 ms

IPv4 Gateway Name: [COS_DEV_SW1](#)

IPv4 Address: 10.250.0.1
MAC Address: Cisco:00000c-07ac01

IPv6 Gateway Name: [Andromeda Automation Procurve](#)

Protocols: RIP, OSPF, HSRP, Statically Configured Router, Proxy ARP Agent, Virtual Router (HSRP)

Ping Results
Response Times: 2 ms, 2 ms, 3 ms
Threshold: 100 ms

Result Codes

- 1: Success
- 2: Success
- 3: Success

[TEST AGAIN](#) [PATH ANALYSIS](#) [...](#)

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 CyberScope 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

 **COS-IT-SW1.netally.com**
1 ms, 1 ms, 1 ms

Gateway Name: [COS-IT-SW1](#)

IPv4 Address: 172.24.0.1
MAC Address: Cisco:6c:fc:90:80:00:00:00
IPv6 Address: --

Protocols: Statically Configured

Ping Results
Response Times: 1 ms, 1 ms, 1 ms
Threshold: 100 ms

Result Codes
1: Success
2: Success
3: Success

Ping
TCP Connect
Capture
Browse
Telnet
SSH

[TEST AGAIN](#) [PATH ANALYSIS](#) [...](#)

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.

Test Targets for Wired and Wi-Fi AutoTest

PING	google	>
	28 ms, 28 ms, 15 ms	
TCP	NetAlly	>
	80 ms, 76 ms, 82 ms	
HTTP	github	>
	1.114 s	
FTP	Asset Server	>
	246 ms	

AutoTest Target tests are user-assignable endpoints to which CyberScope 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](#)

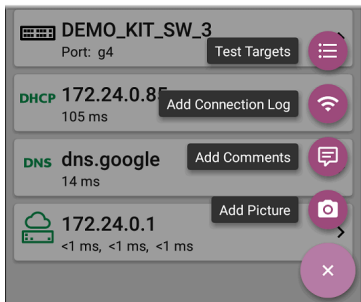
[HTTP](#)

[FTP](#)

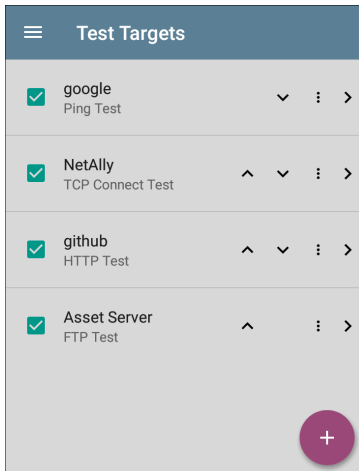
Nmap

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 targets enabled in the current Profile. (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:

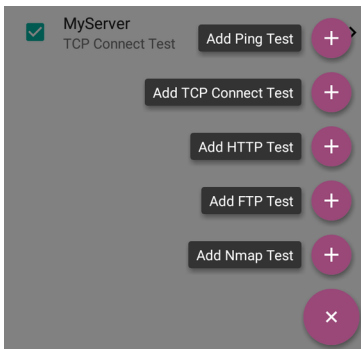
- Select the checkboxes for each Target you want to include in the current profile.
- Tap the up and down arrows to reorder the saved Test Targets on this screen and the

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, FTP or Nmap.



- Tap any target test name to open that test's settings. You can then enter a custom test name, test type, target address, or thresholds. For more information on settings, see:
 - [Ping Test](#)
 - [TCP Connect Test](#)
 - [HTTP Test](#)
 - [FTP Test](#)
 - [Nmap 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.

PING google

9 ms, 33 ms, --

Device Name: [172.217.1.196](#)

IPv4 Address: 172.217.1.196

MAC Address: --

Results

Lookup Time: 3 ms

Response Times: 9 ms, 33 ms, -- ●

Threshold: 250 ms

Result Codes

1: Success

2: Success


3: Timeout error (3)

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

[TEST AGAIN](#)[PATH ANALYSIS](#)

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](#) to app with the path destination configured with the current target.
- Tap the action overflow icon  to open the listed apps or tools with the target pre-populated, for example:
 - **Ping** or **TCP Connect** to open the [Ping/TCP](#) app with the current target address.
 - [Capture](#) traffic from the test target.
 - Browse to the target URL on the internet with your [web browser](#) app.

- **Telnet** or **SSH** to open the [Telnet/SSH tools](#) with the current target address.

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

Ping Test	
Name	google
Device Name	www.google.com
IP Protocol Version	IPv4
Frame Size (bytes)	64
Do Not Fragment	<input type="checkbox"/>
Timeout Threshold	1 s
Reverse Grading	<input type="checkbox"/>

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 device. 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

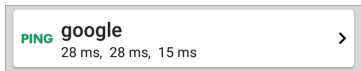
This threshold controls how long the CyberScope waits for a response from the target before failing the test.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

For example, you might have a critical server used by an accounting department. This server must be accessible by the accounting VLAN but not by any other networks. To verify the configuration, you could set up a reverse-graded Ping test, and then run a Wi-Fi AutoTest profile to the server's guest SSID. The test reports a ping failure, which is the desired outcome.

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

PING **google**
4 ms, 4 ms, 5 ms

Device Name: www.google.com

IPv4 Address: 172.217.12.4
MAC Address: --

Results
Lookup Time: 1 ms
Response Times: 4 ms, 4 ms, 5 ms
Threshold: 1 s

Result Codes
1: Success
2: Success
3: Success

[TEST AGAIN](#) [PATH ANALYSIS](#) ...

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 CyberScope to receive a response from the target after sending each of the three connections.
- **Threshold:** The Timeout Threshold indicated in the test's settings.

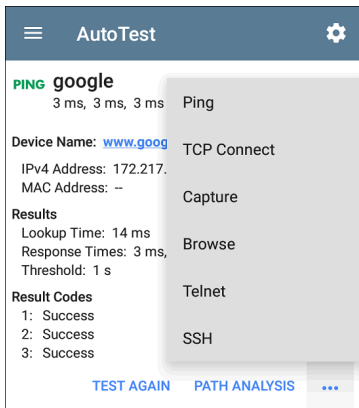
Results Codes: Final status of the test (Success or Failure) for each of the three connections.

Other Actions

Use the **blue links** or the blue action overflow icon **...** button at the bottom of the test results screens to perform other actions.

- Tap **TEST AGAIN** to run the Ping test again.
- Tap **PATH ANALYSIS** to open the Path Analysis app with the Ping test's information.

- Tap the blue action overflow icon **...** to open another testing app (Ping, TCP Connect, or Capture), to **Browse** to the Ping target address in your web browser, or to 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

TCP Connect Test	
Name	google
Device Name	www.google.com
IP Protocol Version	IPv4
Port	80 (www-http)
Timeout Threshold	1 s
Reverse Grading	<input type="checkbox"/> Disabled

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.

Port

Specify the TCP port number for the CyberScope to use to connect to the target.

Timeout Threshold

This threshold controls how long the CyberScope waits for a response from the target before failing the test.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

TCP Connect Test Results

TCP
NetAlly
>

80 ms, 76 ms, 82 ms

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

☰
AutoTest
⚙️

TCP
NetAlly

50 ms, 44 ms, 42 ms

Device Name: ip-184-168-221-49.ip.secureserver.net

IPv4 Address: 184.168.221.49

MAC Address: –

Port: 80 (www-http)

Results

Lookup Time: 21 ms

Response Times: 50 ms, 44 ms, 42 ms

Threshold: 250 ms

Result Codes

1: Success

2: Success

3: Success

TEST AGAIN
PATH ANALYSIS
⋮

Device Name: DNS name of the device tested

IPv4 or IPv6 Address: IP address of the target device

MAC Address: Device's MAC address. 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 CyberScope 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

Other Actions

Use the **blue links** or the blue action overflow icon **...** button at the bottom of the test results screens to perform other actions.

- Tap **TEST AGAIN** to run the Ping test again.
- Tap **PATH ANALYSIS** to open the Path Analysis app with the TCP test's information.
- Tap the blue action overflow icon **...** to open another testing app (Ping, TCP Connect, or Capture), to **Browse** to the target address in your web browser, or to start a **Telnet or SSH** session.

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 based on responses, return codes, and time threshold.

HTTP Test	
Name	github
URL	https://www.github.com
IP Protocol Version	IPv4
Allow Redirects	<input checked="" type="checkbox"/> Enabled
Response Time Threshold	10 s
Web Page Transfer Size	ALL
Response Must Contain	

Name

Tap this field 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 CyberScope 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	
Response Must Not Contain	
Return Code	
200 - OK	
Reverse Grading	<input type="checkbox"/>
Disabled	
HTTP Proxy	<input type="checkbox"/>
Disabled	

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 CyberScope receives a different return code, the test fails.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

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

HTTP **github**
3.671 s





Device Name: [lb-192-30-253-113-iad.github.com](#)

IPv4 Address: 192.30.253.113

MAC Address: --

URL: <https://www.github.com>

Results

Metric	Result
Ping	54 ms
 DNS Lookup	59 ms
 TCP Connect	165 ms
 Data Start	1.288 s
 Data Transfer	2.157 s
Total Time	3.671 s
Threshold	10 s
Data Bytes	90.9 K
Rate (bps)	206.2 K

End User Response Time

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

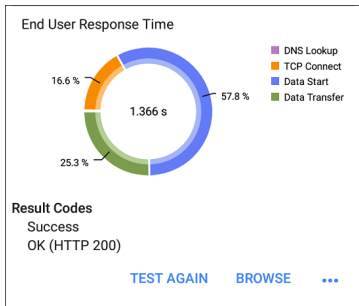
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

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

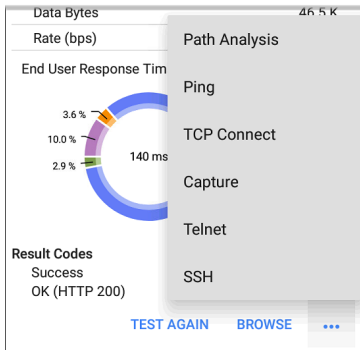
Rate (bps): The measured data transfer rate



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.




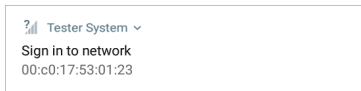
Tap [blue links](#) or the blue action overflow icon **...** at the bottom of the test results screens to run the HTTP **TEST AGAIN**, open another testing app, or **Browse** to the target address in your web browser.

Captive Portal Connections

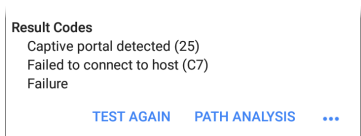
The HTTP test supports connections through a network with a captive portal requirement.

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 [Captive Portals](#) 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.

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.

FTP Test	
Name	Asset Server
FTP Server	10.250.2.218
IP Protocol Version	IPv4
File	internal/iperf3
File Transfer Size	ALL
Direction	Get <input checked="" type="checkbox"/>
Response Time Threshold	10 s

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 CyberScope 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 CyberScope.
- 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 CyberScope, and the test string is repeated to produce the set file size.

Response Time Threshold

This threshold controls how long the CyberScope waits for a response from the FTP server before failing the test. Tap the field to change the value.

Username	
Password	
Reverse Grading Disabled	<input type="checkbox"/>
HTTP Proxy Disabled	<input type="checkbox"/>

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.

Reverse Grading

When Reverse Grading is enabled, a test is considered successful if it fails and a failure if it succeeds. The Results Codes section of the results screen includes the message "Grading has been reversed".

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

Metric	Result
FTP Asset Server	
171 ms	
Device Name: 10.250.2.218	
IPv4 Address: 10.250.2.218	
MAC Address: --	
Get File: /internal/iperf3	
Results	
Ping	50 ms
DNS Lookup	--
TCP Connect	44 ms
Data Start	116 ms
Data Transfer	10 ms
Total Time	171 ms
Threshold	60 s
Data Bytes	24 K
Rate (bps)	1.2 M

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.

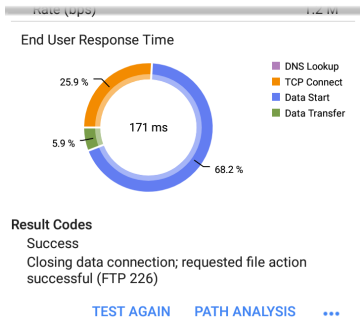
Total Time: The end user response time (EURT), which is the total time it took to download the web page. It is the sum of DNS lookup, TCP connect, data start, and data transfer time. If the Total Time exceeds the Response Time Threshold in the settings, the test fails.

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.

Nmap Test

Nmap tests perform a wide variety of functions. See the [Nmap App](#) chapter for more information on setting up Nmap tests.

Nmap Test Settings

Nmap settings allow test grading criteria based on responses and return code in addition to the time threshold.

Nmap Test	
Name Graded Ports scanme.nmap	
Nmap Test Graded Ports	
Target IPv4: scanme.nmap.org	>

Name

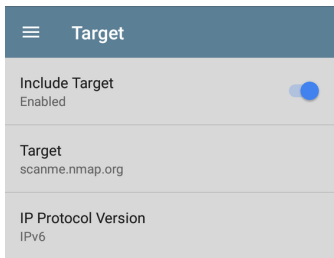
This field allows you to assign a custom name to the test. The name appears on the target test card in the profile.

Nmap Test

This field displays the current Nmap test. The default test is the top test that is listed on the main Nmap test screen. To select a different test, use the keypad to delete the current test name. This displays a menu of available tests. Tap the test you want to use. See [Nmap Tests](#) for more information about the test list.

Target

Tap this field to display the Target screen.



NOTE: Not all Nmap tests require targets.

- **Include Target** - Tap to enable or disable the target options.

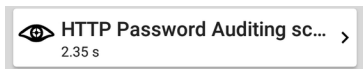
- **Target** - Tap to open a text field to enter the target name.
 - Tap the down arrow to select between a Name (such as a URL) or an IP address.
 - Enter the name or IP address in the field and tap **OK**.
- **IP Protocol Version** - Tap to select either **IPv4** or **IPv6**.

Interface

Tap this field to select the port on which to run the test (any, wired, Wi-Fi, management, etc.).

See [Test and Management Ports](#).

Nmap Test Results



The Nmap results card shows the Nmap icon, which is color-coded to the test results (green for Pass, yellow for Warning, red for Error). The test title depends on the name you assigned to the test.

Nmap Test Results Screen

Nmap test results vary widely depending on the nature of the test. The sample HTTP Password Auditing test, provided by NetAlly, checks for open ports at <https://scanme.nmap.org>, a demonstration website for simple port scans provided by [Nmap.org](https://nmap.org). The scanning locates several open ports that might be cause for concern and generates a warning. The open ports are colored yellow, as is the overall test icon. This provides a quick visual summary of the test results. See [Nmap Output](#) for more information on Nmap results screens.



HTTP Password Auditing

5.63 s

Nmap Test: [HTTP Password Auditing](#)

Command

```
nmap --script http-brute nmap.org
```

Device Name: [nmap.org](#)

IPv4 Address: 45.33.49.119

MAC Address: -

Duration: 5.63 s

Results

Starting Nmap (<https://nmap.org>) at
2023-09-21 18:04 UTC

Nmap scan report for nmap.org
(45.33.49.119)

Host is up (0.019s latency).

Other addresses for nmap.org (not
scanned): 2600:3c01:e000:3e6::6d4e:7061

rDNS record for 45.33.49.119:

ack.nmap.org

Not shown: 993 filtered tcp ports
(no-response)


PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp

Nmap Test: The name of the standard Nmap test that ran. Tap the blue hyperlink to [edit the test parameters](#).

Command: The Nmap command line that ran to produce the results.

Device Name: The device on which the test was performed. Tap the blue hyperlink to open the [Discovery details for the device](#).

Actions

- To automatically scroll to the next green, yellow, or red highlighted text in the output, tap the Next icon  in the screen header.
 - The display returns to the first result if you tap the icon again after displaying the last highlighted text.
 - The results may not change when there is no highlighted text or if all highlighted text is already displayed.
- Tap the test name link to open the Nmap Test settings. This link gives you a quick way to change settings before making more test runs.
- Tap **TEST AGAIN** to run just the target test again.

- Tap **PATH ANALYSIS** to open the **Path Analysis** app with the path destination configured with the current target.
- Tap the action overflow icon **•••** to open a list of apps or tools with the target pre-populated:
 - Tap **Ping** or **TCP Connect** to open the **Ping/TCP** app with the current target address.
 - Tap **Capture** to open the **Capture** app with the current target address.
 - Tap **Browse** to the target URL on the internet with your **web browser** app.
 - Tap **Telnet** or **SSH** to open the **Telnet/SSH tools** with the current target address.

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](#).



Air Quality Profile

Top 2.4 GHz Channels By Utilization

Channel	APs	802.11 (%)
11	2	7
1	2	6
12	0	6
10	0	4

Channel	APs	Non-802.11 (%)
4	0	11
10	0	7
7	0	7
2	0	4

Top 2.4 GHz Channels By Co-Channel Interference

Channel	APs
11	2
1	2
5	1
9	1



The CyberScope 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.



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



Top 5 GHz Channels By Utilization

Channel	APs	802.11 (%)
153	0	7
149	1	6
161	0	6
157	6	5
Channel	APs	Non-802.11 (%)
52	0	1
56	0	1
--	--	--
--	--	--

Top 5 GHz Channels By Co-Channel Interference

Channel	APs	
157	6	
36	2	
149	1	
--	--	

Top 5 GHz Channels By Adjacent Channel Interference

Channel	APs	
149	6	



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)

Viewing and Saving Results


Viewing Channel Utilization

Tap the blue **CHANNELS MAP** link at the bottom of the Air Quality Profile screen to open the **Channels Map** display in the Wi-Fi app. This

display gives you real-time visual results of the utilization on each channel.

Uploading Results to Link-Live

Tap the blue **UPLOAD GRAPHS TO LINK LIVE** to upload graphic results to Link-Live. This opens the Link-Live sharing screen.

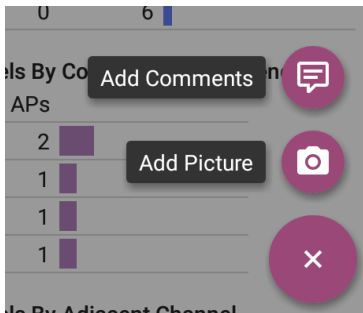
1. Use the default file name (which has a <DATE-TIME> format) or tap the Graphs Image Name field to open a touch keyboard to type a custom name.
2. Tap **SAVE TO UPLOADED FILES** to upload to the Results page  on [Link-Live.com](https://www.link-live.com).

Air Quality Profile FAB


(Optional) On the AutoTest Air Quality Profile results screen, tap the floating action button (FAB) and follow the screen instructions to attach comments and images to the results on the [Link-Live](https://www.link-live.com) website.

- The **Add Comments** option opens a Link-Live sharing screen where you can enter text and job 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.

Air Quality Profile

Name
Air Quality Profile

Channel Scan Cycles
3

AP Signal Level Threshold
-75 dBm

Grading

Utilization
Enabled


Warning
35 %

Failure
75 %

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.

Co-Channel Interference

Enabled



Warning Threshold

4 APs

Failure Threshold

8 APs

Adjacent Channel Interference

Enabled



Warning Threshold

4 APs

Failure Threshold

8 APs



Nmap App

Nmap is a powerful utility for network discovery and security auditing. You can scan networks, send packets, analyze responses, and run scripts to assess network security and diagnose vulnerabilities. Nmap tests can run against single hosts or large-scale networks. Nmap tests can also run in combination with the [Autotest](#) and [Discovery](#) applications.

Nmap Chapter Contents

This chapter describes Nmap tests, shows how to create tests, details test settings, shows how to run tests with the Nmap Runner, and gives examples of Nmap output.

- [Introduction to Nmap](#)
- [Nmap Tests](#)
- [Nmap Settings](#)
- [Nmap Runner](#)
- [Nmap Output](#)

Introduction to Nmap

Nmap uses raw IP packets to determine:

- What hosts are available on a network
- What services (application name and version) the hosts offer
- What operating systems (and versions) are running
- The type of packet filters or firewalls in use

The Nmap app supports Nmap scripts to help you enhance Nmap functionality. These scripts include:

- Predefined Nmap scripts
- User scripts that you create
- Custom discovery scripts to be used with the Discovery app

Nmap can be used for:

- Auditing device or firewall security by finding what network connections can be made
- Identifying open ports on hosts to prepare for auditing

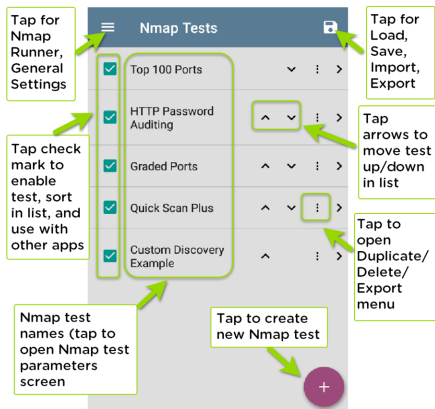
- Network inventory, network mapping, maintenance and asset management
- Security auditing by identifying new servers on a network
- Sending network traffic to network hosts and then analyzing responses and response time
- Finding vulnerabilities in a network
- Sending DNS queries and searching sub-domains
- Managing service upgrade schedules
- Monitoring host or service uptime

For additional information, see:

- [Nmap.org](https://nmap.org) for detailed information on Nmap
- NetAlly's [Cyber Security Blog](#) for information on building custom scripts, using the CyberScope scripting engine, vulnerability assessments, cyber security assessments, and vulnerability scanning.

Nmap Tests

The main Nmap Tests screen displays a list of Nmap tests including predefined demonstration tests provided by NetAlly and any custom tests that you have created or imported.



Predefined Tests

NetAlly provides the following predefined Nmap tests to that you can run as-is or copy and modify for your own purposes. These tests provide examples of Nmap features and capabilities on your test unit.

Top 100 Ports: Scans and lists information for the 100 most common ports in use on a target that you provide.





HTTP Password Auditing: Provides an example of script usage in Nmap tests by using the `http-brute` script to check authentication for port 80 on a web server and performs a brute-force password test if needed.

Graded Ports: Demonstrates the use of regular expressions (regex) by using expressions to grade or mark up results that must contain a range of values and must not contain another set of values.

Quick Scan Plus: Performs a fast port scan limited to the top 100 most common TCP ports with light-intensity OS and version detection.

Custom Discovery Example: Demonstrates a test that runs as part of the Discovery app, which may provide additional information and arguments to run the test. This sample test is a wrapper for the `custom-discovery-example.nse` script. The example script documents the API between Discovery and the script. In this case, Discovery provides the script arguments. Discovery tests can run against every address that it can find on the target network and can be a powerful aid to network administrators.


Other List Actions


- Select the checkbox  to enable/disable running the test in the [Nmap Runner](#), to enable/disable moving a test in the list, and to make the test available to the [AutoTest](#) and [Discovery](#) apps.
- Tap the up or down arrow icons   to move a test up or down in the list.
- Tap the action overflow icon  for a test to open the Duplicate/Delete menu:

- Tap **Duplicate** to copy the selected test. This opens the Nmap Test parameters screen, which lets you [rename and edit the parameters for the test](#). Duplicated tests are added to the list of tests.
- Tap **Delete** to delete the selected test. (You are warned if the test is in use by [AutoTest](#), [Discovery](#) or Nmap.)
- Tap **Export** to create an export file of the current test to save to internal or connected external storage.
- Tap **Export To Link-Live** to upload the test directly to [Link-Live](#). You can then push the test to other CyberScope or CyberScope Air units.


Creating a New Test

To create a new Nmap test:

1. On the main Nmap Tests screen, tap the floating action icon . This creates a new blank test and opens the Nmap Test parameter screen.

2. Use the Nmap Test parameter screen to [edit the parameters for the test](#).
3. Either tap the system Back icon or tap the navigation menu icon  and then select **Nmap Tests** to return to the main test list. Your new test is now included in the list.
4. Follow the instructions in [Running Nmap Tests](#) to run the new test.

Load, Save, Import, and Export App Settings

The save button  at the top right within main Nmap app screen opens a menu with the following selections:

- **Load** opens a previously saved Nmap configuration.
- **Save As** saves the current configuration 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.
- **Export To Link-Live:** Exports the current settings directly to [Link-Live](#).

Automatic and Manual Importing

- Nmap settings or tests can be pushed from Link-Live to your test unit. After the download completes, these settings or tests are automatically imported with a notification. The Nmap app then returns to the main Nmap list.

NOTE: If the notification indicates a failure, try to manually import the settings or tests to get more specific reason for the failure.

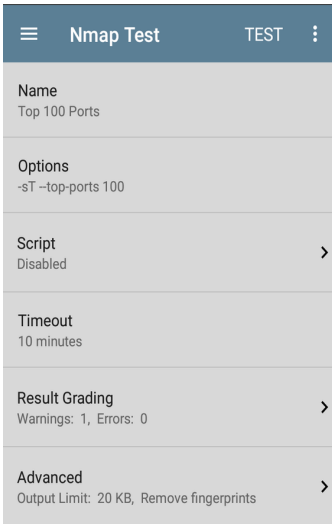
- Automatically imported settings may alter the current settings test settings.
- Importing an individual Nmap test file adds (or modifies) only the individual Nmap test. No other Nmap settings are changed.
- Importing a Nmap setting file replaces all existing Nmap settings.

For more information, see:

- [Saving App Settings and Configurations](#)
- [Import/Export Settings](#)
- [Import/Export Settings for All Apps](#)

Editing Nmap Test Parameters

To edit the basic parameters for a test, tap the test in the list on the main Nmap Tests screen. This displays the Nmap Test screen.



Name: The name of the test. Use the text editor to edit the name if desired.

Options: Nmap options for the test. (For example, the default Top 100 Ports test lists `-sT --top-ports 100`.) Use the text editor to edit the options if desired.

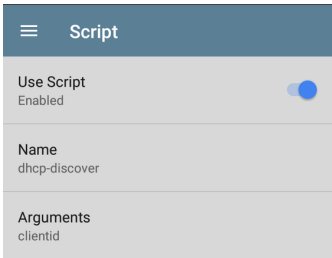
Script: - Tap this field to display the Script screen.

NOTE: NetAlly recommends that you create and test your Nmap scripts in whatever development environment you prefer, upload the scripts to Link-Live, and then use Link-Live's Nmap features to push the scripts to your organization's CyberScope units. For more information, see:

<https://nmap.org/nsedoc/scripts/>

and

[Introduction to NMAP Scripting Engine on CyberScope](#)

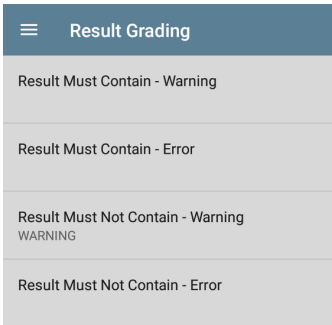


- **Use Script** - Tap to enable or disable the script options.
- **Name** - Tap the Name field to enter the script name:
 1. Use the text editor to type the beginning of the script name. The Nmap app presents matching scripts as you type.
 2. Tap **OK** when the Name is complete.
- **Arguments** - Tap to open a text editor to type the arguments for the script.

Timeout: - Tap to disable or to choose a preset value. You can also enter a custom value.

Result Grading

Tap **Result Grading**: to enter text or regex strings for the Result Must Contain or Result Must Not Contain parameters. You can enter a string for one warning and one error for each parameter.



Result Must Contain: Specifies a value that the result must contain. Tap the field to open a text editor to enter a string or regex value. For example, the Graded Ports sample test uses this value:

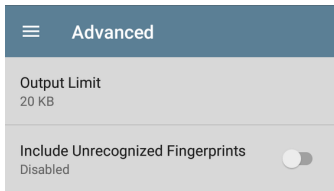
```
regex:\n25/tcp +filtered +SMTP
```

Result Must Not Contain: Specifies a value that the result must *not* contain. Tap the field to open a text editor to enter a string or regex value. For example, the Graded Ports sample test uses this value:

```
regex:\d+tcp +open
```

Advanced

Tap the field to open the Advanced option screen.



- **Output Limit** - Tap to open a selection window for output limit values or to select no limit.

NOTE: some Nmap tests can generate significant output, so setting a reasonable output limit can help clarify test results.

- **Include Unrecognized Fingerprints** - Tap to enable/disable inclusion of unrecognized operating system "fingerprints" in output results.

Changing the Test Type

If you need to change the test's type between a Standard Nmap Test and a Custom Discovery Test, tap the action overflow menu icon to open the Test Type option, and then tap **Test Type**. Choose the test type from the dialog.

About Custom Discovery Tests: CyberScope allows these tests for enhancing discovered devices with additional custom scripting. A typical application would be integration into enterprise IT systems. You can retrieve additional information via API (GET) and display results with the other device details to embellish the results on CyberScope. Alternatively, a custom script can push information to an API (PUT) to augment existing IT software and applications. Custom Discovery script development goes beyond the scope of this guide, but the [Custom Discovery Example](#) provides a sample

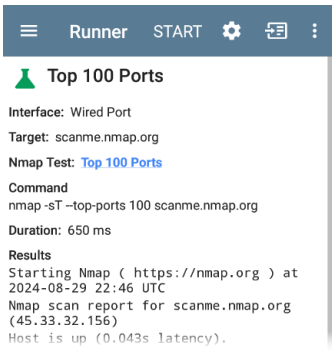
test that you can use to become familiar with how such tests are used with CyberScope.

Regex Resources




For more information about the form of regex used with CyberScope, see [Regular expression syntax cheat sheet](#).


Running Nmap Tests

The Nmap Runner runs tests, lets you edit run settings, and lets you upload results.



1. Begin on the main Nmap Tests screen, and tap the test you want to run. This opens the Nmap Test parameter screen, which lets you [edit the parameters for the test](#).
2. When you have changed any parameters that you want, tap **TEST** to open the Runner screen.

3. To adjust the run settings for this specific test (such as specifying a target if the test requires a target), tap the settings icon  to open the [Nmap Runner Settings](#) screen. When you have finished, tap the system Back icon  to return to the main Runner screen.
4. Tap **START**. This runs the test with the parameters and settings that you have chosen.
5. (Optional) Tap the action overflow icon , and then select **Upload to Link-Live** to upload the test results to the [Link-Live](#) cloud service.
 - a. Enter a comment about the test in the Comment field.
 - b. Enter a more specific information about the test or results in the Job Comment field.
 - c. Tap **Save to Link-Live**.

NOTE: The Next icon  in the screen header automatically scrolls to between green, yellow, or red highlighted text in the [Nmap Output](#).

Nmap Runner Settings

These Nmap runner settings specify the run-time settings for the test. These settings may change with each run of the test, in contrast to the more stable test parameters that get saved with the test.

Nmap Runner Settings	
Mode	Nmap Test
Nmap Test	HTTP Password Auditing
Target	IPv4: nmap.org >
Interface	Any Port

Mode

Selects the method for running the test.

Nmap Test - Uses the parameters specified in an Nmap Test to construct the Nmap command.

Command Line - Runs the test with an editable command line, starting with a default Nmap command. This mode is convenient if you know specific changes that you want to make to the command line options.

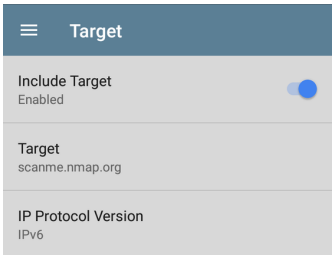
Nmap Test

(For Nmap Test mode only)

- Displays the name of the current test.
- To select a new test:
 1. Use the text editor to delete the current test name. This displays a list of available tests.
 2. Select a new test from the list, and then tap **OK**.

Target

(For Nmap Test mode only) Tap this field to display the Target screen.



NOTE: Not all Nmap tests require targets.

- **Include Target** - Tap to enable or disable the target options.
- **Target** - Tap to open a text field to enter the target name.
 - Tap the down arrow to select between a Name (such as a URL) or an IP address.
 - Enter the name or IP address in the field and tap **OK**.
- **IP Protocol Version** - Tap to select either **IPv4** or **IPv6**.


Interface

Tap this field to select the port on which to run the test (any, wired, Wi-Fi, management, etc.).

See [Test and Management Ports](#).

Nmap Output

This section gives details of Nmap output and presents two examples of how you can use the NetAlly [Nmap parameters](#) to enhance the output appearance. There are also many output options in the Nmap utility, as documented at Nmap.org.

- To automatically scroll to the next green, yellow, or red highlighted text in the output, tap the Next icon  in the screen header.
 - Note that the Next button is always displayed and functional, although it may not result in any screen changes, for example if there are no green/yellow/red highlighted text sections or if all the highlighted text sections are already visible on the screen.
 - The display returns to the first result if you tap the icon again after displaying the last highlighted text.
- Tapping the link for the test name in the output opens the [Nmap Test parameter screen](#) so that you can edit the parameters

for new test runs.



HTTP Password Auditing

Interface: Wired Management Port

Target: nmap.org


Nmap Test: [HTTP Password Auditing](#)

Command

`nmap --script http-brute nmap.org`

Duration: 6.06 s

Results

- The [Output Limit](#) parameter in the [Advanced options](#) controls the output size.
- To upload test results to Link-Live, tap the action overflow icon  at the top of the output screen, and then tap **Upload to Link-Live**. Enter any desired comments or job comments on the upload screen, and then tap **SAVE TO LINK-LIVE**.

Below are examples of how you can use the NetAlly [Nmap parameters](#) to grade and organize output appearance.

- **Password Audit with Result Grade**

Warning: The first example shows part of a results screen for the sample HTTP Password Auditing test as run against nmap.org. The Result Must Not Contain parameter is set to the text "open" and the Result Grade parameter is set to **Warning**. When the text "open" appears in the port results, the icon in the output header is colored yellow to indicate the warning, as are the strings in the output results.



Runner

START



HTTP Password Auditing

Interface: Wired Management Port

Target: nmap.org

Nmap Test: [HTTP Password Auditing](#)

Command

```
nmap --script http-brute nmap.org
```

Duration: 6.06 s

Results

Starting Nmap (https://nmap.org) at
2023-05-30 02:30 UTC

Nmap scan report for nmap.org
(45.33.49.119)

Host is up (0.018s latency).

Other addresses for nmap.org (not
scanned): 2600:3c01:e000:3e6::6d4e:7061

rDNS record for 45.33.49.119:

ack.nmap.org

Not shown: 993 filtered tcp ports
(no-response)

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
70/tcp	closed	gopher
80/tcp	open	http

- **Password Audit with Result Grade**

Error: The second example also shows part of a results screen for the sample HTTP Password Auditing test as run against

nmap.org. The Result Must Not Contain parameter is also set to the text "open", and the Result Grade parameter is set to **Error**. When the text "open" appears in the port results, the icon in the output header is colored red to indicate the error, as are the strings in the output results.



Runner

START



HTTP Password Auditing

Interface: Wired Management Port

Target: nmap.org

Nmap Test: [HTTP Password Auditing](#)

Command

```
nmap --script http-brute nmap.org
```

Duration: 6.33 s

Results

Starting Nmap (https://nmap.org) at
2023-05-30 02:34 UTC

Nmap scan report for nmap.org
(45.33.49.119)

Host is up (0.019s latency).

Other addresses for nmap.org (not
scanned): 2600:3c01:e000:3e6::6d4e:7061

rDNS record for 45.33.49.119:

ack.nmap.org

Not shown: 993 filtered tcp ports
(no-response)

PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smt
70/tcp	closed	gopher
80/tcp	open	http

- **Password Audit with Regex Expression and Result Grade Error:** The final example shows how you use regex with the HTTP Password Auditing test to organize and grade the

output. The Result Must Contain parameter is set to "regex:PORT +STATE +SERVICE|[0-9]+ filtered|\d+ closed" to control spacing of the output results. The Result Must Not Contain parameter is set to "regex:open +ssh". The Result Grade parameter is set to **Error**. The partial results screen below shows the closed port data colored green due to meeting the regex criteria. An open ssh port generates an error that colors that result red as well as the Nmap icon at the top of the screen.



Nmap

 10.250.3.9Nmap Test: [Top 100 Ports](#)

Command

nmap -sT --top-ports 100 10.250.3.9

Duration: 540 ms

Results

Starting Nmap (<https://nmap.org>) at
2023-05-31 21:22 UTC

Nmap scan report for 10.250.3.9

Host is up (0.0011s latency).

Not shown: 97 closed tcp ports
(conn-refused)

PORT	STATE	SERVICE
------	-------	---------

22/tcp	open	ssh
--------	------	-----

80/tcp	open	http
--------	------	------

443/tcp	open	https
---------	------	-------

MAC Address: 28:B3:71:38:37:40 (Ruckus
Wireless)Nmap done: 1 IP address (1 host up)
scanned in 0.54 seconds

Result Codes



Discovery App

The 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, Nmap, Path Analysis, and connection tests.

Devices are discovered in the local broadcast domains where the CyberScope 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](#)

[Main Discovery List Screen](#)

[Discovery Details Screens](#)

[Device Types](#)

[Device Names and Authorization](#)

[Discovery Settings](#)

[Problem Settings](#)

[TCP Port Scan Settings](#)


Introduction to Discovery



Discovery uses Ethernet, fiber, and Wi-Fi to find, classify, and display 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
- Results of Nmap tests

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 CyberScope's discovery process begins when the unit is powered on. A [channel scanning notification](#)  in the top Status Bar indicates that the CyberScope 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 CyberScope has discovered.

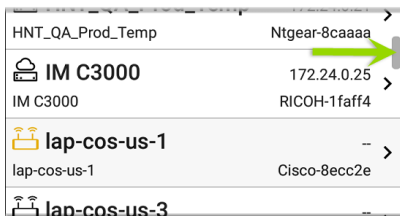
Discovery (589)		🔍	⋮
🔍	📏	Name	▼
	AndroLinkSysWav	10.250.2.147	>
	AndroLinkSysWav	Belkin-454655	
	Andromeda Automati...	10.250.3.224	>
	Andromeda Automation Procurve	HP-235cc0	
	Angela's EtherScope ...	10.250.2.139	>
	Angela's EtherScope nXG - 530000	NetAlly-530000	
	Cetus	10.250.2.166	>
	Cetus	Dell-faa680	
	Cisco2500WLC	10.250.3.235	>
	Cisco2500WLC	Cisco-556c80	
	cos-lab-ad.netally.eng	--	>
	cos-lab-ad.netally.eng	VMware-678cc2	
	COS_DEV_SW4	10.250.0.4	>
	COS_DEV_SW4	Dell-b63fb6	
	cos_dev_sw27_huawei	10.250.0.12	>

Discovery (22)		Q	⋮
📶	↑	Name	▾
 dlinkrouter	192.168.0.1	>	
dlinkrouter	D-LinkIn-4cc988		
 Kayes CyberScope - 5...	192.168.0.78	>	
Kayes CyberScope - 57C000	NetAlly-57c000		
 192.168.0.102	192.168.0.102	>	
192.168.0.102	SamsungE-32a93a		
 AmazonTe:74ecb2-b854cb	-	>	
AmazonTe:74ecb2-b854cb	AmazonTe-b854cb		
 ARRISGro:6c639c-ac404c	-	>	
ARRISGro:6c639c-ac404c	ARRISGro-ac404c		
 ARRISGro:c863fc-5b4f39	-	>	
ARRISGro:c863fc-5b4f39	ARRISGro-5b4f39		
 Espressi:ac67b2-49aabc	-	>	
Espressi:ac67b2-49aabc	Espressi-49aabc		

Like in AutoTest and other CyberScope 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, supports 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.

Total number of discovered devices

Discovery
Settings

Discovery (589)










Refresh
Discovery

Filter

Name

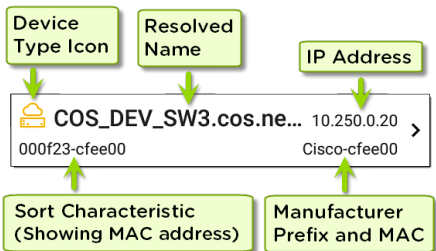
Sort

Touch
a card
to view
device
details.

	AndroLinkSysWav	10.250.2.147	>
	AndroLinkSysWav	kin-454655	>
	Andromeda Automati...	10.250.3.224	>
	Andromeda Automation Procurve	HP-235cc0	>
	Angela's EtherScope ...	10.250.2.139	>
	Angela's EtherScope nXG - 530000	NetAlly-530000	>
	Cetus	10.250.2.166	>
	Cetus	Dell-faa680	>
	Cisco2500WLC	10.250.3.235	>
	Cisco2500WLC	Cisco-556c80	>
	cos-lab-ad.netally.eng	-	>
	cos-lab-ad.netally.eng	VMware-678cc2	>
	COS_DEV_SW4	10.250.0.4	>
	COS_DEV_SW4	Dell-b63fb6	>
	cos_dev_sw27_huawei	10.250.0.12	>


Discovery List Cards

The information displayed on each device card varies depending on the selected Sort element and the data the CyberScope was able to discover.

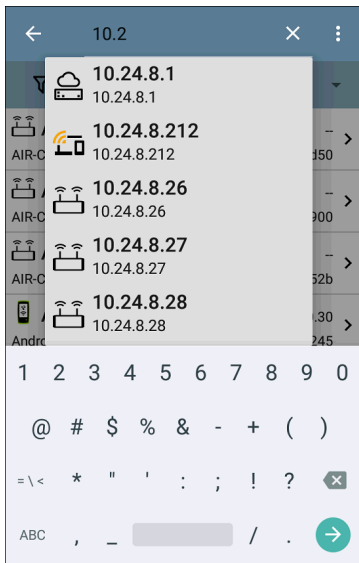


The lower left field displays the characteristic by which the Discovery list is currently sorted. In the image above, the list is sorted by MAC address. See [Discovery Sorts](#) in this topic for more about sorting.

Searching the Discovery List


The main Discovery screen offers a search feature. Tap the search icon  at the top of the

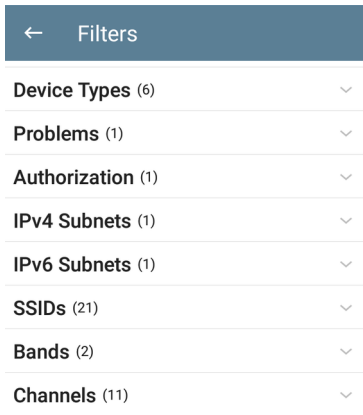
screen to search discovered devices.





Filtering the Discovery List

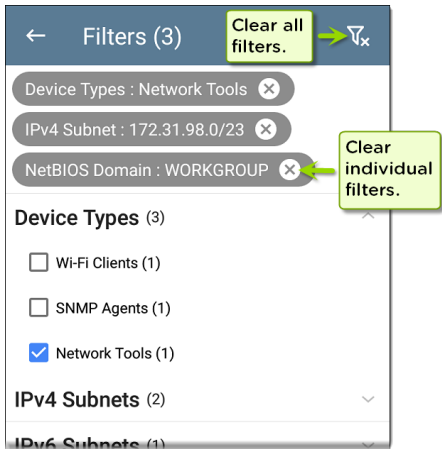
Tap the filter button  near the top left of the main Discovery screen to set filters that control which devices are displayed in the list.



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.

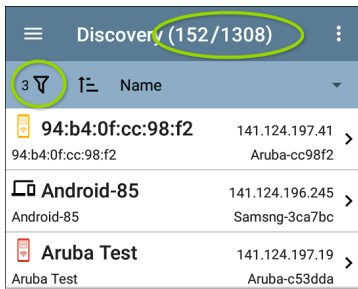
When filters are selected, those active filters are displayed at the top of the Filters screen.







- Tap the **X** 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.



Discovery (152/1308)	
3 	Name
 94:b4:0f:cc:98:f2	141.124.197.41 > 94:b4:0f:cc:98:f2 Aruba-cc98f2
 Android-85	141.124.196.245 > Android-85 Samsung-3ca7bc
 Aruba Test	141.124.197.19 > Aruba Test Aruba-c53dda

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).

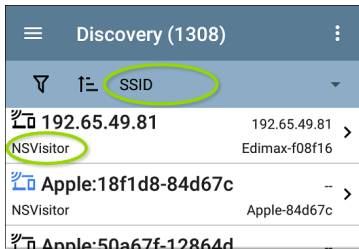
The number of active filters displays to the left of the filter icon (3 active filters in the image above).

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.

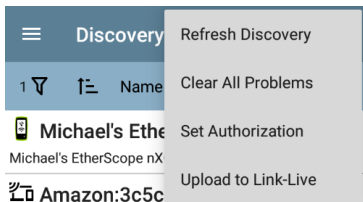
Security Auditing – Batch Authorization

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. In the example below, 38 devices belong to other offices and have an Unspecified authorization.

Set Authorization

38 of 226 devices selected

- Authorized (0)
- Neighbor (0)
- Flagged (0)
- Unknown (0)
- Unauthorized (0)
- Unspecified (38)

CANCEL

OK

NOTE: The initial selection on this screen defaults to the category with the highest count. If other categories have non-zero counts, select **OK** to change the authorization settings for all devices to the selected category.

Select the appropriate security category. To continue the example above, you can select **Neighbor**, and then tap the **OK** button to identify the Unspecified devices from other offices as Neighbor.

Set Authorization

38 of 226 devices selected

Authorized (0)

Neighbor (38)


Flagged (0)

Unknown (0)








Unauthorized (0)

Unspecified (0)

CANCEL **OK**

You can [filter](#) the list by tapping the Filter icon , tapping **Authorization**, and then tapping


Neighbor to show only the Neighbor devices. You can also [sort](#) the list by Authorization to display the discovered devices with the Neighbor category clearly identified.

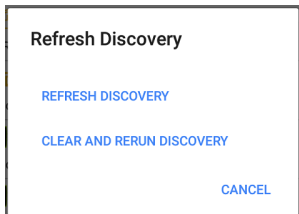
Discovery (79/276)		🔍	⋮
1	🔼	Authorization	▼
 AIR-CAP3702I-CO	-	>	
Neighbor		Cisco-000d53	
 AirCheck_G3_5500c4	10.250.2.236	>	
Neighbor		TRENDnet-eb8c72	
 BlackForestMist-Garage	-	>	
Neighbor		Mist-dd6dd2	
 den-colspr-ap2	-	>	
Neighbor		ExtremeN-01bae5	
 AmazonTe:dc91bf-938721	-	>	
Neighbor		AmazonTe-938721	
 Apple:6c7e67-d13251	-	>	
Neighbor		Apple-d13251	
 Apple:88665a-496103	-	>	
Neighbor		Apple-496103	

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. If Discovery is set to use Nmap tests, the Nmap results also upload.

**Link-Live**

by NetAlly



Discovery Snapshot Name

20190802_131842

Comment

1st Floor

Job Comment

Psych Building

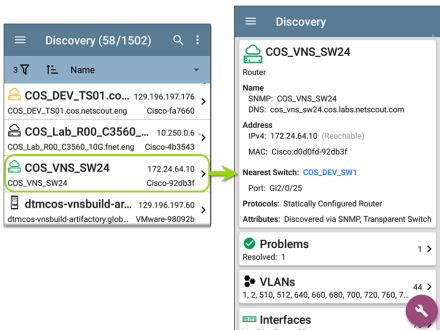
SAVE TO ANALYSIS FILES

See the [Link-Live chapter](#) for more information.


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 CyberScope was able to discover. In other words, only the discoverable information for each device is shown on the Details screen.

 **Discovery**


 **123.136.196.236**
Switch
Address
IPv4: 123.136.196.236 (Reachable)
IPv6: fe80::7ad2:94ff:fec0:e607
MAC: Ntgear:78d294-c0e607
Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 2 >
IPv4: 1 IPv6: 1 MAC: 1

 **VLANs** 3 >
1, 2, 3

 **Interfaces** 15 >
Up: 2 Down: 13

 **SNMP** >
Uptime: 11 weeks 1 day 5 hours 14 minutes



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 CyberScope, 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 CyberScope can discover.

Top Details Card

The top card on the Details screen summarizes the discovered data for the selected device.



 **Aruba Test**

Wi-Fi Controller

Name
SNMP: Aruba Test

Address
IPv4: 163.166.137.19 (Unassociated)
MAC: Aruba:186472-c53dda

Nearest Switch: [163.166.136.236](#)

Port: g1

Protocols: Statically Configured Router

Services: DHCP Server

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 CyberScope 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 screenshot shows the Discovery app interface. At the top, there is a blue header with a hamburger menu icon and the text "Discovery". Below the header, there is a white card with a grey border. The card contains the following information:

- Cisco3702** (with a yellow Wi-Fi icon)
- Lightweight AP
- Name**
 - AP: Cisco3702
 - SNMP: Cisco3702
- Address**
 - IPv4: 10.250.3.69 (Reachable)
 - IPv6: 2001:c001:c0de:500:ba38:61ff:fe6e:1ae0
 - MAC: [Cisco:b83861-6e1ae0](#)
- 802.11**
 - Channels: 1, 64
 - Type: 802.11ac
- Nearest Switch:** ~ [Unknown Switch 3](#) ~
- Wi-Fi Controller:** [Cisco2500WLC](#)
10.250.3.235
- Last Seen:** 5:23:20 PM

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

These fields may appear on the top card of a Device Details screen, depending on the device type and the information CyberScope discovered:

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

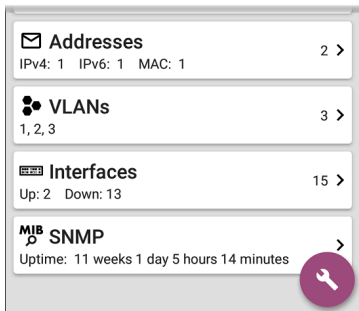
Guest OS: Operating system running on the virtual machine

Memory Reservation: Amount of memory reserved for the virtual machine

Last Seen: Time at which CyberScope most recently detected the device

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.

Addresses (3)		
↑	Address	▼
IPv4 10.250.0.1 10.250.0.120	BSSID	/22 549 >
IPv6 2001:c001:c0de 2001:c001:c0de	IP Address	... 549 >
IPv6 fe80::16 fe80::1618:77ff::	IPv6 Address	>
	Mfg-MAC Address	549 >
	MAC Address	

The rest of this topic provides examples of each type of Details screen and options for additional analysis.

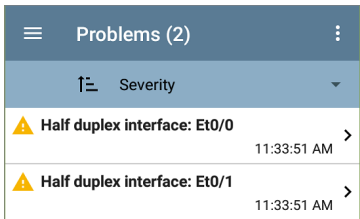
Remember, you can tap any card with a right pointing arrow ➤ to open a new screen with more information about the device or characteristic.

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.

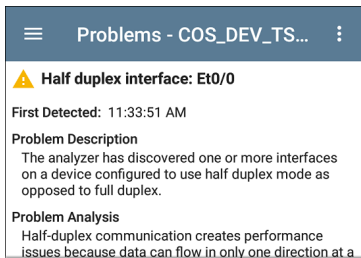


Tap the Problems card to view the Problems list screen (unless only 1 Problem is detected, in which case, the detailed Problem description opens, skipping the list screen).




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.

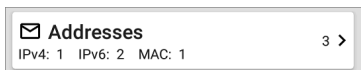


The screenshot shows a mobile application interface with a dark blue header bar. On the left is a hamburger menu icon, and on the right is a vertical ellipsis (three dots) icon. The header text reads "Problems - COS_DEV_TS...". Below the header, a yellow warning triangle icon is followed by the text "Half duplex interface: Et0/0". Underneath this, it says "First Detected: 11:33:51 AM". The section is titled "Problem Description" and contains the text: "The analyzer has discovered one or more interfaces on a device configured to use half duplex mode as opposed to full duplex." Below that, it is titled "Problem Analysis" and contains the text: "Half-duplex communication creates performance issues because data can flow in only one direction at a".

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 screenshot shows a mobile application interface with a light gray header bar. On the left is an envelope icon followed by the text "Addresses". On the right is the text "3 >". Below the header, it says "IPv4: 1 IPv6: 2 MAC: 1".

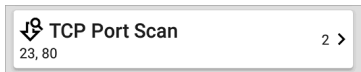
The Addresses card displays the number of each type of address discovered: IPv4, IPv6, MAC, and/or BSSID. Tap to view the addresses and related information.

≡ Addresses (3)	
↑ ≡ Address	▼
IPv4 10.250.0.120 10.250.0.120	10.250.0.0/22 Dell-3b5649 >
IPv6 2001:c001:c0de:500:1618:77f... 2001:c001:c0de:500:1618:77ff:fe3b:...	Dell-3b5649 >
IPv6 fe80::1618:77ff:fe3b:5649 fe80::1618:77ff:fe3b:5649	Dell-3b5649 >

From the Addresses list screen, you can sort the list order and tap any of the discovered addresses to investigate the address further.

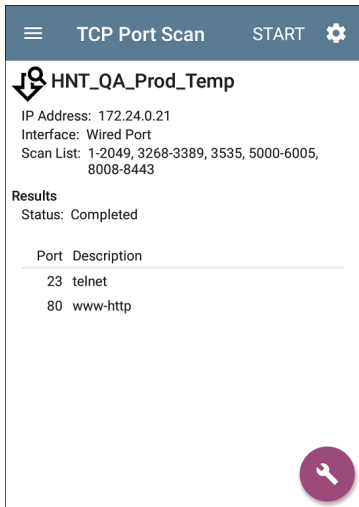
TCP Port Scan

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 screenshot shows the 'TCP Port Scan' results screen. At the top, there is a dark blue header with a hamburger menu icon on the left, the title 'TCP Port Scan' in the center, and the word 'START' and a gear icon on the right. Below the header, the device name 'HNT_QA_Prod_Temp' is displayed with a downward-pointing arrow icon. The scan details are listed: 'IP Address: 172.24.0.21', 'Interface: Wired Port', and 'Scan List: 1-2049, 3268-3389, 3535, 5000-6005, 8008-8443'. A 'Results' section follows, with 'Status: Completed'. Below this is a table with two columns: 'Port' and 'Description'. The table contains two entries: port 23 for 'telnet' and port 80 for 'www-http'. In the bottom right corner of the screen, there is a purple circular button with a white wrench icon.

☰ TCP Port Scan START ⚙

↓ HNT_QA_Prod_Temp

IP Address: 172.24.0.21
Interface: Wired Port
Scan List: 1-2049, 3268-3389, 3535, 5000-6005, 8008-8443

Results
Status: Completed

Port	Description
23	telnet
80	www-http

🔧

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

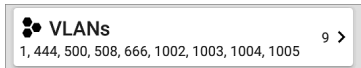
Status: Current status of the port scan

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.

COS_DEV_SW33	
 VLANs	
VLAN	Description
1	default
444	VLAN0444
500	VLAN0500
508	LabWiFi
666	VLAN0666
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

The VLANs Details screen also shows the description with each VLAN ID.

Interfaces

Interface are discovered using SNMP.

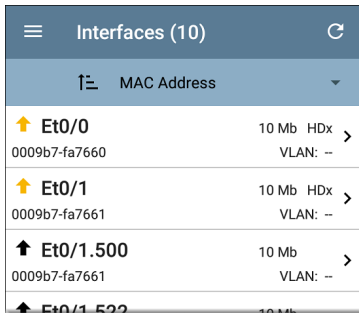
 Interfaces	171 >
Up: 20 Down: 151	

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.

Interfaces (171)		↻
↑	Interface Status	▼
↑	VLAN-1002 Status: up	0 b VLAN: 1002 >
↑	VLAN-1003 Status: up	0 b VLAN: 1003 >
↑	VLAN-1005 Status: up	0 b VLAN: 1005 >
↓	Fa1 Status: down	100 Mb VLAN: -- >
↓	Gi1/3 Status: down	1 Gb FDx VLAN: 1 >

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.



The screenshot shows a mobile application interface for network discovery. At the top, there is a header bar with a hamburger menu icon on the left, the text "Interfaces (10)" in the center, and a refresh icon on the right. Below the header is a filter bar with a list icon and the text "MAC Address" followed by a dropdown arrow. The main content is a list of network interfaces, each with a status icon (upward arrow), name, MAC address, speed, type, and VLAN information, along with a right-pointing chevron for more details.

MAC Address	Speed	Type	VLAN
0009b7-fa7660	10 Mb	HDx	--
0009b7-fa7661	10 Mb	HDx	--
0009b7-fa7661	10 Mb		--
0009b7-fa7661	10 Mb		--

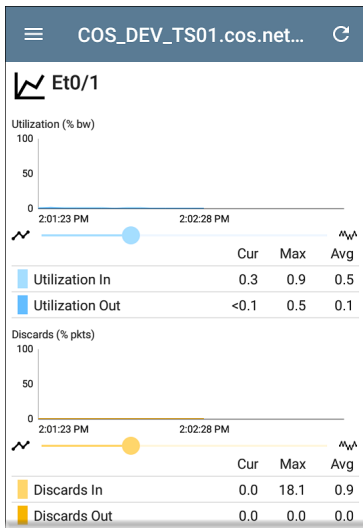
Tap an Interface row to open a new Discovery Details screen for that Interface.

The screenshot shows a mobile application interface for network discovery. At the top, there is a blue header bar with a hamburger menu icon on the left, the text "COS_DEV_TS01.cos.net..." in the center, and a refresh icon on the right. Below the header, the main content area is divided into three sections. The first section is titled "Et0/1" with an upward-pointing arrow icon. It contains the text "DOT1Q Trunk to CISCO_3750_PoE COS_DEV_SW2 f...", "Status: up", "Speed: 10 Mb", "Duplex: HDx", "MTU: 1500", "Connected Device: COS_DEV_SW1", "Port: Gi2/0/30", and "Address" with "MAC: Cisco:0009b7-fa7661". The second section is titled "Devices" with a folder icon and shows "0" devices with a right-pointing arrow. The third section is titled "Statistics" with a line graph icon and shows "Util: 0.3 %", "Discards: 0.0 %", and "Errors: 0.0 %" with a right-pointing arrow.

The Interface Details screen contains a description of the interface and information about its Status, Connected Device and Port, and Address.

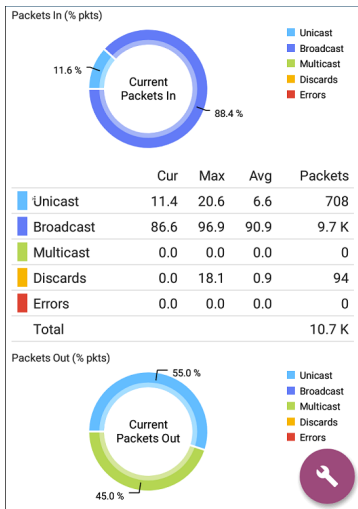
MTU: Maximum Transmission Unit, the maximum packet frame size configured on the interface port

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

 **MIB SNMP**

Uptime: 5 weeks 6 days 2 hours 57 minutes



This card shows SNMP Uptime. Tap the card for additional details.



COS_DEV_SW34

 **MIB SNMP**
SNMP System Group

Uptime: 5 weeks 6 days 2 hours 58 minutes

Manufacturer: Cisco

Model: cat4500e

Serial Number: FOX1407GRJA

HW Version: V02

SW Version: 15.2(2)E7

Description:

Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-ENTSERVICES-M), Version 15.2(2)E7, RELEASE SOFTWARE (fc3)

Technical Support:

<http://www.cisco.com/techsupport>

Copyright (c) 1986-2017 by Cisco Systems, Inc.

Compiled Wed 12-Jul-17 14:36 by

SNMP

Type: SNMP v1/v2/v3

Engine ID: 80000009030068efbd6f4b80

Communication: SNMP v2

Using: Default Community String: public

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 CyberScope 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 CyberScope may be unable to directly identify the connected switch, the devices connected to it provide clues about where the switch is operating.




 **Connected Devices**

8 >

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.


Connected Devices (8)		
 IP Address		
 10.250.2.143	--	>
10.250.2.143	NetAlly-02506e	
 10.250.2.177	--	>
10.250.2.177	TRENDn-af1e30	
 10.250.3.32	--	>
10.250.3.32	NetAlly-0210...	

Resources

 **Resources** >
CPU: 28% Memory: 35%

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.

COS_DEV_SW34		
 Resources		
	Cur	Max
CPU %	12	12
Memory %	60	60
Last Update: 1:44:22 PM		

By default, CyberScope 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.

Cisco2500WLC		
SSIDs		
SSID	Security	VLAN
✓ CiscoQATest-maana	WPA2-P, WPA-P	--
✓ Cisco WEP64 OA	WEP	--
✓ aa-Cisco-Wep	WEP	--
✓ aonly	WPA2-P, WPA-P	--
✓ Cisco ISE	WPA2-E	--
✓ RF Chamber	WPA2-P, WPA-P	--
✓ Lobo	WPA2-P, WPA-P	--
✓ COS Cisco Captive Portal	Web	--
✗ Portal Test	Web	--
✓ [Cisco Hidden]	WPA2-P	--
✓ Cisco 2.4G	WPA2-P	--

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.



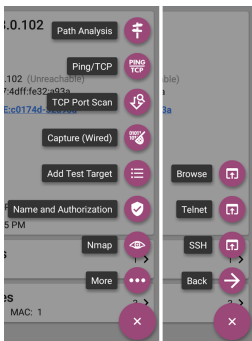
Discovery App Floating Action Menu

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](#), [Capture](#), or [Nmap](#) 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 that avoids making you retype the target addresses or hostnames in other testing apps.

- Tap **Nmap** to add an Nmap test. See [Adding Nmap Tests Using the FAB](#) for more



information.

- Tap **TCP Port Scan** to open the [TCP Port Scan screen](#) in the Discovery app.
- 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 **Browse** to open the Chromium browser.
 - Tap [Telnet or SSH](#) to open the JuiceSSH app.


- Tap **Back** to return to the primary FAB list.


Adding Nmap Tests Using the FAB

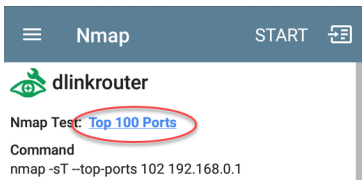
Using the FAB menu to create additional Nmap tests for Discovery allows you to add and modify tests, allowing you to fine-tune test settings and collect additional Nmap information.

To add or edit an Nmap test:


1. Tap a device on the main discovery list screen to open the details screen for the device. This screen includes any existing Nmap tests already set up for the device.
2. Create a new Nmap test:
 - a. Tap the **FAB** button.
 - b. Select **Nmap** to open the list of available Nmap tests.
 - c. Select a test, and then tap **OK**. This runs the test and opens a new summary card for the test on the device details screen.

(The icon  indicates the test was added using the FAB.)

3. Tap the summary card to view the test results.
 - To automatically scroll to the next green, yellow, or red highlighted text in the output, tap the Next Result icon  in the screen header. (See [Nmap Output](#) for more details.)
4. To adjust the test settings, tap the blue hyperlink at the top of the results screen.



This opens the [Nmap Test](#) screen, from which you can change the Nmap settings.


5. Tap the system Back icon  to return to the results screen.


6. To run the modified test, tap **START**. This activates the STOP button while the test is running.
7. (Optional) Tap **STOP** while the test is running to halt the test. You can then adjust test settings without having to wait for a lengthy test to finish.
8. (Optional) Repeat this procedure step to add or edit additional tests.

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).

 **Discovery**

 **Rack5SW1.fnet.eng**
Router


Name
SNMP: Rack5SW1.fnet.eng


Address
IPv4: 10.250.3.207 (Reachable)
MAC: Cisco:00141c-8945c1



Nearest Switch: [COS_DEV_SW1](#)
Port: Gi2/0/39

Protocols: Statically Configured Router

Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 6 >
IPv4: 6 MAC: 5

 **VLANs** 66 >
1, 2, 21, 42, 78, 85, 154, 202, 236, 378, 478, 5...

 **Interfaces** 
Up: 12 Down: 30

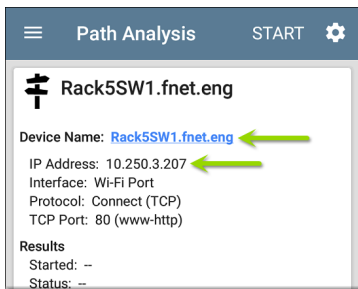
When you open the FAB and select a different app, such as Path Analysis, only the address and name listed at the top of the Details screen are populated in the Path Analysis app.




 **Rack5SW1.fnet.eng**
Router

Name
SNMP: Rack5SW1.fnet.eng ←

Address
IPv4: 10.250.3.207 (Reachable) ←
MAC: Cisco:00141c-8945c1



☰ **Path Analysis** START ⚙️

 **Rack5SW1.fnet.eng**

Device Name: [Rack5SW1.fnet.eng](#) ←

IP Address: 10.250.3.207 ←

Interface: Wi-Fi Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)

Results
Started: --
Status: --

To open another screen or app with a different address, open the Addresses card, and select another address to view its Details screen.

Device Types

The Discovery app lists and analyzes the types of devices explained in this section. Different data may be available to the CyberScope 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 show examples of data that Discovery may display for each device type.

Routers

CyberScope discovers IP routers by monitoring traffic and querying hosts.

 **Discovery**

 **COS_DEV_SW34**

Router

Name
SNMP: COS_DEV_SW34


Address
IPv4: 10.250.0.34 (Reachable)
MAC: Cisco:68efbd-6f4bbf

Nearest Switch: [Rack5SW1.fnet.eng](#)


Port: Gi1/0/11
VLAN ID: 500

Protocols: Statically Configured Router


Attributes: Discovered via SNMP, Transparent Switch


 **VLANs** 17 >

1, 244, 500, 801, 803, 804, 805, 806, 825, 830...

 **Interfaces** 171 >


Up: 20 Down: 151


 **SNMP** >



Switches

Switches are also discovered by monitoring traffic and querying hosts.

 **Discovery**


 **cos-dev-sw18-poe**

Switch


Name
SNMP: cos-dev-sw18-poe

Address
IPv4: 10.250.3.216 (Reachable)
MAC: Cisco:503de5-220c43


Attributes: Discovered via SNMP, Transparent Switch

 **Addresses** 2 >



IPv4: 2 MAC: 2

 **VLANs** 37 >

1, 11, 196, 500, 502, 504, 508, 510, 511, 518, ...

 **Interfaces** 38 >

Up: 9 Down: 29

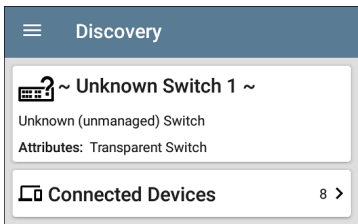
 **SNMP** 

Uptime: 27 weeks 2 days 7 hours 25 minutes

Unknown Switches

Unknown switches are detected indirectly by analyzing traffic going through surrounding switches. The CyberScope 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 CyberScope 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.

☰
Discovery



Compass.netally.eng

Network Server

Name
 Virtual Machine: [Compass.netally.eng](#)
 DNS: [compass.fnet.eng](#)
 NetBIOS: COMPASS

Address
 IPv4: 10.250.3.221 (Reachable)
 IPv6: 2001:c001:c0de:500:d1f5:d8e0:a81:3397
 MAC: VMware:000c29-13235b

Nearest Switch: ~ [Unknown Switch 4](#) ~

Hypervisor: [COS-PNT-VM.fnet.eng](#)
 10.250.3.251

Virtual Machine
 Guest OS: Windows Server 2008 Standard Edition,
 32-bit Service Pack 2 (Build 6003)
 Memory Reservation: 2,048MB

Services: DNS, Virtual Machine





 **Addresses**

IP 1 1 IP 6 0 MAC 0

Hypervisors

VMware hypervisors are discovered via SNMP. The hypervisor's SNMP agent must be enabled for the CyberScope to discover it and classify it as a hypervisor.

 **Discovery**

 **COS-PNT-VM.fnet.eng**

Hypervisor

Name
SNMP: COS-PNT-VM.fnet.eng



Address
IPv4: 10.250.3.251 (Reachable)
IPv6: fe80::1618:77ff:fe34:db2a
MAC: Dell:141877-34db2a

Nearest Switch: ~ **Unknown Switch 4** ~

Hypervisor
Product Name: VMware ESXi
Product Version: 6.7.0
Product Build: 13644319
Memory: 98207MB
CPUs: 2
Virtual Machines: 16

Services: Hypervisor

Attributes: Port Aggregation

 **Addresses** 

IPv4: 1 IPv6: 1 MAC: 1

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.

☰ **Discovery**

 **Cisco ACS 5.8 Linux**

Virtual Machine

Name
Virtual Machine: Cisco ACS 5.8 Linux

Address
IPv4: 10.250.0.59 (Reachable)
IPv6: 2001:c001:c0de:500:20c:29ff:fe0b:e61c
MAC: VMware:000c29-0be61c

Nearest Switch: ~ Unknown Switch 4 ~

Hypervisor: COS-PNT-VM.fnet.eng
10.250.3.251

Virtual Machine
Guest OS: Linux 2.6.32-431.20.3.el6.x86_64 Red Hat Enterprise Linux Server release 6.4 (Santiago)
Memory Reservation: 4,096MB


Services: Virtual Machine


 **Addresses**
IPv4: 1 IPv6: 2 MAC: 1



Wi-Fi Controllers

CyberScope can discover SNMP enabled Wi-Fi controllers, including Cisco and Aruba Wi-Fi Controllers.


 **Discovery**


 **Cisco2500WLC**
Wi-Fi Controller


Name
SNMP: Cisco2500WLC



Address
IPv4: 10.250.3.235 (Reachable)
"MAC: Cisco:ece1a9-556c80

Attributes: Discovered via SNMP, Transparent Switch
AP Capacity: 75

 **APs** 2 >

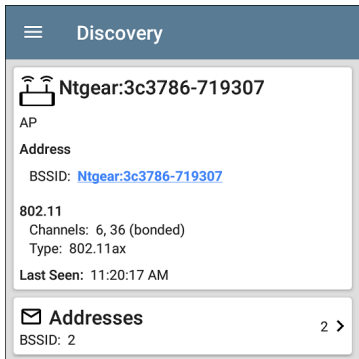
 **SSIDs** 16 >

 **VLANs** 1 >
1

 **Interfaces** 
Up: 2 Down: 3


Access Points (APs)

The CyberScope discovers APs through wireless packet analysis and SNMP queries with a linked connection through a management or test port.



The screenshot shows the 'Discovery' section of the app. At the top, there is a blue header with a hamburger menu icon and the word 'Discovery'. Below this, a card displays information for an AP. The card has a white background and a grey border. It starts with a Wi-Fi icon and the text 'Ntgear:3c3786-719307'. Below that, it says 'AP'. Under the heading 'Address', it lists 'BSSID: [Ntgear:3c3786-719307](#)'. Further down, it shows '802.11' with sub-entries 'Channels: 6, 36 (bonded)' and 'Type: 802.11ax'. At the bottom of this card, it says 'Last Seen: 11:20:17 AM'. Below the main card, there is another section titled 'Addresses' with an envelope icon, showing 'BSSID: 2' and a '2 >' indicator.

Discovery

 Ntgear:3c3786-719307

AP

Address


BSSID: [Ntgear:3c3786-719307](#)

802.11

Channels: 6, 36 (bonded)

Type: 802.11ax

Last Seen: 11:20:17 AM

 **Addresses** 2 >


BSSID: 2

See also [APs in the Wi-Fi analysis app](#).

Wi-Fi Clients

Wireless clients are discovered through wireless packet analysis and SNMP queries with a linked connection through a management or test port.

☰ Discovery

 **Samsng:4c6641-701864**

Wi-Fi Client

Address

MAC: [Samsng:4c6641-701864](#)


802.11

Channels: 60
Type: 802.11ac

AP: [lap-cos-us-1](#)

SSID: NSVisitor
Security: WPA2-P

Last Seen: 11:15:45 AM

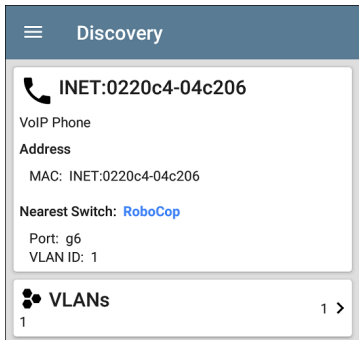
 **Problems** 1 >

Warnings: 1

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.



The screenshot shows the Discovery App interface. At the top is a dark blue header with a hamburger menu icon on the left and the word "Discovery" in white. Below the header is a white card with a grey border. The card contains a phone icon, the text "INET:0220c4-04c206", and the label "VoIP Phone". Underneath is the "Address" section with "MAC: INET:0220c4-04c206". The "Nearest Switch" is listed as "RoboCop" in blue. Below that, "Port: g6" and "VLAN ID: 1" are shown. At the bottom of the card is a "VLANs" section with a cluster icon, the number "1", and a right-pointing arrow.

Discovery

 **INET:0220c4-04c206**


VoIP Phone

Address

MAC: INET:0220c4-04c206


Nearest Switch: [RoboCop](#)


Port: g6
VLAN ID: 1


 **VLANs** 1 >


Printers


The CyberScope identifies IP printers via the SNMP Printer MIB and IPX printers via diagnostic requests and queries.


 **Discovery**


 **TOSHIBA e-STUDIO3005AC**
Printer
Name
SNMP: TOSHIBA e-STUDIO3005AC
mDNS: MFP12073521
NetBIOS: MFP12073521
Address
IPv4: 143.131.143.43 (Reachable)
IPv6: fe80::280:91ff:feb8:3a31
MAC: Tokyo:008091-b83a31

 **Problems** 1 >
Warnings: 1

 **Addresses** 3 >
IPv4: 1 IPv6: 2 MAC: 1

 **Interfaces** 2 >
Up: 2 Down: 0


 **SNMP**




SNMP Agents

SNMP agents are discovered using SNMP queries. See [SNMP Configuration](#).

NOTE: If CyberScope 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](#).


 **Discovery**

 **LAB Sensor 1**
SNMP Agent

Name
SNMP: LAB Sensor 1

Address
IPv4: 10.250.0.76 (Reachable)
MAC: HWServ:000a59-022933







Nearest Switch: [JuniperEX2200](#)
Port: ge-0/0/23

MIB **SNMP** 
Uptime: 6 days 4 hours 29 minutes

See also [SNMP Details](#).

Network Tools


The CyberScope can also identify other NetAlly network testers (CyberScope, AirCheck G2, OneTouch AT, LinkRunner (AT and G2), and Test Accessory).

Discovery (122/708)		
1	Device Type	
 fe80::2c0:17ff:fe53:138	EtherScope nXG	NetAlly-530138
 fe80::2c0:17ff:fe53:146	EtherScope nXG	NetAlly-530146
 10.250.3.147	AirCheck G2	NetAlly-350593
 NetAlly:00c017-353246	AirCheck G2	NetAlly-353246
 10.250.2.117	LinkRunner G2	NetAlly-c50070
 10.250.2.132	Test Accessory	NetAlly-330e87

The image above shows several NetAlly tools as they appear in the main Discovery list.

CyberScope displays all the information it can gather about each tool on the Details screen.

☰
Discovery



10.250.2.240


LinkRunner G2

Address

IPv4: 10.250.2.240 (Reachable)
 IPv6: fe80::2c0:17ff:fec5:88
 MAC: NetAlly:00c017-c50088

Nearest Switch: [PV_Mike_NetgearGS110TP](#)


Port: g6
 VLAN ID: 500



Addresses

2 >

IPv4: 1 IPv6: 1 MAC: 1




VLANs


1 >

500

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.

 **Discovery**


 **ubuntu**


Host/Client

Name
mDNS: ubuntu

Address
IPv4: 10.250.2.109 (Reachable)
IPv6: 2001:c001:c0de:500:b844:4388:4fb7:4506
MAC: ORICO:f01e34-1fbaa4

Nearest Switch: [PV_Mike_NetgearGS110TP](#)
Port: g3
VLAN ID: 500

 **Addresses** 4 >
IPv4: 1 IPv6: 3 MAC: 1

 **VLANs** 1 >
500

NOTE: A MAC address that begins with LocalAdm indicates that the address has been locally randomized to prevent unauthorized tracking.



Discovery

**localAdm:227367-a99246**

Wi-Fi Client

AddressMAC: [localAdm:227367-a99246](#)**802.11**

Channels: 48

Type: --

AP: [localAdm:decbac-51a778](#)

SSID: ngenius&sniffer

Security: WPA2-E

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 CyberScope 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:

Wi-Fi - BSSIDs (150)		
Filter	Sort	Authorization
	Ntgear:3c3786-719306	-33 dBm >
Unauthorized	Nighthawk 802.11ax 5GHz	CH: 36
	Cisco:b83861-84aaf0	-82 dBm >
Neighbor	Cisco WEP64 SA	CH: 36
	Cisco:b83861-84aaf0	-67 dBm >
Neighbor	CiscoQATest-mañana	CH: 1
	Cisco:78bc1a-0fd908	-64 dBm >
Authorized	[NGP-004]	CH: 36

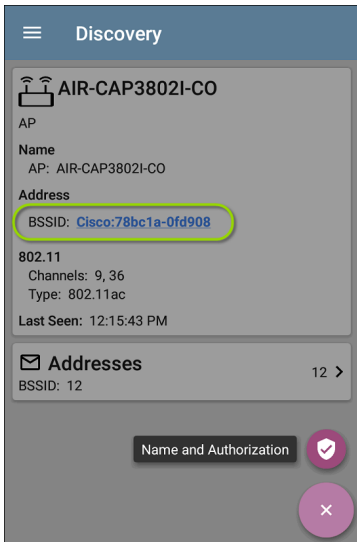
Applying a Name and/or Authorization

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.

Name and Authorization

MAC Address: Cisco:78bc1a-0fd908

User Name: Conference Room AP

Authorization

Authorized

Neighbor

Flagged

Unknown

Unauthorized

Unspecified

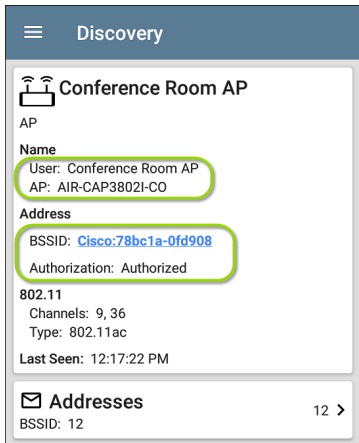
CANCEL OK

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 screenshot shows the 'Discovery' app interface. At the top, there is a blue header with a hamburger menu icon and the word 'Discovery'. Below the header, there is a card for 'Conference Room AP'. The card contains the following information:

- AP**
- Name**
 - User: Conference Room AP
 - AP: AIR-CAP3802I-CO
- Address**
 - BSSID: [Cisco:78bc1a-0fd908](#)
 - Authorization: Authorized
- 802.11**
 - Channels: 9, 36
 - Type: 802.11ac
- Last Seen: 12:17:22 PM

At the bottom of the card, there is a section for 'Addresses' with an envelope icon, the text 'Addresses', and a right arrow. Below this, it says 'BSSID: 12'.

The user-assigned name for the AP and Authorization for the BSSID also appear on the Wi-Fi BSSID Details screen, as shown below.

Wi-Fi - BSSID

 **Cisco:78bc1a-0fd908**
BSSID

SSID: [AmNaCa](#)

AP: [Conference Room AP](#)
BSSID: 78bc1a-0fd908
Authorization: Authorized

802.11

Channel: [9](#)

Types: n, g, b
Signal: -60 dBm
SNR: 33 dB
Security Type: WPA2-P

Last Seen: 2:30:38 PM

↑↓ Rates and Capabilities >

📶 Clients 0 >





📈 RF and Traffic Statistics >

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.

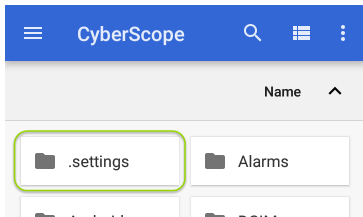
To view all assigned Authorizations for a device, open the Discovery or Wi-Fi Details screen for the device and view the Addresses or BSSIDs screen. Then, sort by Authorization.


Addresses (14)		
Authorization		
 Cisco:b83861-84aaf3	CH: 36	>
Flagged	Cisco WEP128 OA	
 Cisco:b83861-84aaf1	CH: 1	>
Neighbor	Cisco WEP64 OA	
 Cisco:b83861-84aafc	CH: 1	>
Authorized	Cisco WEP128 OA	
 Cisco:b83861-84aaf0	CH: 1	>
Neighbor	Cisco WEP64 OA	

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 CyberScope'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 folder and sub-folders, as shown above.

If desired, you can manually edit this file on the CyberScope unit, or you can create a new authname.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 CyberScope 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:

 Who is this?	-38 dBm >
Flagged	Sonicw


To edit the authname.txt file on the CyberScope, third-party apps, such as QuickEdit Text Editor, are available from the NetAlly [App 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**.



Discovery



Discovery Settings



Problem Settings



TCP Port Scan Settings



General Settings



Feature Access



About



(Tap here to skip to [Problem Settings](#), [TCP Port Scan](#), or back to [General Settings](#).)


Discovery Settings	
Active Discovery Ports	All
Extended Ranges	0 Extended Ranges >
ARP Sweep Rate	100/second
Refresh Interval	90 minutes
SNMP	SNMPv1/v2: Enabled, SNMPv3: Enabled >
Nmap	Nmap: Enabled, Custom: Enabled >

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.

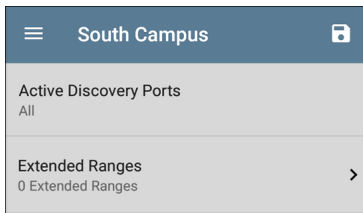
2. When you finish configuring, tap the back button  to return to the main [Discovery List screen](#).
3. Then, [Refresh Discovery](#) from the action overflow menu  to apply the new configuration.

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

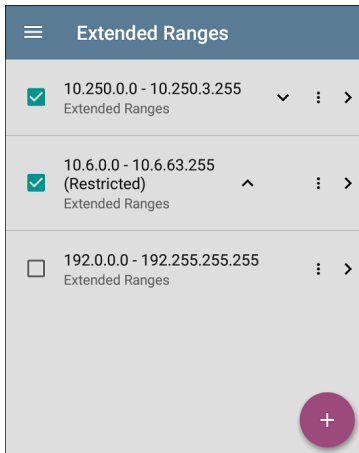
The Extended Ranges screen allows you to enter addresses of non-local subnets on which you want the Discovery process to run. Discovery sweeps all of the enabled Extended Ranges for devices, whether directly connected or off-net. The CyberScope performs Ping sweeps on subnets that are not directly connected 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 CyberScope always discovers management subnets, regardless of your network port connections.

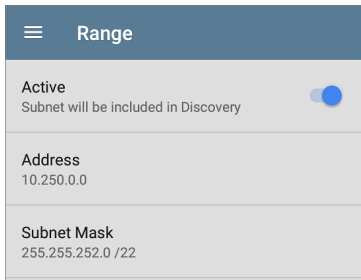
Tap the field to open the Extended Ranges list screen.



- 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.

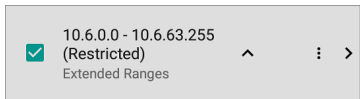


Range	
Active	<input checked="" type="checkbox"/>
Subnet will be included in Discovery	
Address	10.250.0.0
Subnet Mask	255.255.252.0 /22

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 CyberScope 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 CyberScope 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 CyberScope 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 CyberScope 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.

Community Strings	
<input checked="" type="checkbox"/>	cos dev sw1 Community Strings
<input checked="" type="checkbox"/>	Default Community String: public Community Strings
<input type="checkbox"/>	Default Community String: private Community Strings


The CyberScope 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 CyberScope 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.

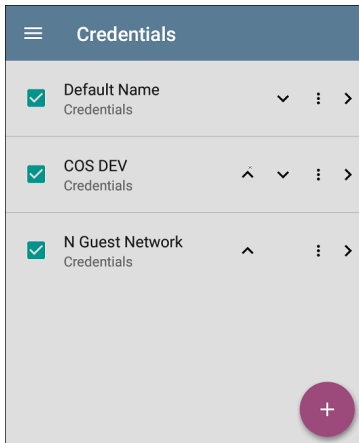
SNMPv3

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 CyberScope 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. CyberScope 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.

Credential Sets	
Name	Default Name
Username	
Authorization Type	None
Authorization Password	
Privacy Type	None
Privacy Password	

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

CyberScope Discovery supports two SNMPv3 Authorization types: HMAC-SHA and HMAC-MD5. If Authorization is required, enter the appropriate password.

Privacy Type and Password

CyberScope 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 CyberScope 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 CyberScope 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, CyberScope 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.

Devices Discovered Through Other Devices

- Routers and Subnets
- Switches
- VoIP Devices
- Wi-Fi Clients
- Virtual Machines

CANCEL

OK

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 CyberScope is reading the CDP and LLDP caches of one switch, it contains other switches. If this option is enabled, the CyberScope 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](#).

Nmap Tests

Tap this field to open the Nmap settings.

Run Test Against Each Device (Nmap Section)

Tap this field to enable or disable Nmap tests to run against each device discovered. (Shows or hides the Nmap Test field.)

Nmap Tests

(Displayed only if the Nmap option for Run Tests Against Each Device is enabled.) Tap this field to open a selection list of Standard Nmap Tests.

(This list contains standard Nmap tests that are check-marked in the [main Nmap Tests screen](#).)

Run Tests Against Each Device (Custom Discovery Section)

Tap this field to enable or disable custom Discovery tests to run against each device discovered. (Shows or hides the Custom Discovery Tests field.)

Custom Discovery Tests

(Displayed only if the Custom Discovery option for Run Tests Against Each Device is enabled.) Tap this field to open a selection list of Custom Discovery Tests. (This list contains Custom Discovery Tests that are check-marked in the [main Nmap Tests screen](#).)

Auto AP Grouping Rules

Auto AP Grouping Rules
6 AP Grouping Rules




This feature allows you to adjust the AP Grouping Rules that control how the CyberScope

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 CyberScope. The **Prefix filters** in all of the default grouping rules are set to 000000-000000.

AP Grouping Rules			
<input checked="" type="checkbox"/>	Grouping 1 FFFFFFFFFFC0	▼	⋮ >
<input checked="" type="checkbox"/>	Grouping 2 00FFFFFFFFFF	▲ ▼	⋮ >
<input checked="" type="checkbox"/>	Grouping 3 FFFFFF0FFFFF	▲ ▼	⋮ >
<input checked="" type="checkbox"/>	Grouping 4 00FF0FFFFFFF	▲ ▼	⋮ >
<input checked="" type="checkbox"/>	Grouping 5 0DFFFFFF0FFFF	▲ ▼	⋮ >
<input checked="" type="checkbox"/>	Grouping 6 F0FFFFFFFFF0	▲	⋮ >



As with other settings list screens, 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.

AP Grouping Rules	
Name	Grouping 1
Prefix filter	000000000000
Filter mask	FFFFFFFFFC0

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 with BSSIDs that all start with b83861. By specifying a Prefix filter of 003861-000000, you limit the grouping rule to just those APs.

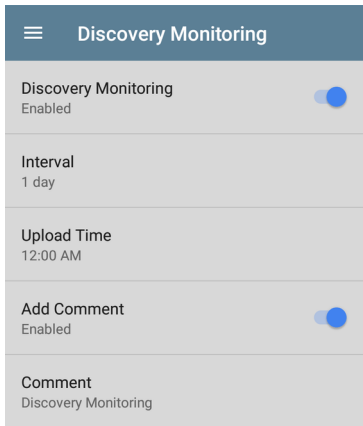
Filter mask

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 FFFFFFFF-FFFFC0, so any BSSIDs that vary only by the lower six bits are grouped together.

Discovery Monitoring

Monitoring allows Discovery to periodically collect updated network information and send network snapshots to Link-Live. You can then use the Discovery Difference and Monitoring features in the Link-Live Analysis tab to detect changes. This feature can help update Discovery at times of peak activity or detect the addition of a new device, for example.



Discovery Monitoring Option

Discovery Monitoring is disabled by default. Tap the toggle button to enable Discovery Monitoring and display the configuration fields.

Interval

(Appears only if Discovery Monitoring is enabled.) Tap **Interval** to open a selection menu

to choose a time interval in days or to enter a custom value. This controls the time interval between Discovery network snapshots sent to Link-Live.

Upload Time

(Appears only if Discovery Monitoring is enabled.) Tap **Upload Time** to open a selection menu to choose the time of day at which a Discovery network snapshot is sent to Link-Live.

Add Comment


Tap **Add Comment** to enable the Comment field.

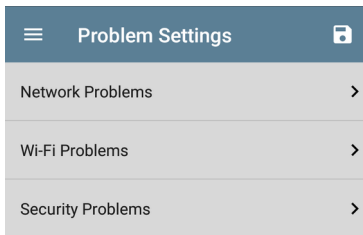
Comment

(Appears only if Add Comment is enabled.) Tap this field to open a text box to enter a comment for the monitoring activity.

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**.

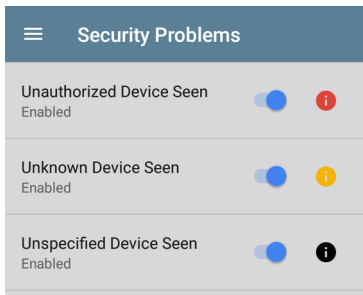


Problems are categorized as Network, Wi-Fi, or Security.




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.

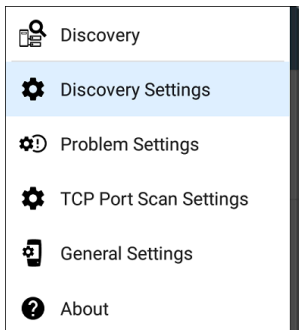
- Tap the red  , yellow  , or black  information icons to the right of each Problem to read a detailed description and recommended actions.
- **Red** icons indicate Failure conditions.
- **Yellow** icons indicate Warning conditions.
- Black icons indicate that the Failure or Warning status is determined by the [Nmap app](#).

When you finish configuring, tap the back button  to return to the main Discovery screen.

TCP Port Scan Settings

The TCP Port Scan feature checks for open ports on the current device. To run scan, tap the **FAB** on the **Discovery Details** screen, and then tap **TCP Port Scan**. The CyberScope 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.

TCP Port Scan Settings	
Interface	Any Port
Scan List	1-2049, 3268-3389, 3535, 5000-6005, 8008-8443
Timeout Threshold	1 s

Interface: Tap the field to select the CyberScope 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 CyberScope 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 CyberScope, and measurements update with each channel scan cycle.

The CyberScope supports 802.11a/b/g/n/ac/ax technologies. CyberScope 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](#)


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.

When CyberScope links to a network, 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 Screens

To switch between the different Wi-Fi app screens, tap the menu icon  (or swipe right) to open the left-side [navigation drawer](#).



Channels Map



Channels (10 active)



SSIDs (13)



APs (9)



BSSIDs (27)



Clients (27)



Bluetooth (16)



General Settings



Feature Access





About

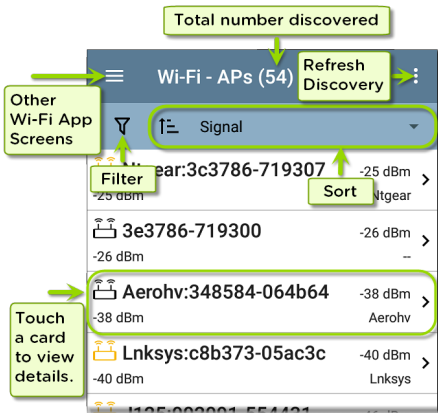
The Wi-Fi app's navigation drawer displays a real-time count (in parentheses) of each wireless component CyberScope has detected. Tap an option to open the corresponding screen.

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:

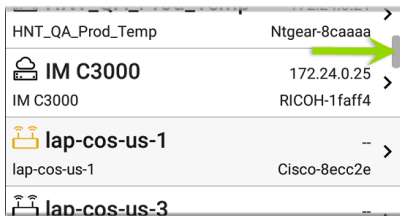


As with AutoTest and other CyberScope screens, the icons in Wi-Fi analysis change color to indicate a **Warning** or **Failure** condition. The app also displays icons in **Blue** to indicate Problem-related information that does not constitute a warning or failure, and **Green** to indicate that a previous 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

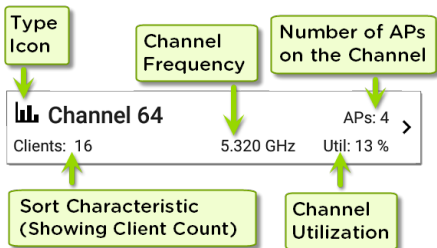
Discovery app are also applied to the Wi-Fi Analysis app.

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.



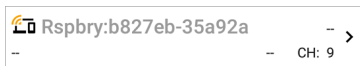
Wi-Fi List Cards

The information displayed on each card varies depending on the selected Sort characteristic and the data the CyberScope was able to discover. For example, a card on the Channels list screen displays the channel number, frequency, connected APs, and utilization.

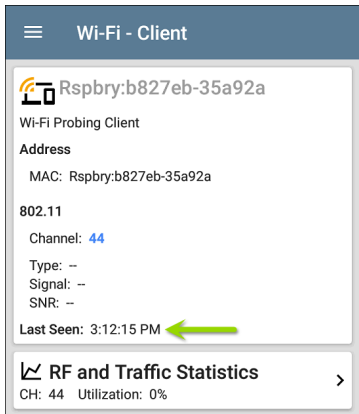


The lower left field displays the characteristic by which the list screen is currently sorted. In the image above, the Channels list is sorted by Client Count.


If a device is grayed out, the CyberScope 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 CyberScope, is shown on the device's Details screen.



☰ **Wi-Fi - Client**

 Rspbry:b827eb-35a92a

Wi-Fi Probing Client

Address

MAC: Rspbry:b827eb-35a92a


802.11


Channel: 44

Type: --

Signal: --

SNR: --

Last Seen: 3:12:15 PM 

 **RF and Traffic Statistics** >


CH: 44 Utilization: 0%

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.

← Channel Filters	
Bands (3)	▼
Devices (1)	▼
SSIDs (70)	▼
APs (55)	▼
BSSIDs (244)	▼
Problems (1)	▼

NOTE: The Channels, AP, BSSID, and Client screens include the ability to filter on Problems.

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:

← Overlap Filters	
Channels (5)	∨
SSIDs (9)	∨
Signal (3)	∨
SNR (4)	∨
802.11 Type (5)	∨
Security (3)	∨

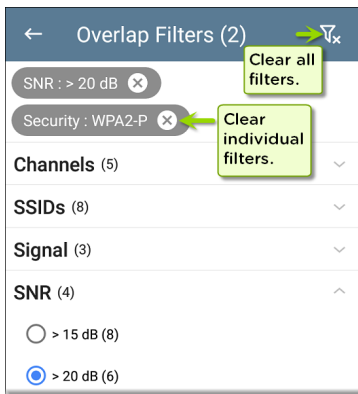
The number in parentheses shows how many active network characteristics are detected for each category. (The example shows (5) active Channels, (9) SSIDs, and so on.)

Tap a category to select filters by tapping the checkboxes or radio buttons.

Security (3)	∧
<input type="checkbox"/> WPA2-E (2)	
<input checked="" type="checkbox"/> WPA2-P (9)	
<input type="checkbox"/> WPA-P (5)	


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.)

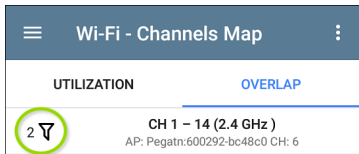
In this example, the Overlap screen shows only those APs that fall under your chosen filter parameters.



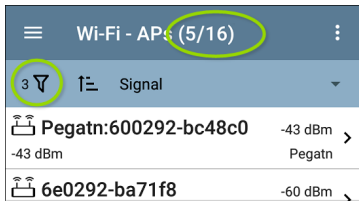
When filters are selected, those active filters are displayed at the top of the Filters screen.

- 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.

The screenshot shows the 'Wi-Fi - APs (55)' screen with a sort menu open. The menu options are:

- Signal
- Name
- Problem
- Mfg Prefix
- SSID Count
- BSSID Count
- Channel Count
- Client Count
- Authorization

Below the menu, several AP entries are visible, each with a signal strength indicator and a right-pointing arrow:

AP Icon	AP Name	Signal Strength	Sort Option
📶	192.168	-29 dBm	Bm >
📶	AsusTk:	-34 dBm	Bm >
📶	10.24.8.	-39 dBm	Bm >
📶	10.24.8.	-39 dBm	Bm >
📶	10.24.8.	-40 dBm	Bm >
📶	Lnksys:	-42 dBm	Bm >
📶	10.24.8.35	-43 dBm	

Select a Sort option to order the list based on your selected characteristic.

Wi-Fi - APs (16)		
Filter	Sort	
	Tchclr:7c9a54-be4263	-68 dBm >
SSIDs: 4		Tchclr
	Pegatn:600292-bc48c0	-42 dBm >
SSIDs: 3		Pegatn
	Tchclr:7c9a54-be425a	-66 dBm >
SSIDs: 3		Tchclr


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.

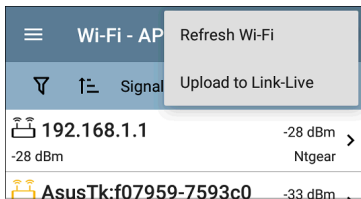
Tap the sort order icon to switch the sort order between normal and reverse order.

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.

Set Authorization

38 of 226 devices selected


- Authorized (0)
- Neighbor (0)
- Flagged (0)
- Unknown (0)
- Unauthorized (0)
- Unspecified (38)


CANCEL

OK

See [Wi-Fi Details Screens](#) 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.



Link-Live

by NetAlly



Wi-Fi Snapshot Name

20190812_210303

Comment

3rd floor

Job Comment

Union Hall



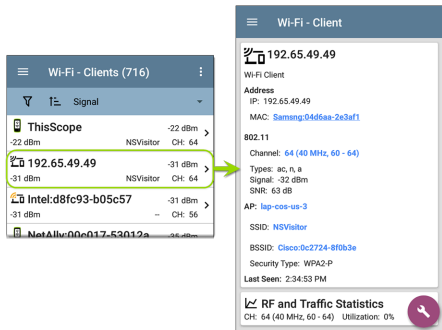
SAVE TO ANALYSIS FILES

See the [Link-Live chapter](#) for more information.

[Back to Title and Contents](#)

Wi-Fi Details Screens

Tap any card on a Wi-Fi list screen (SSIDs, APs, BSSIDs, Clients, etc.) to open the Details screen for that device or network ID.



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.

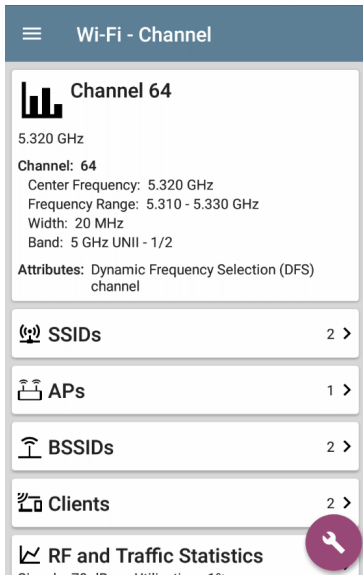
NOTE: Non-underlined links open in the same app (in this case Wi-Fi), and **under-**

[lined 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 CyberScope, 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.

☰ **Wi-Fi - Channel**

 **Channel 64**

5.320 GHz

Channel: 64


Center Frequency: 5.320 GHz


Frequency Range: 5.310 - 5.330 GHz


Width: 20 MHz


Band: 5 GHz UNII - 1/2



Attributes: Dynamic Frequency Selection (DFS) channel

 **SSIDs** 2 >

 **APs** 1 >

 **BSSIDs** 2 >

 **Clients** 2 >

 **RF and Traffic Statistics** 

Signal: 70 dBm Utilization: 10%

The Channel Details screen above shows how many SSIDs, APs, BSSIDs, and Clients 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.

Wi-Fi - BSSIDs (16/149)			
1	Signal		
	Cisco:b83861-84aaf1	-73 dBm	>
-73 dBm	Cisco WEP128 SA	CH: 64	
	Cisco:b83861-84aaf3	-73 dBm	>
-73 dBm	Cisco WEP128 OA	CH: 64	
	Cisco:b83861-84aafd	-73 dBm	>
-73 dBm	aa-Cisco-Wep	CH: 64	

See the topics for each Wi-Fi app screen type (SSIDs, APs, etc.) for more discussion of the corresponding Details screen.

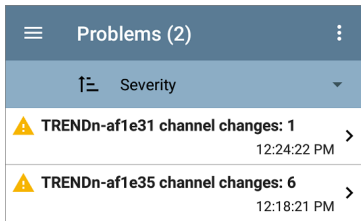
Wi-Fi Problems Screen

If any of the enabled Wi-Fi Problems are detected, the Problems card appears on the Wi-Fi Details screen.


The screenshot shows the 'Wi-Fi - AP' screen. At the top, there is a blue header with a hamburger menu icon and the text 'Wi-Fi - AP'. Below the header is a card for the access point 'TRENDn:d8eb97-af1e2c'. The card contains the following information: an AP icon, the name 'TRENDn:d8eb97-af1e2c', the type 'AP', the AP ID 'AP: TRENDn:d8eb97-af1e2c', the manufacturer 'Mfg Prefix: TRENDn', the standard '802.11', supported types 'Types: ac, n, g, a, b', security 'Security Type: WPA2-P', signal strength 'Signal: -54 dBm', and 'Last Seen: 3:47:10 PM'. Below this card is a 'Problems' card with a yellow warning icon, the text 'Problems', 'Warnings: 2', and a right-pointing arrow with the number '2'. At the bottom, there is a partially visible 'SSIDs' card with a signal icon.

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 CyberScope.

RF and Traffic Statistics Overview

The Channel, BSSID, and Client Details screens can display RF and Traffic Statistics if any traffic is detected.

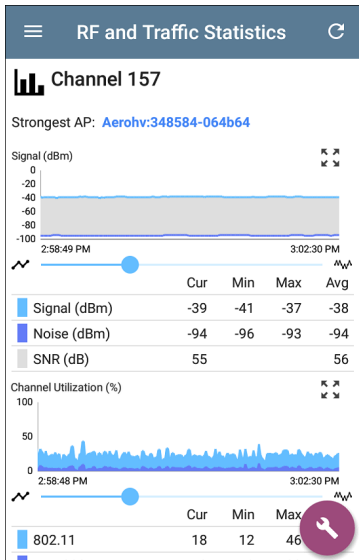
This section describes the common elements of the RF and Traffic Statistics screen. See the topic for each type of Details screen for differences.



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

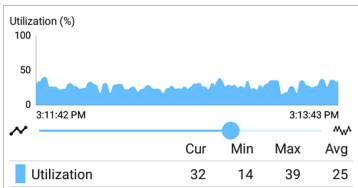
measurements. The Current column contains measurements from the last second. Min, Max, and Avg columns show cumulative measurements gathered during the time the RF and Traffic screen has been open.

Tap the refresh button  at the top of the screen to clear and restart the measurements.

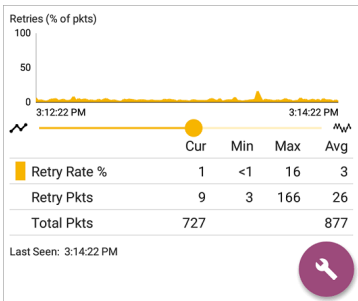
Signal (dBm) graph: Plots the signal strength in dBm of the selected AP or AP with the strongest signal on a channel

- 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.



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 CyberScope 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.

The screenshot displays the 'Wi-Fi - BSSID' screen. At the top, there is a blue header with a menu icon and the title 'Wi-Fi - BSSID'. Below this, a grey card contains the following information: a Wi-Fi icon, the BSSID 'ASUSTekC:d850e6-cc9c9c', the SSID 'wisornet-wpa2psk', the AP 'router.asus.com', the BSSID 'd850e6-cc9c9c', the channel '802.11', and the channel '48 (80 MHz, 36 - 48)'. Technical details include 'Types: ac, n, a', 'Signal: -46 dBm', 'SNR: 43 dB', and 'Security Type: WPA2-P'. The 'Last Seen' time is '9:43:28 PM'. To the right of these details are two buttons: 'Locate' and 'Connect', each with a corresponding circular icon. Below the main card are three more sections: 'Rates and Capabilities' with a 'Capture (Wi-Fi)' button and a circular icon; 'Clients' with a 'Name and Authorization' button and a circular icon; and 'RF and Traffic Statistics' with a circular icon containing an 'X'.

ASUSTekC:d850e6-cc9c9c
BSSID
SSID: wisornet-wpa2psk
AP: router.asus.com
BSSID: d850e6-cc9c9c
802.11
Channel: 48 (80 MHz, 36 - 48)
Types: ac, n, a
Signal: -46 dBm
SNR: 43 dB
Security Type: WPA2-P
Last Seen: 9:43:28 PM

Locate

Connect

↑↓ Rates and Capabilities Capture (Wi-Fi)

📶 Clients Name and Authorization

📊 RF and Traffic Statistics
CH: 48 (80 MHz, 36 - 48) Utilization: 0%

5. Tap **Locate**. This opens the Locate screen and causes your CyberScope 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).



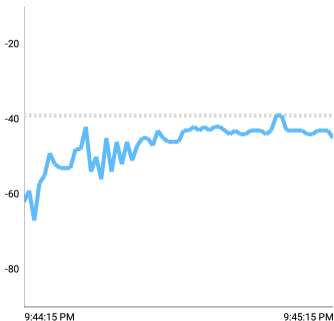
Locate BSSID

**ASUSTekC:d850e6-cc9c9c**

Channel: 48 (80 MHz, 36 - 48)

Signal: -45 dBm

Signal (dBm)





Last Seen: 9:45:15 PM



External Antenna



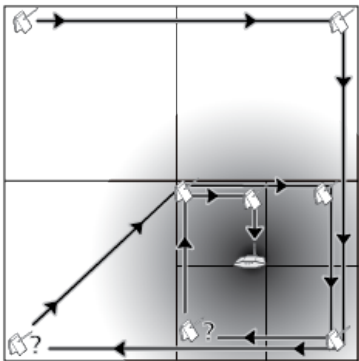
- Tap the speaker icon  to enable an audible tone that increases in pitch as the signal strength of the device increases (as you get closer to it).
 - Tap the speaker icon  to toggle sound on or off.
 - Use the volume buttons on the side of the unit to keys to control tone volume.
- Tap the **External Antenna** toggle to enable 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

CyberScope 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.

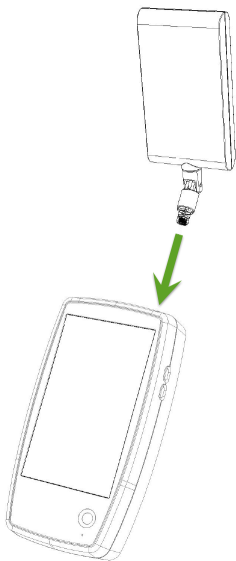
7. Repeat steps 3 through 6 until you find the device.

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

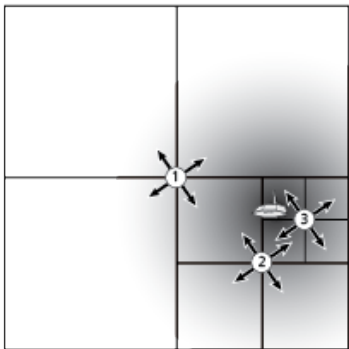
In large, open areas, the directional external antenna can help determine the direction of a signal source more precisely than the internal antennas. Visit NetAlly.com for purchasing information.

1. If using the Directional Tri-band (2.4, 5, and 6 GHz) external antenna, screw the antenna's RP-SMA connector into the topXXX antenna port (shown below). If using the Dual-band (2.4 and 5 GHz) Flag antenna, screw the external antenna cord into the antenna port.



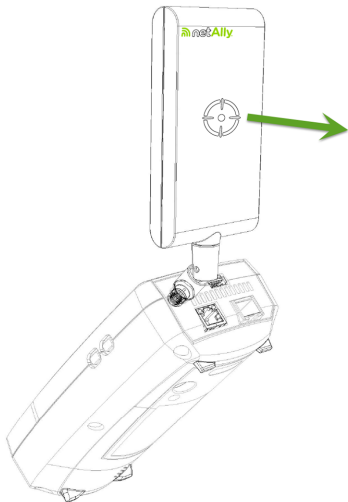
2. On the RF and Traffic Statistics screen, tap the **External Antenna** toggle to enable the external antenna.

- (Optional) Tap the speaker icon to toggle the audible tone on or off.
- Divide the area you want to search into four sections.



- Go to the center of your search area.
- 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.

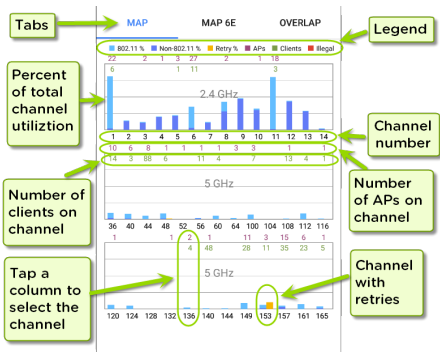
Channels Map

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**.



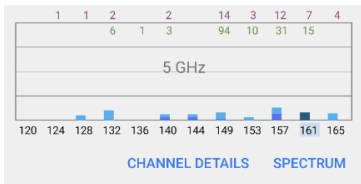
Map and Map 6E Tabs

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).

- 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 without APs can still show 802.11 utilization because of overlap from adjacent channels.)
- Client counts for the channel are shown near 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.

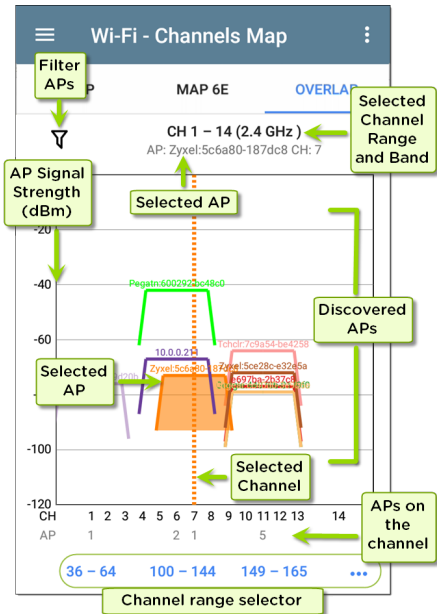


The [Channel Details](#) screen lets you examine the addresses and devices operating on the channel and perform a deeper analysis.

The [Spectrum](#) link opens the Spectrum app, a Wi-Fi spectrum analyzer that provides data about signal strength and noise.

Overlap Tab

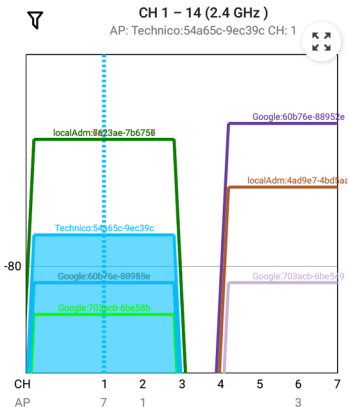
Tap **Overlap** to view access point channel, coverage, and overlap. This can help you spot potential coverage issues. Each discovered AP is shown as a colored bracket on a graph based on channel coverage (on the x-axis) and signal strength in dBm (on the y-axis).



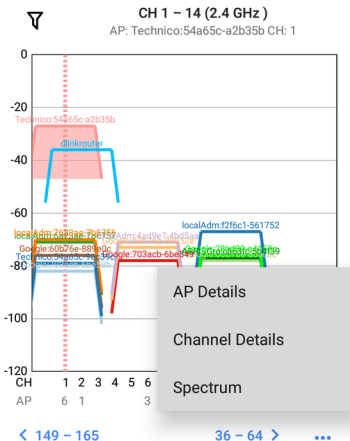
- Tap the Filter icon  near the top left to open the Overlap Filters screen to control

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.



- 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.


Wi-Fi - Channels (43)			
Channel	Frequency	APs	Util
Channel 1 Channel 1	2.412 GHz	APs: 11	Util: 32 %
Channel 2 Channel 2	2.417 GHz	APs: 0	Util: 20 %
Channel 3 Channel 3	2.422 GHz	APs: 0	Util: 0 %
Channel 4 Channel 4	2.427 GHz	APs: 0	Util: 7 %
Channel 5 Channel 5	2.432 GHz	APs: 1	Util: 37 %
Channel 6 Channel 6	2.437 GHz	APs: 11	Util: 53 %
Channel 7 Channel 7	2.442 GHz	APs: 0	Util: 0 %


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


 **Wi-Fi - Channel**


 **Channel 1**
2.412 GHz
Channel: 1
Center Frequency: 2.412 GHz
Frequency Range: 2.402 - 2.422 GHz
Width: 20 MHz
Band: 2.4 GHz


 **Problems** 1 >
Warnings: 1

 **SSIDs** 24 >
[Hidden], Battle Mountain Crestron, CiscoE42...

 **APs** 17 >
10.250.2.101, 10.250.3.9, Cisco-Li:20aa4b-0f...

 **BSSIDs** 46 >
18b169-8e7456, 18b169-8e7457, 18b169-c7...

 **Clients**



The Channel Details screen displays the channel's Center Frequency under the icon,

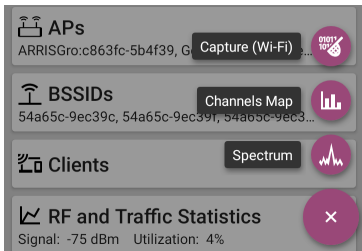
along with the Frequency Range, Width, and Band.

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 CyberScope has discovered.

Wi-Fi - SSIDs (89)		
Filter	Sort	Signal
 Cisco WEP64 OA		-61 dBm > APs: 1
-61 dBm		
 HNTNetgear2.4G		-61 dBm > APs: 1
-61 dBm		
 Cisco 5G		-62 dBm > APs: 2
-62 dBm		
 CiscoQATest-mañana		-62 dBm > APs: 1
-62 dBm		
 Cisco WEP128 OA		-62 dBm > APs: 1
-62 dBm		
 Cisco WEP128 SA		-62 dBm > APs: 1
-62 dBm		
 Home-Guest-2.4G		-62 dBm > APs: 1
-62 dBm		

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. 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


 **Wi-Fi - SSID**


 **LRG**
Broadcast SSID
SSID: LRG
Types: ac, n, g, a, b
Security Type: WPA2-P
Strongest AP: [Sonicwal:18b169-c84602](#)
Signal: -35 dBm
Last Seen: 3:10:00 PM

 **APs** 13 >
Sonicwal:18b169-8e7456, Sonicwal:18b169-...

 **BSSIDs** 22 >
18b169-8e744f, 18b169-8e7457, 18b169-c7f...

 **Channels** 9 >
1, 6, 11, 36, 40, 44, 149, 157, 161

 **Clients** 19 >



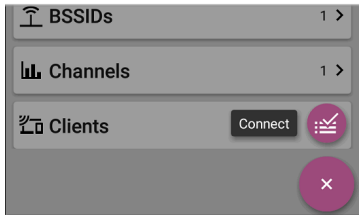
In addition to the Signal and Security Type, the SSID Details displays the AP on the network with the strongest signal, 802.11 Types that the APs in

the network support, and the time the CyberScope last detected activity on the network (Last Seen).

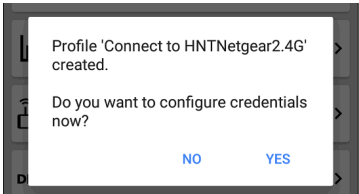
CyberScope can detect and display 802.11 types a/b/g/n/ac/ax.

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.

APs

The APs list screen displays all the Access Points discovered operating on your wireless networks.

Wi-Fi - APs (54)		
Filter	Sort	Signal
	Ntgear:3c3786-719307	-26 dBm > Ntgear
	3e3786-719300	-29 dBm > --
	Lnksys:c8b373-05ac3c	-39 dBm > Lnksys
	Aerohv:348584-064b64	-40 dBm > Aerohv
	J125:002091-554431	-46 dBm > J125
	Lnksys:c8d719-a51bcb	-48 dBm > Lnksys
	Cisco3702 Kris A	-50 dBm

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

☰ Wi-Fi - AP

 **Ntgear:3c3786-719307**

AP

AP: [Ntgear:3c3786-719307](#)

Mfg Prefix: Ntgear


802.11

Types: ax, ac, n, g, a, b


Security Type: WPA2-P

Signal: -28 dBm


Last Seen: 4:09:05 PM

 **Problems** 2 >


Warnings: 2

 **SSIDs** 2 >

Nighthawk 802.11 ax 2.4GHz, Nighthawk 802.1...

 **BSSIDs** 2 >

3c3786-719306, 3c3786-719307

 **Channels** 2 >

6, 36 (80 MHz, 36 - 48)

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 CyberScope.



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.

Wi-Fi - BSSIDs (121)			
	Signal		
 3e3786-719300	-27 dBm	Nighthawk-Guest ...	CH: 6
 Ntgear:3c3786-719307	-28 dBm	Nighthawk 802.1...	CH: 6
 Ntgear:3c3786-719306	-37 dBm	Nighthawk 802.1...	CH: 36
 Aerohv:348584-064b64	-39 dBm	HNT 802.11ax	CH: 157
 Lnksys:c8b373-05ac3b	-42 dBm	The Office Netwo...	CH: 1
 Lnksys:c8d719-a51bcb	-48 dBm	Linksys15538	CH: 1
 1125-002091-554431	-49 dBm		

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

 **Wi-Fi - BSSID**

 **localAdm:cad676-e0adc0**
Reduced Neighbor Report (Transmitted)
SSID: **QA-Meraki-WPA3-E**
AP: **localAdm:cad676-e0adc0**
BSSID: cad676-e0adc0
802.11
Channel: **52 (40 MHz, 52 - 56)**
Types: ax, ac, n, a
Signal: -36 dBm
SNR: 58 dB
Tx Power: 22 dBm
Security Types: WPA3-E, FT-WPA2-E
QBSS Station Count: 1
QBSS Channel Utilization: 3%
Amendments: k, v
Last Seen: 4:30:28 PM

 **RNR BSSIDs** 3 >

 **Rates and Capabilities**



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 (802.11 Amendment r is indicated by an **FT-** prefix).
- QBSS station count and channel utilization
- Active 802.11 Amendments (k or v)
- 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.



Rates and Capabilities



localAdm:cad676-e0adc0

Reduced Neighbor Report (Transmitted)

Rates (Mbps)

Supported: 12, 18, 24, 36, 48, 54

Basic: 12, 24

Country Code: US

802.11 Capabilities

BSS Transition (v): true

Radio Resource Measurement (k): true

802.11n Capabilities

SGI 20 MHz: true

SGI 40 MHz: true

Max AMPDU: 65535 bytes

	Tx	Rx
Max Rate	600.0 Mbps	600.0 Mbps
Max Streams	4	4
Max MCS	31	31

802.11ac Capabilities

SGI 80 MHz: true

SGI 160 MHz: false

Max AMPDU: 1048575 bytes

MU Beamformer: true

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

- BSS Transition amendment (v) status is shown.
- vRadio Resource Measurement amendment status is shown.
- 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

CyberScope can also report Advanced 802.11ax (Wi-Fi 6) capabilities detected in the beacon.

Rates and Capabilities		
802.11ax Capabilities		
Max AMPDU: 4194303 bytes		
SU Beamformer: true		
SU Beamformee: true		
MU Beamformer: false		
	Tx	Rx
Max Rate	573 Mbps	573 Mbps
Max Streams	4	4
Max MCS	11	11
Advanced 802.11ax Capabilities		
+HTC HE Support: true		
TWT Requester Support: false		
TWT Responder Support: false		
Fragmentation Support: 1		
Maximum Number Of Fragmented MSDUs/A-MSDUs Exponent: 0		
Minimum Fragment Size: None		
HE Link Adaptation Support: 0		
All ACK Support: false		
BSR Support: false		
Broadcast TWT Support: false		
32-bit BA Bitmap Support: false		
MU Cascading Support: false		
Ack-Enabled Aggregation Support: false		
DM Control Support: false		

Interworking

CyberScope can also report Interworking information (also known as Passpoint and Hotspot 2.0) detected in the beacon.

Rates and Capabilities		
Max Rate	216.7 Mbps	216.7 Mbps
Max Streams	3	3
Max MCS	23	23
802.11ac Capabilities		
SGI 80 MHz: true		
SGI 160 MHz: false		
Max AMPDU: 1048575 bytes		
MU Beamformer: false		
	Tx	Rx
Max Rate	288.9 Mbps	288.9 Mbps
Max Streams	3	3
Max MCS	9	9
Interworking		
Access Network Type: Chargeable public (2)		
Internet: true		
ASRA: false		
ESR: false		
UESA: false		
Venue Group: 0		
Venue Type: 0		
ANQP OI Count: 0		
Roaming OIs: Google (f4f5e8)		
Hotspot 2.0 Version: 2		
DGAF Disabled: true		

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:



RF and Traffic Statistics



D-LinkIn:802689-4cc98a

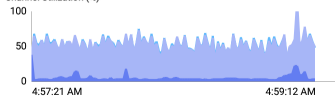
Channel: 153 (80 MHz, 149 - 161)

Signal (dBm)



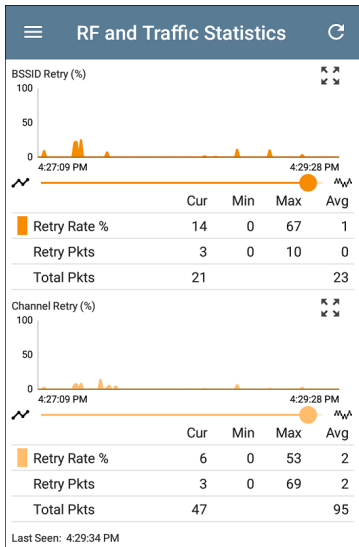
	Cur	Min	Max	Avg
Signal (dBm)	-43	-44	-37	-38
Noise (dBm)	-95	-95	-92	-94
SNR (dB)	52			55

Channel Utilization (%)



	Cur	Min	Max	Avg
CH 802.11	48	24	100	53
BSSID 802.11	46	<1	94	48

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**.

The screenshot displays the 'Wi-Fi - BSSID' screen in the Wi-Fi Analysis App. At the top, there is a blue header with a hamburger menu icon and the text 'Wi-Fi - BSSID'. Below the header, the main content area is divided into several sections:

- BSSID Section:** Features a Wi-Fi icon, the BSSID 'ASUSTekC:d850e6-cc9c9c', and the label 'BSSID'. Below this, it shows 'SSID: wisornet-wpa2psk', 'AP: router.asus.com', and 'BSSID: d850e6-cc9c9c'.
- Channel Section:** Displays '802.11' and 'Channel: 48 (80 MHz, 36 - 48)'.
- Signal and Security Section:** Lists 'Types: ac, n, a', 'Signal: -46 dBm', 'SNR: 43 dB', and 'Security Type: WPA2-P'. To the right of these details are two buttons: 'Locate' and 'Connect', each with a corresponding icon.
- Last Seen:** Shows 'Last Seen: 9:43:28 PM'.
- Navigation Section:** Contains three large buttons with icons: 'Rates and Capabilities' (with a double-headed arrow icon), 'Capture (Wi-Fi)' (with a Wi-Fi signal icon), and 'Clients' (with a Wi-Fi signal icon).
- Bottom Section:** Features a button labeled 'Name and Authorization' (with a shield icon) and a button with a close icon (an 'X' in a circle).



At the bottom of the screen, there is a section for 'RF and Traffic Statistics' showing 'CH: 48 (80 MHz, 36 - 48) Utilization: 0%'.

- 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](#).



Clients


The Clients list screen displays the wireless clients the CyberScope has discovered connected to your wireless networks.

Wi-Fi - Clients (61)		
Filter	Sort	Signal
	192.168.0.105	-34 dBm >
-34 dBm	LiftingRound	CH: 153
	ARRISGro:189c27-59da36	-50 dBm >
-50 dBm	RuleGViolation	CH: 157
	Sonos:48a6b8-a730a3	-62 dBm >
-62 dBm	--	CH: 6
	Sonos:48a6b8-a730a3	-62 dBm >
-62 dBm	--	CH: 6
	localAdmin:6632b1-3eb...	-68 dBm >
-68 dBm	--	CH: 153
	fe80::f28a:76ff:fe6c:82d0	-70 dBm >
-70 dBm	Fragblast	CH: 8
	Sonos:48a6b8-a72f15	-71 dBm >

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 CyberScope icon  shown in the image above.

Tap a Client's card to open the Details screen.

Client Details

 **Wi-Fi - Client**

 **10.24.8.111**
Wi-Fi Client

Address
IP: 10.24.8.111
MAC: [localAdm:d65834-911230](#)



802.11
Channel: [157 \(40 MHz, 157 - 161\)](#)
Types: ac, n, a
Signal: -47 dBm
SNR: 42 dB

AP: [10.24.8.36](#)

SSID: [LRG](#)

BSSID: [Sonicwal:18b169-c8decf](#)
Security Type: WPA2-P

Last Seen: 9:29:39 PM

 **RF and Traffic Statistics**
Channel Utilization: 7% 

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 Cyber-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:

 UGSI:6c0b84-c1f09f

Wi-Fi Probing Client

AddressMAC: [UGSI:6c0b84-c1f09f](#)

802.11

Channel: 6

Types: g, b

Signal: -45 dBm

SNR: 50 dB

Last Seen: 11:03:02 AM

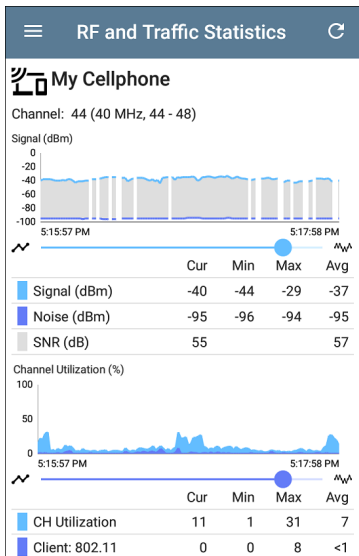
Probes For: _OpenWrt_5G, Nighthawk 802.11ax
5GHz, NETGEAR17-5G

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.)

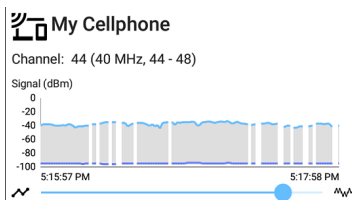
See [RF and Traffic Statistics Overview](#) in the Wi-Fi Details Screens topic for an explanation of the common elements of this screen.



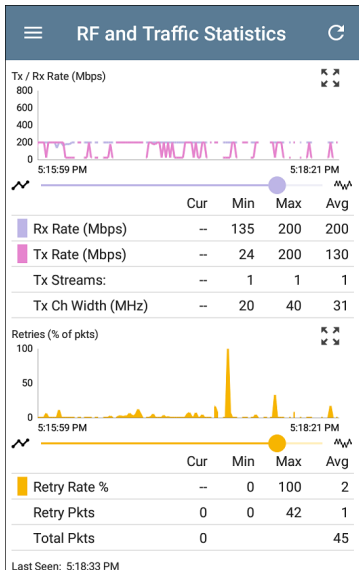
The Signal graph shows the signal in light blue, noise in dark blue, and a calculated SNR.

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 CyberScope to display during those times.



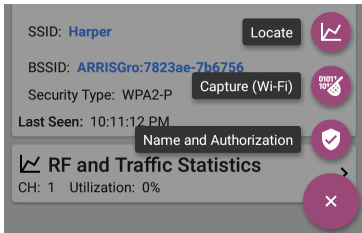
The Clients RF and Traffic Statistics screen also displays a graph of Transmit (Tx) and Receive (Rx) Rates in Mbps, number of Tx Streams, and Tx Channel Width in MHz.



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](#).

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 CyberScope 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 .

Bluetooth (8)		Refresh	More
Sort	Signal		
 05F446-211985	-71 dBm	>	Microsoft
 007C2D-C82BDC	-73 dBm	>	Samsung Electronics Co. Ltd.
 032CDE-4E99ED	-76 dBm	>	Apple, Inc.
 40F6CD-B08D5B	-76 dBm	>	Google
 68644B-0905B8	-78 dBm	>	Apple, Inc.

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 CyberScope 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, CyberScope 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



Wi-Fi - Bluetooth Device



BCA89B-86EAFc

Bluetooth Device

Name: S37cfefccafd5c1c0C

Address: BCA89B-86EAFc

RSSI: -66 dBm

Company

Name: Apple, Inc.

ID: 76

Beacon Type: iBeacon

UUID: 74278bda-b644-4520-8f0c-720eaf059935

Major ID: 0

Minor ID: 13343

Tx Power: -59 dBm

Advertisement

Flags: General Discoverable, Br Edr not Supported

Data: 0201061aff4c00021574278bdab64445208f0c
720eaf0599350000341fc50302221113095333
376366656666363616664356331633043

Last Seen: 5:24:51 PM

The Wi-Fi - Bluetooth Device screen shows the following:

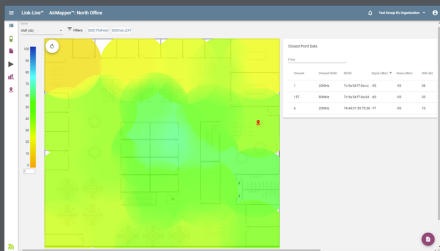
- Address
- RSSI

- 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.



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](https://link-live.com), you can view heatmaps and Wi-Fi measurements for each data collection point.





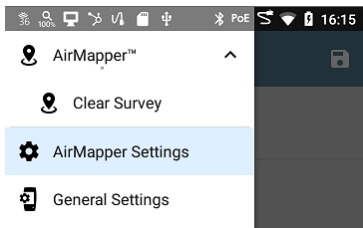
The Signal heatmap is available to all Link-Live users. **AllyCare** Support customers can also view maps of Noise, SNR, and Max TX and RX Rates. Visit [NetAlly.com/Support](https://netally.com/support).

AirMapper Settings

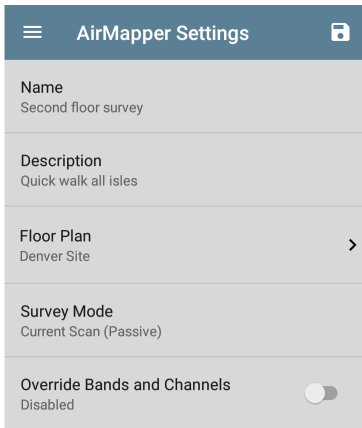
Setting up the AirMapper app to perform a survey involves naming the survey, loading a floor plan image, specifying its dimensions, setting scanning mode, and overriding bands and channels.

- 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



AirMapper Settings	
Name	Second floor survey
Description	Quick walk all isles
Floor Plan	Denver Site >
Survey Mode	Current Scan (Passive)
Override Bands and Channels	Disabled <input type="checkbox"/>

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

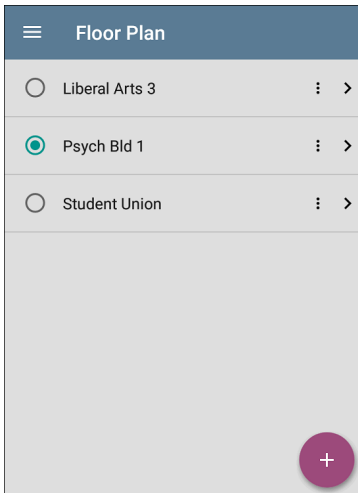
NOTE: You can configure floor plans on Link-Live and then send them to your CyberScope. A notification appears when a new floor plan arrives:




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.



- Fill out the remaining fields for the Floor Plan as needed:

Floor Plan	
Name	DenverSite
Imported File	DenverSite.png
Dimensions	500 x 711 feet >
Signal Propagation	20.0 feet

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. **Auto Sampling (Passive)** is the default and preferred way to perform a survey. AirMapper automatically records data (at the interval specified with the Auto Sampling Period setting) between two points that you choose. This simplifies data sampling and can prevent oversampling. For example, if your survey includes a long hallway or open space, you can take a manual sample measurement at one end of the area, go to the other end, and then take

another measurement. AirMapper fills in the line between the two measurements with automatic measurements made at the sampling period. See [Collecting AirMapper Data](#) for more information.

2. **Current Scan (Passive)** Passive surveys allow 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.
3. **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.
4. **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.

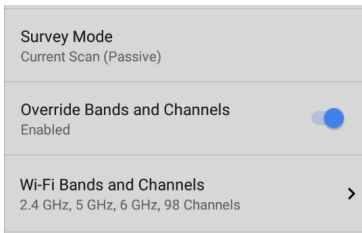
Auto Sampling Period

(Enabled for Auto Sampling mode only.) Tap to choose a preset sampling period or to enter a custom value. This setting controls how frequently an Auto Sampling survey takes automatic measurements between points that you select manually.

Dwell Time

(Enabled for passive survey modes only.) Tap to 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.

Wi-Fi Bands and Channels	
Wi-Fi Band(s)	2.4 GHz, 5 GHz, 6 GHz
2.4 GHz Channels	All
5 GHz Channels	All
6 GHz Channels	All

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

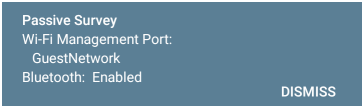
You can reopen the AirMapper settings to change the **Floor Plan > Dimensions** or **Signal Propagation** size after starting your survey. Existing data points are retained on the map unless you select a different Floor Plan.

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.

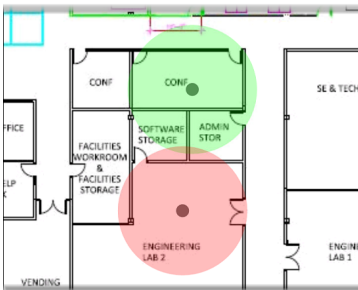
1. Tap **START** to begin the survey.
2. A message displays the survey type, radio, and Bluetooth status. This message appears each time you begin or restart or return to the survey from another app. Tap **Dismiss** to remove the message.

A screenshot of a dark blue rectangular message box with white text. The text is arranged in four lines: 'Passive Survey', 'Wi-Fi Management Port:', 'GuestNetwork', and 'Bluetooth: Enabled'. In the bottom right corner of the box, the word 'DISMISS' is written in white capital letters.

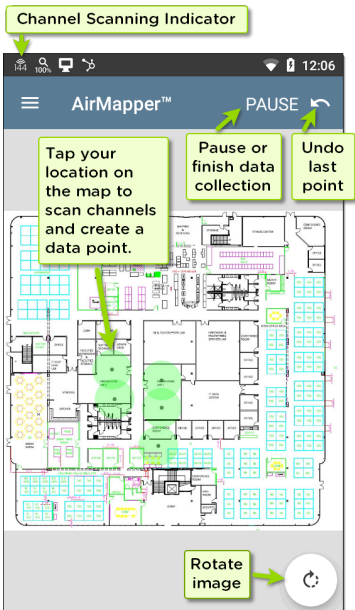
Passive Survey
Wi-Fi Management Port:
GuestNetwork
Bluetooth: Enabled

DISMISS

3. To collect data, move around your site, and tap the map at your current location to scan the enabled wireless channels in that spot. This displays a red circle on the floor plan.
 - Do not move from your location until the data point on the screen turns from red to green. (This takes only a few seconds and shows when the scan is complete.)



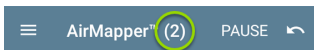
- You can undo the last point, rotate the image, and use swiping or pinch-to-zoom gestures to pan and zoom the map as needed.



- If you use the default Auto Sampling (Passive) survey, you can collect data

points automatically, especially when sampling in straight lines such as long hallways or when crossing open spaces.

- a. Tap the floor plan to take a survey measurement, and wait for the circle to turn green.
- b. Move across the survey area, walking steadily in a straight line. Your unit emits a tone and increments a counter on the AirMapper screen header each time it reaches the value set in the Auto Sampling Period setting.






TIP: Tap the floor plan if you have to change directions or if you change your pace to walk either faster or slower.

- c. Tap floor plan again when you reach the end of the straight line. AirMapper automatically spaces

regular measurements along the path between the two locations you tapped, according to the Auto Sampling Period. These measurements are displayed in blue. (The second green circle may overlap differently depending on where you tap the floor plan a second time.)




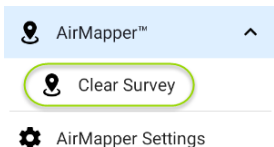
- To check the Wi-Fi status, look at the icon  in the top status bar to see the channels that the CyberScope is scanning in real time.
4. To stop or pause your survey, tap **PAUSE**. This changes the Undo icon to the upload icon .
- If you want to upload your results to Link-Live, tap the upload icon , select **Upload to Link-Live** to display the Link-Live sharing screen. See [Uploading AirMapper Surveys to Link-Live](#) for more

information. (You can resume your survey after uploading.)

- Tap **RESUME** to add more data points.



- To start a new AirMapper survey, open the AirMapper Settings (tap the navigation menu icon  or swipe from the left-side drawer) and select **Clear Survey**.



- To stop your survey, close AirMapper.


Conducting a Connected (Active) Survey

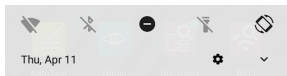
The steps for conducting a connected active survey have several key differences from those for a passive survey:

1. Before beginning the survey, use AutoTest to run a [Wi-Fi profile](#) that connects to the desired SSID.
2. Tap **START** to begin the survey. If you did not start the AutoTest profile or if the test is still in progress, a message displays at the bottom of the screen, and the survey cannot start.
3. Collect data as you would a passive survey, as described above.
 - If the connection is lost (such as by roaming out of range or a signal blockage), the link notification changes to an X. AutoTest continuously tries to reconnect to the SSID.

Survey points taken during this unlinked time are displayed in yellow to indicate

areas where there is not coverage for that SSID.

- You can check the Wi-Fi connection in several ways during your survey:
 - To check the Wi-Fi status, look at the icon  in the top status bar to see the channels that the CyberScope is scanning in real time.
 - Swipe down from the top of the screen to expand the system notification pull-down list and display the actively connected channels and channel width.



 NetAlly ▾

Wi-Fi linked on channel 2 @ 20 MHz

Tap the down arrow next to NetAlly to show additional information:


NetAlly ^

Wi-Fi linked on channel 2 @ 20 MHz

-34 dBm 72.2 Mbps Roams: 0

SSID: Fragblast

IP Address: 192.168.0.109

- If AutoTest was the recently used application other than AirMapper, you can double-tap the Recent button  at the bottom of the screen to quickly toggle between AirMapper and Autotest.
4. To stop or pause your survey, tap **PAUSE**, as described above for a passive survey.


AirMapper Survey Tips

Use these additional tips to make your survey process easier.

Changing Dwell Time During a Survey

NetAlly does not recommend that you change settings during a survey. An exception is **Dwell Time**, which sets the amount of time the CyberScope lingers on each channel to gather data. You can increase the Dwell Time value to

get averages of beacon signal. To change the Dwell Time setting:

1. Tap **Pause** to pause your survey.
2. Open the AirMapper settings, (tap the navigation menu icon  or swipe from the left-side drawer).
3. Tap **Dwell Time** to set a new value.
4. Return to the AirMapper screen and tap **Resume** to return to your survey.

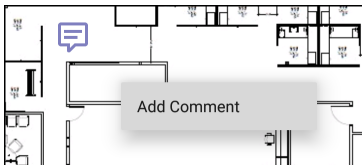
Add Wi-Fi Management Port Data

For active or passive surveys, the active connection data is uploaded along with your other survey data if the Wi-Fi Management port is connected to an SSID. You can then view this information in its own heatmap displays on Link-Live.

Add and Edit Comments

- To edit a comment, long-press on the comment. (If two comments are very close together, AirMapper selects the comment closest to where you pressed.) A context

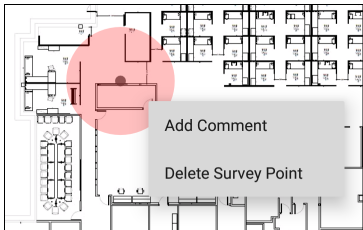
menu appears. Tap **Add Comment**. A dialog appears for you to type your comment. When you are done, tap **OK** to add the comment.



- To edit or delete a comment, locate the comment, and then long-press on it. The selected comment turns dark and a menu appears. Tap **Edit Comment** to change the comment, and then tap **OK** to save the edit. To delete the comment, select **Delete** from the menu.

To Delete Survey Points


Long press over the survey point you want to delete. 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**.





CAUTION: There is no undo for deleting a survey point. Once deleted, you cannot recover the data.

Upload AirMapper Surveys to Link-Live

Uploading your data to Link-Live lets you view colored heatmaps and use various analytical tools.

1. Tap the upload icon .
2. Select **Upload to Link-Live** from the pop-up menu to display the Link-Live sharing screen.

**Link-Live**
by NetAlly



Survey Name


North Office

Comment

Quick Coverage Test

Job Comment

Event Check



SAVE TO AIRMAPPER FILES

3. (Optional) Use the Link-Live sharing screen to enter a survey name, a comment for the overall survey, and a job comment (such as

a note about the overall job status).


NOTE: The Job Comment remains the same until you delete or change it.

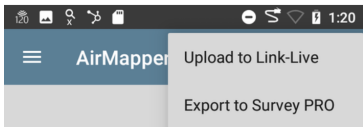
4. Tap **SAVE TO AIRMAPPER FILES** to upload the data and return to the main AirMapper screen. You can then return to the AirMapper screen and tap **Resume** to return to your survey to add more data points, start another survey, or close AirMapper.

NOTE: When you upload data from a survey (or save it locally), your unit also uploads a Discovery analysis file to assist with data analysis on Link-Live. When you upload an active survey, the connection log is also uploaded.

To Export AirMapper Data to AirMagnet Survey PRO

When your survey data collection is complete, you can export the data as a .amp file for import into AirMagnet Survey PRO for advanced analysis, planning and reporting.

1. Tap the upload icon .
2. Tap **Export to Survey PRO** in the pop-up menu.



3. (Optional) Type a new name the .amp file.
4. (Optional) Tap one of the file folders displayed in the upper part of the screen to select a local file location.
5. Tap the **Save** button to create the .amp file and upload it to Link-Live (or to save the file locally).



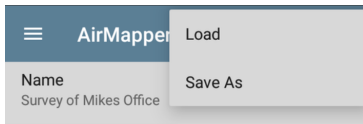
6. Export the .amp file from Link-Live to download it to your PC for use with AirMagnet Survey PRO.

To Load and Save AirMapper Settings

You can save the entire survey configuration as named settings by tapping the disk icon in the title bar.



This allows to load saved settings or to save the current settings.





Path Analysis App

Path Analysis traces the connection points, including intermediate routers and switches, between the CyberScope 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, CyberScope 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 CyberScope. The default destination is www.google.com.

Populating Path Analysis from Another App

Like other CyberScope 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**.

Path Analysis Settings	
Device Name	10.250.2.166
Interface	Any Port
Protocol	Connect (TCP)
TCP Port	80 (www-http)

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 device port to run the path analysis runs. Tap the field to select a port. (See [Selecting Ports](#) for explanations of the different ports.)

CyberScope 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 selection dialog.

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.)


Running Path Analysis


Tap the **START** button at the top of the app screen to begin a Path Analysis.

NOTE: CyberScope must be linked on the Interface (Port) selected in the app's settings. See [Test and Management Ports](#) for help.

The screenshot shows the Path Analysis app interface. At the top is a dark blue header with a hamburger menu icon, the text "Path Analysis", the "START" button, and a gear icon for settings. Below the header is a list of three device entries, each in a white card with a grey border.

Device 1:  **www.google.com** 2
 Device Name: www.google.com
 IP Address: 142.250.69.228
 Interface: Any Port
 Protocol: Connect (TCP)
 TCP Port: 80 (www-http)
Results
 Started: 4:24:59 PM
 Status: Destination not reached in 30 hops
[UPLOAD TO LINK-LIVE](#)


Device 2:  **CyberScope #2 - c09a - 570...** >
 Out: Wired Port 1 Gb FDx

Device 3:  **COS-DEV-SW1.NetAlly.com** >
 --, --, -- Hop: 1

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 CyberScope), 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 CyberScope Cards

 **google.com**
10 ms, 6 ms, 11 ms

Device Name: [google.com](#)

IP Address: 172.217.1.206
Interface: Any Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)

Results
Started: 2:26:58 PM
Status: Destination reached in 11 hops

[UPLOAD TO LINK-LIVE](#)

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 CyberScope Card



This CyberScope 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 CyberScope if you have [claimed it to Link-Live](#).

Tap the card to view more details. The example below shows the SSID, Channel, and other Wi-Fi information the CyberScope can display after running a Path Analysis over Wi-Fi.



Path Analysis



REAL CyberScope #1 - 53c5 - 57...

Device Name: [REAL CyberScope #1 - 53c5 - 570048](#)

IP Address: 10.250.3.45



Out: Wi-Fi Management Port

SSID: [HNTManagement](#)BSSID: [ExtremeN:b027cf-72b2a7](#)Channel: [153](#)

Protocol: --

Security: --

Under the CyberScope 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.



192.168.249.81


8 ms, 4 ms, 3 ms


Hop: 2



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.

 **Path Analysis**









 **192.168.249.81**
8 ms, 4 ms, 3 ms Hop: 2

Router: [192.168.249.81](#)

IP Address: 192.168.249.81

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.

Path Analysis		START	⚙️
	No Reply -, -, -	Hop: 5	>
	4.34.62.118 23 ms, 22 ms, 18 ms	Hop: 6	>
	ae-6.pat1.nez.yahoo.com 47 ms, 40 ms, 46 ms	Hop: 7	>
	Split Route 41 ms, 25 ms, 34 ms	Hop: 8	>
	Split Route 38 ms, 45 ms, 31 ms	Hop: 9	>
	Split Route 48 ms, 28 ms, 47 ms	Hop: 10	>
	slb8-1-flk.ne1.yahoo.com 39 ms, 41 ms, 38 ms	Hop: 11	>
	www.yahoo.com 35 ms, 61 ms, 46 ms	Hop: 12	>


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.

☰
Path Analysis



Split Route

41 ms, 25 ms, 34 ms Hop: 8

Response 1: et-0-0-0.msr1.ne1.yahoo.com

IP Address: 216.115.105.25

Response 2: et-0-0-0.msr2.ne1.yahoo.com


IP Address: 216.115.105.179

Response 3: et-19-1-0.msr2.ne1.yahoo.com

IP Address: 216.115.105.181

Layer 3 Interfaces and Statistics

Statistics for Interfaces on Layer 3 devices may be identified and measured if the CyberScope has SNMP access.



COS_DEV_SW1

13 ms, 12 ms, 13 ms Hop: 3 >

In: Gi1/0/47

1 Gb FDx


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.

 **Path Analysis**

 **COS_DEV_SW1**
13 ms, 12 ms, 13 ms Hop: 3

Router: [COS_DEV_SW1](#)

IP Address: 192.168.249.82

 In: [Gi1/0/47](#)

Speed: 1 Gb
Duplex: FDx

Statistics
Util: 0.3 % Discards: 0.0 % Errors: 0.0 %



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.

 **Path Analysis** START 



Interface: Any Port
Protocol: Connect (TCP)
TCP Port: 80 (www-http)

Results
Started: 3:41:34 PM
Status: Destination reached in 1 hop



[UPLOAD TO LINK-LIVE](#)

 **CyberScope #2 - c09a - 570...** 



Out: Wired Port 1 Gb FDx

 **COS_DEV_SW1** 

In: Gi1/0/13	VLAN: 500	1 Gb FDx
Out: Gi2/0/24	VLAN: 500	1 Gb FDx

 **cos-dev-sw18-poe** 

In: Gi0/1	VLAN: 500	1 Gb FDx
Out: Gi0/7	VLAN: 500	1 Gb FDx

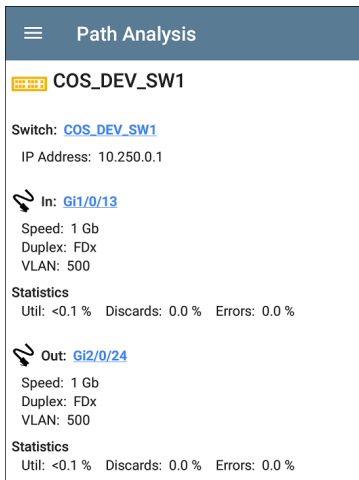
 **Cetus** 

6 ms, 4 ms, 6 ms Hop: 1

The CyberScope 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.



The screenshot shows the 'Path Analysis' app interface. At the top, there is a blue header with a hamburger menu icon and the text 'Path Analysis'. Below the header, the device name 'COS_DEV_SW1' is displayed with a yellow keyboard icon to its left. Underneath, the switch name 'Switch: COS_DEV_SW1' is shown in blue, followed by the IP address 'IP Address: 10.250.0.1'. The 'In' interface section is marked with a red lightning bolt icon and shows 'In: Gi1/0/13' in blue, with details: 'Speed: 1 Gb', 'Duplex: FDx', and 'VLAN: 500'. Below this is a 'Statistics' section with 'Util: <0.1 %', 'Discards: 0.0 %', and 'Errors: 0.0 %'. The 'Out' interface section is also marked with a red lightning bolt icon and shows 'Out: Gi2/0/24' in blue, with details: 'Speed: 1 Gb', 'Duplex: FDx', and 'VLAN: 500'. A second 'Statistics' section follows with 'Util: <0.1 %', 'Discards: 0.0 %', and 'Errors: 0.0 %'.

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 CyberScope 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

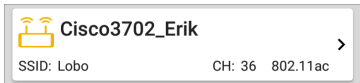
Discards: Percentage of total packets that have been dropped

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.

 **Path Analysis**

 **Cisco3702_Erik**

AP: [Cisco3702_Erik](#)

IP Address: 10.250.3.69

 SSID: [Lobo](#)


BSSID: [Cisco:b83861-84aaf9](#)

Channel: [36](#)

Protocol: 802.11ac

Security: --

No layer 2 devices discovered

 **Layer 2 Path**

No layer 2 devices discovered

In some cases, the CyberScope does not discover Layer 2 devices between Layer 3 devices. There may not be any Layer 2 devices, or CyberScope 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:

**Link-Live**

by NetAlly



Path Analysis Name

20190419_131047

Comment


Conference Room B

Job Comment

Union Hall



SAVE TO ANALYSIS FILES

Path Analysis results are uploaded to the **Analysis** page  on Link-Live.

[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 CyberScope. (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 management Wi-Fi and Bluetooth. (The Spectrum app notifies you if these services are turned on.)


To turn off management Wi-Fi and Bluetooth:


1. Swipe down from the top of the CyberScope screen to display the system icons.
 2. Tap the Wi-Fi icon  until it indicates that Wi-Fi is off .
 3. Tap the Bluetooth icon  until it indicates that Bluetooth is off .
- (Optional) See [Spectrum Settings](#) 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:

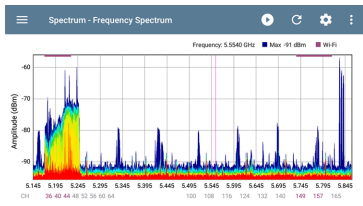
- **Pause:** Tap the Pause icon  to stop updates of the display. This can help you examine patterns and anomalies without updated data overriding your current view.
- **Resume:** Tap the Resume icon  to cancel a pause and continue live data updates.

- **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](#).

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.

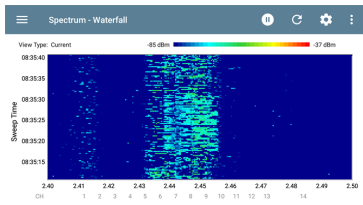


- Blues and greens ("cool" colors) indicate less RF detected at that frequency and amplitude.
- Yellow, orange, and red ("hot" colors) indicate the repeated presence of RF at that frequency and amplitude.
- Darkest blue indicates infrequent RFs while red indicates the continuous presence of RF at that amplitude.
- The top of the chart shows numerical details for display markers you have set and the Wi-Fi legend color.
- The range for the Y-axis (Amplitude) scales automatically according to data values.

- The X-axis displays channels and frequencies.
- The chart shows active Wi-Fi APs and clients by colorizing the channel numbers and by displaying a bar across Wi-Fi frequency range at the top of the chart.

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.

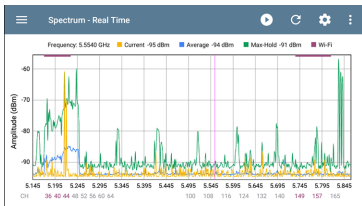


- The vertical axis shows the measurement time, and the horizontal axis shows frequencies and channels.

- 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](#) 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).



- Yellow lines indicates the current values.
- Blue line indicates the average values, which are calculated using all measurements accumulated since the graph was last cleared.
- Green lines indicate the highest measured value (Max-Hold).
- The top of the chart shows numerical details for display markers you have set and the Wi-Fi legend color.
- The range for the Y-axis (Amplitude) scales automatically according to data values.
- The X-axis displays channels and frequencies.

- The chart shows active Wi-Fi APs and clients by colorizing the channel numbers and by displaying a bar across active Wi-Fi frequency range at the top of the chart.

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**.



Link-Live
by NetAlly



Graphs Image Name

20220309-012724

Comment

Enter Comment

Job Comment

Enter Job Comment



SAVE 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.

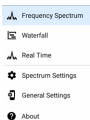
Spectrum Settings

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](#) 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](#) 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 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 environments.
3. Tap **OK** to return to Spectrum Settings.

4. Tap the back button  to return to the Spectrum view.



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.

The screenshot shows the Discovery app interface for a device named "cos-lab-vm-cisco". The device is identified as a Router with the name "cos-lab-vm-cisco" and SNMP ID "cos-lab-vm-cisco". The IPv4 address "10.250.0.11" is highlighted with a green oval and labeled as "(Reachable)". The MAC address is "Cisco:40f4ec-f47681". The device is a Statically Configured Router, discovered via SNMP. A "Path Analysis" button is visible. Below this, the "Addresses" section shows 2 IPv4 addresses and 1 MAC address, with a "Ping/TCP" button and a "PING/TCP" icon. The "VLANs" section lists VLANs 1, 196, 500, 508, 526, and 560, with a "Capture (Wired)" button and a "0101 101" icon. The "Interfaces" section shows 2 up and 41 down interfaces, with a "Browse" button and a "43" icon. A "MIB SNMP" section is partially visible at the bottom. A large pink "X" button is on the right side of the interface.

If you open the Ping/TCP app from this screen, the IPv4 address from the Discovery app is already configured as the Ping/TCP target.

The screenshot shows the Ping/TCP app interface. The title bar contains a menu icon, the word "Ping", the word "START", and a settings gear icon. Below the title bar, the text "PING/TCP" is followed by the IPv4 address "10.250.0.11", which is highlighted with a green oval.

Configuring Ping/TCP Settings Manually

To configure the target and settings manually, open the app's settings .

Ping/TCP Settings	
Device Name	www.google.com
IP Protocol Version	IPv4
Interface	Any Port
Number Of Tests	Continuous
Protocol	Ping
Frame Size (bytes)	64
Interval	1 s

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 CyberScope 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): (Appears only if the **Ping** Protocol is selected.) Specifies the total size of the payload and header the CyberScope 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: (Appears only if the **Ping** Protocol is selected.) Controls how much time passes between each Ping sent from the CyberScope. 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: (Appears only if the **TCP Connect** Protocol is selected.) Indicates the port number your CyberScope 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 CyberScope waits for a response from the target before the test is failed.

Do Not Fragment: (Appears only if the **Ping** Protocol is selected.) Tap the toggle button to enable. See the Frame Size setting description above.

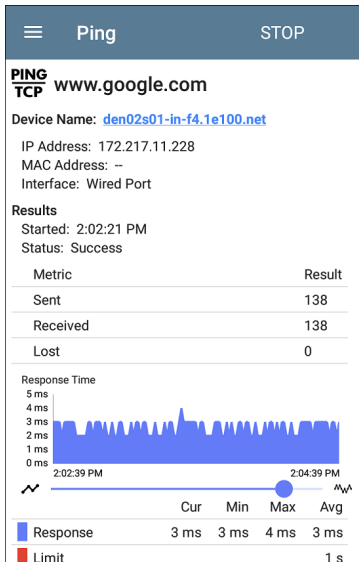
Running Ping/TCP Tests

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 CyberScope 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 CyberScope 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



Capture App

Packet capture is the process of recording network traffic in the form of packets as data streams back and forth over the 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.

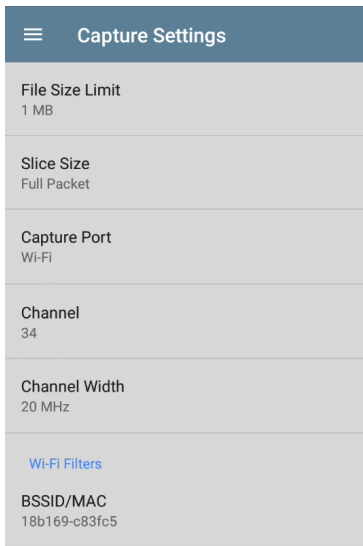
When you open Capture from Home and do not configure any filters, all packets from the switch or channel are captured. The default Wired capture saves all the packets sent from the local switch to the CyberScope. The default Wi-Fi capture saves the packets seen on channel 1.

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.

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.



Capture Settings	
File Size Limit	1 MB
Slice Size	Full Packet
Capture Port	Wi-Fi
Channel	34
Channel Width	20 MHz
Wi-Fi Filters	
BSSID/MAC	18b169-c83fc5

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 CyberScope 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.

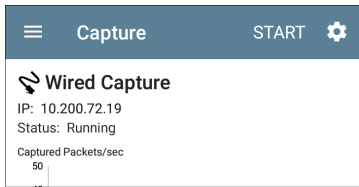
Channel Width: (Appears only if you select a Channel number in the 5-GHz or 6-GHz band, above channel 14). Tap to select a width of 20, 40, 80, or (for 6-GHz band only) 160 MHz.

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.

Running and Viewing Captures

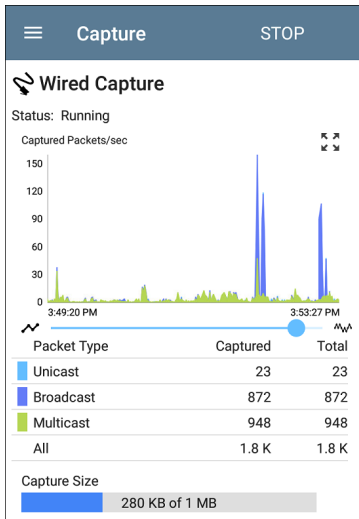
To start Capturing, tap **START** at the top of the app screen.



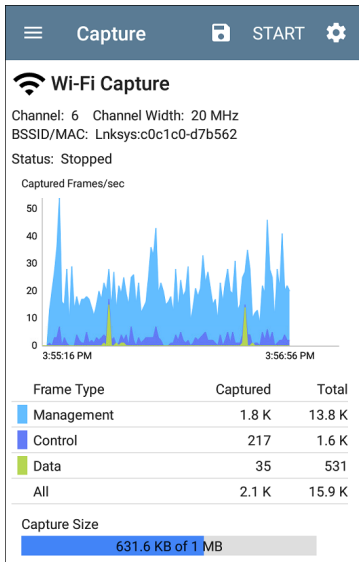
The current Status of the capture and any applied filters are shown under the capture type (Wired or Wi-Fi). The image above indicates that the app captures traffic for IP 10.200.72.19 only.

The Capture screen shows the real-time status of the capture as it runs.

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.



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.

- If you navigate away from the Capture app, the capture process continues to run in the background until the File Size Limit (see [Capture Settings](#)) is reached.
- A capture also stops if you open the Wi-Fi app (which initiates scanning) or if you connect to a Wi-Fi network using AutoTest.
- 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.
- Tap **STOP** to stop the running capture before it reaches the File Size Limit.

Once a capture is completed, the **Save Capture** dialog appears automatically.

Tap the Save icon  to reopen this dialog.

Save Capture

File Name
20190426_125423.pcap

Save To
Downloads/CaptureFiles

Save to Link-Live

Comment
P-082


Job Comment
North Office

CANCEL SAVE AS SAVE

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 CyberScope file system. 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.



Link-Live Cloud Service

The screenshot displays the Link-Live Cloud Service interface. On the left, a sidebar shows a list of test results with columns for test name, time, and status. The main area shows a detailed view for a test titled "Shared ACK-G3-E - 550078" performed on 1/23/23 at 1:43 PM. The interface includes a search bar, navigation icons, and a "Share Album" button. The test details are organized into several sections:

- Test:** Shared ACK-G3-E - 550078, MAC: 00C817-550078, Device: AirCheck G3, Type: Wireless, Profile: InOffice-IPv6-Connect to LRG, Firmware: 2.2.0.43, Wired Management IP: 10.24.8.3.31, WiFi Management IP: 10.24.8.101.
- Link:** PHY Rate: 400 Mbps, Retry Rate: 0%, Signal: -94 dBm, Noise: -90 dBm, SAR: 56 dB, Success.
- Access Point:** 10.24.8.20, SSID: LRG, BSSID: 8021188169-c884cf, 802.11 Types: 8, 9G, 11, Channel: 149, Channel Util (%): 5, Non-802.11 Util (%): 0.5.
- DHCP:** IP: 10.24.8.247, Server: 10.24.8.1, Subnet: 255.255.254.0, DHCP Total: 3417 ms, Local IP: fe80::2c0:1791:fe55:78.
- DNS:** DNS 1: 127.0.0.1.
- Gateway:** 10.24.8.1.

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 CyberScope is claimed.

The comprehensive CyberScope offers more features for analyzing your network in Link-Live than previous testers. Claim your CyberScope to Link-Live.com to access these functions:

- Check for software updates and update your CyberScope software.
- Download third-party applications from the NetAlly [App Store](#) to use on your CyberScope.
- 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 CyberScope's web browser to create and manage your account.

Claiming the Unit

On Link-Live.com

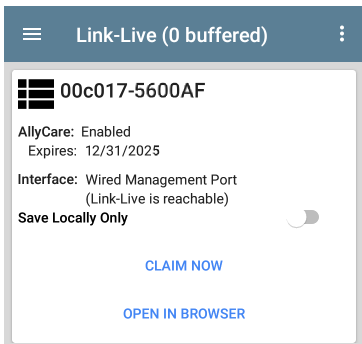
1. The first time you sign in to Link-Live.com, a pop-up window appears, prompting you to claim a device.

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 CyberScope image, and follow the claiming instructions on the Link-Live website.

On the CyberScope Unit

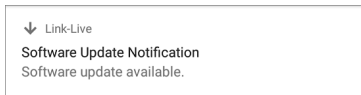
1. Open the Link-Live app. Your unit's MAC address is displayed.



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 CyberScope 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 CyberScope 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 CyberScope 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.

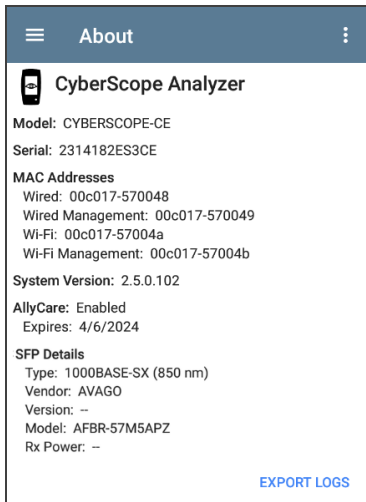
For more information on how to use the [Link-Live.com](#) website, click or tap the

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 CyberScope from Link-Live, tap the [navigation drawer](#) icon  in the Link-Live app, tap [About](#), and then tap **UNCLAIM**.



About

 **CyberScope Analyzer**

Model: CYBERSCOPE-CE

Serial: 2314182ES3CE

MAC Addresses

- Wired: 00c017-570048
- Wired Management: 00c017-570049
- Wi-Fi: 00c017-57004a
- Wi-Fi Management: 00c017-57004b

System Version: 2.5.0.102

AllyCare: Enabled

Expires: 4/6/2024

SFP Details

- Type: 1000BASE-SX (850 nm)
- Vendor: AVAGO
- Version: --
- Model: AFBR-57M5APZ
- Rx Power: --

[EXPORT LOGS](#)

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.

[ALLYCARE CODE](#)

[EXPORT LOGS](#)

Tap **AllyCare Code** to open a dialog to enter an AllyCare Activation Code.

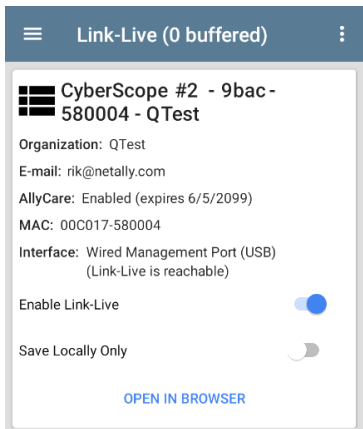
Private Link-Live Settings

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 CyberScope 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 screenshot shows the Link-Live app interface. At the top, a dark blue header contains a hamburger menu icon on the left, the text "Link-Live (0 buffered)" in the center, and a vertical ellipsis menu icon on the right. Below the header is a white card with a grey border. The card displays the following information:

- CyberScope #2 - 9bac - 580004 - QTest**
- Organization: QTest
- E-mail: rik@netally.com
- AllyCare: Enabled (expires 6/5/2099)
- MAC: 00C017-580004
- Interface: Wired Management Port (USB)
(Link-Live is reachable)
- Enable Link-Live:
- Save Locally Only:

At the bottom of the card, there is a blue button labeled "OPEN IN BROWSER".

The CyberScope 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 CyberScope's Link-Live app are informational.

AllyCare indicates the status of NetAlly's optional AllyCare services. See [NetAlly.-com/Support](https://www.netally.com/Support) for more information.

Interface shows which network interface Link-Live currently uses to post results and the network status.


The **Enable Link-Live** toggle button turns the Link-Live features on or off. If Link-Live is disabled here, the CyberScope 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 CyberScope'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.

☰ **Link-Live (2 buffered)** ⋮


 **CyberScope #2 - 9bac - 580004 - QTest**


Organization: QTest
E-mail: rik@netally.com
AllyCare: Enabled (expires 6/5/2099)
MAC: 00C017-580004
Interface: Wired Management Port (USB)
(Link-Live is reachable)

Enable Link-Live

Save Locally Only

[OPEN IN BROWSER](#)

Discovery Snapshot 
Apr 25, 2023 11:16:24 PM

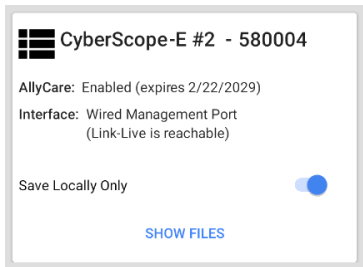
Wi-Fi Snapshot 
Apr 25, 2023 11:16:25 PM

The buffered files displayed automatically upload to Link-Live.com once your CyberScope connects to an active network.

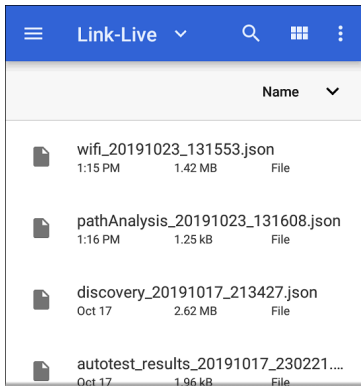
Saving Locally Only

If you do not want to send your results to the Link-Live website, you can still save results locally to your CyberScope 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.



The screenshot shows the Link-Live mobile application interface. At the top is a blue header with a hamburger menu icon, the text "Link-Live" with a dropdown arrow, a search icon, a grid icon, and a vertical ellipsis icon. Below the header is a light gray bar with the word "Name" and a dropdown arrow. The main content area displays a list of four JSON files, each with a file icon, the filename, the time it was created, the size, and the file type.

	Name			
	wifi_20191023_131553.json	1:15 PM	1.42 MB	File
	pathAnalysis_20191023_131608.json	1:16 PM	1.25 kB	File
	discovery_20191017_213427.json	Oct 17	2.62 MB	File
	autotest_results_20191017_230221....	Oct 17	1.96 kB	File

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 CyberScope.


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:


**Link-Live**
by NetAlly

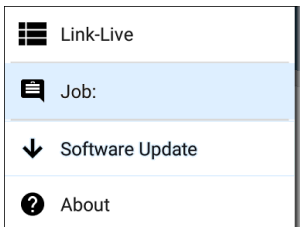
File Name
client1024rsa-new.pem

Comment
Certs

Job Comment
South Campus Wi-Fi

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 CyberScope. 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](https://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

Save to Link-Live



UPLOAD TO LINK-LIVE

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.

**Link-Live**

by NetAlly

**Wi-Fi Snapshot Name**

20190429_122109

Comment

Conference Room B



Job Comment

North Office



SAVE TO ANALYSIS FILES

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.



Link-Live

by NetAlly



Comment

Conference Room B

Job Comment

North Office



SAVE TO LAST TEST RESULT



SAVE TO UPLOADED FILES

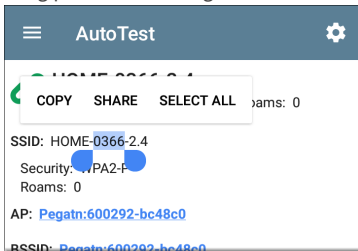
Remember, the regular **Comment** field uploads only to the current result or file, while the **Job**

Comment field uploads with all results and files until you change it.

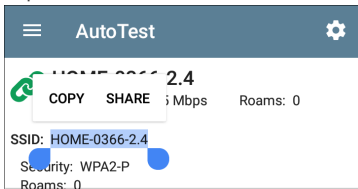
Sharing a Text File to Link-Live

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.

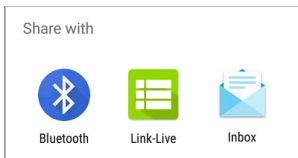
1. Long press a text string to select it.




2. Tap **Select All** if needed.




3. Tap **SHARE**.



4. Select the Link-Live icon to open the [Link-Live sharing screen](#).


**Link-Live**
by NetAlly



File Name

Comment

Job Comment



SAVE TO LAST TEST RESULT

5. Enter any **comments** as needed, and then tap **SAVE TO LAST TEST RESULT**.

Basic Wired Testing With Link-Live Pairing

Link-Live allows you to add several simple wired tests by pairing a NetAlly LinkSprinter or Test Accessory with your CyberScope. This ability lets you run wired tests and view the results on your unit. For example, you may wish to make sure that an AP is getting adequate PoE and basic connectivity while performing a Wi-Fi survey or running other Wi-Fi tests. The wired data is uploaded to Link-Live and then shared to your CyberScope to give you more complete information.

Tests available are:

- Power Over Ethernet (PoE)
- Wired link verification
- DHCP link verification
- Gateway detection
- Link-Live access verification
- (LinkSprinter only) Wi-Fi availability

You can also view the information on Link-Live, which includes supplemental information fields.

Before You Begin

- You must have a Test Accessory iPerf Tester or a LinkSprinter Pocket Network Tester. To acquire one of these devices, contact your [netally.com](https://www.netally.com) representative or visit: [netally.com](https://www.netally.com)
- Read the user guide available for your product, available at: <https://www.netally.com/support/user-guides/>

Link-Live Setup


1. Log into your Link-Live account. (You can use a PC or start the Link-Live app on your CyberScope and then select the **Open in Browser** option.)
2. Make sure your CyberScope is [claimed](#) to Link-Live.
3. Using the same Link-Live organization to which you claimed your CyberScope, claim your Test Accessory or LinkSprinter as per

the instructions in the documentation.


4. Select the **Units** option from the left-side menu. This displays your claimed devices.
5. Select your CyberScope. (On a PC, you can use the filter icons at the top of the list.) This displays your device information.
6. Scroll down until you see the Pair Unit heading.
7. Tap or click on the **Pair Unit** toggle button next to the Test Accessory or LinkSprinter that you want to pair with your unit.
8. Turn off your Test Accessory or LinkSprinter and unplug its Ethernet wire connection.

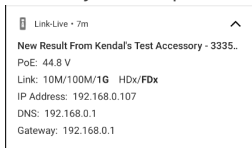
Run the Paired Test and View Results

To run a paired wiring test:

1. With your Test Accessory or LinkSprinter turned off, plug the Ethernet cable connection that you want to test into the test port. (All test LEDs activate for a few seconds, and then the PoE icon LED  remains on if there is adequate power from

the connection.)

2. Wait about 90 seconds for a tests to complete. All five LEDs turn green if the tests are successful. The test results are uploaded to Link-Live and then shared with your CyberScope.
3. To view the results on your CyberScope:
 - a. Wait for the paired test icon  to appear on the system notification bar.
 - b. Swipe down from the top of the screen to view the notifications list.
 - c. Locate and tap on the down arrow for the notification from Link-Live that shows a new result from your Test Accessory or LinkSprinter.



- PoE voltage is listed
- Bold fields in the Link details show actual speed and duplex.
- The IP Address is the DHCP IP.
- The DNS is the primary server (DNS 1)
- Ping times to reach google.com are not included.

NOTE: successive tests replace the data in the notice.

4. To view the results on a PC:
 - a. In Link-Live, select the **Results** option from the left-side menu. This displays your test results for all your claimed devices.
 - b. Select the results you want for the paired Test Accessory or LinkSprinter from the list. (On a PC, you can use the Search function to look for specific devices, folders, etc.) This displays the same information as the CyberScope system notification described above,

but it adds additional information fields:

- Link polarity
- DHCP subnet mask
- Gateway ping time and public IP address
- Ping time for google.com
- (LinkSprinter only) Information on the nearest switch (switch name, model, IP/MAC address, port number, and type)



Performance Test App

The CyberScope'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 CyberScope, 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 CyberScope reports round-trip data for all measurements. Separate upstream and downstream traffic measurements are not possible.

The CyberScope 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 CyberScope or a OneTouch AT 10G.

Other NetAlly testers work with the CyberScope to perform network performance testing:

- **OneTouch AT 10G** can act as the Source or a Peer for Performance tests.

[NetAlly.com/products/OneTap](https://www.netally.com/products/OneTap)

- **LinkRunner AT** and **LinkRunner G2** each have a Reflector feature for exchanging Performance test traffic.
([NetAlly.com/products/LinkRunner G2](http://NetAlly.com/products/LinkRunner%20G2))
- 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 Link-live.com/downloads. Select CyberScope from the drop-down menu to view the list of downloads.

In this Chapter

Performance Test Settings



Configuring Performance Endpoints

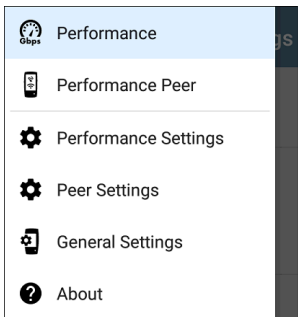
Running a Performance Test

Running CyberScope as a Performance Peer

Performance Test Settings

The Performance app has both **Performance** settings that apply when the CyberScope 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 CyberScope is the source.

Peer Settings control the CyberScope Performance Peer when another device is the source. See [Running CyberScope as a Performance Peer](#).



Saving Custom Performance Tests

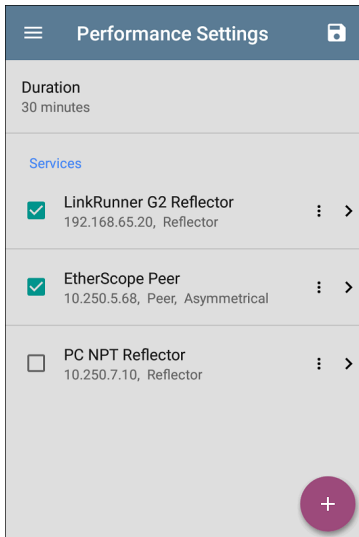
The Performance app allows you to save two levels of test configurations: individual **Services** and complete **Performance Tests** with *up to eight* enabled Services.


- **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](#) .

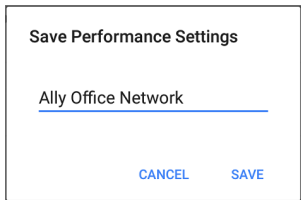


Tap the save icon  to load, save, import, or export a settings configuration.

- **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."



The screenshot shows the 'Performance Settings' screen for a test named 'Ally Office Network'. At the top, there is a blue header with a hamburger menu icon on the left, the title 'Ally Office Network' in the center, and a save icon on the right. Below the header, the 'Duration' is set to '30 minutes'. Underneath, there is a section titled 'Services' in blue. A single service is listed: 'LinkRunner G2 Reflector' with the IP address '192.168.65.20, Reflector'. To the left of the service name is a green checkmark, and to the right are three vertical dots and a right-pointing arrow.

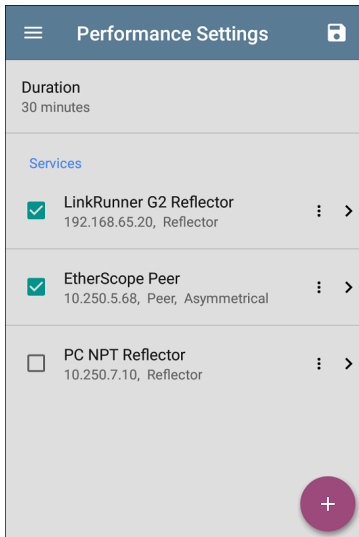
Once you save a Performance Test configuration, the custom name you entered appears at the top of the Performance Settings screen (above) and main Performance Test screen (below).



The screenshot shows the main 'Performance' test screen for 'Ally Office Network'. The blue header contains a hamburger menu icon, the title 'Performance', and a 'STOP' button. Below the header, there is a white card with a speedometer icon and the text 'Ally Office Network' followed by 'Gbps'. Below this, the test details are listed: 'Duration: 1 minute', 'Started: 3:27:07 PM', and 'Status: Next update in 26 seconds'. A table with four columns is shown: 'Loss', 'Latency', and 'Jitter'. Below the table, the service 'LinkRunner G2 Reflector' is listed with a refresh icon on the left and a right-pointing arrow on the right. Underneath the service name, there are four dashes representing data points for each column.

	Loss	Latency	Jitter
LinkRunner G2 Reflector	--	--	--

Configuring the Source CyberScope







Open the Performance Settings screen from the main Performance results screen  or the left-side [navigation drawer](#) .





 Performance Settings 

Duration
30 minutes

Services

- LinkRunner G2 Reflector**  
192.168.65.20, Reflector
- EtherScope Peer**  
10.250.5.68, Peer, Asymmetrical
- PC NPT Reflector**  
10.250.7.10, Reflector



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 CyberScope 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	
Service Name LinkRunner G2 Reflector	
Endpoint Device 10.250.3.112, Reflector	>
Frame Size 512 Bytes	
Bandwidth Rate: 1 Mbps	>
Thresholds Loss: 0.3 %, Jitter: 20 ms, Latency: 100 ms	>
Layer 2 Options VLAN Overrides: Disabled	>
Layer 3 Options TOS: Default (0)	>

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.

☰	Endpoint Device
IPv4 Address	10.250.2.187
Communication UDP Port	3842 (netally-perf)
Endpoint Type	Peer
Traffic Flow	Asymmetrical

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.

Frame Size

128 Bytes


256 Bytes


512 Bytes

1024 Bytes


1518 Bytes

9600 Bytes

Frame Size Mix
abceg 

Custom Value 

[CANCEL](#) [OK](#)

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.

Frame Size Mix

Mix: abceg

User Size: 512 Bytes

<	✕	>
a 64	b 128	c 256
d 512	e 1024	f 1280
g 1518	h 9600	u User

CANCEL OK

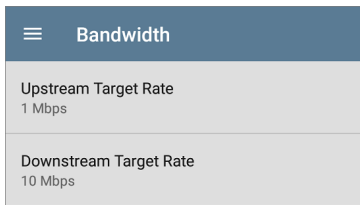
On the Frame Size Mix keyboard shown above, each letter (a through h) is associated with a frame size. The default pattern is "abceg," meaning the traffic pattern follow a repeating sequence of 64, 128, 256, 1024, and 1518 bytes. Use the letter keys along with the arrows and backspace button to edit 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.



Bandwidth	
Upstream Target Rate	1 Mbps
Downstream Target Rate	10 Mbps

- 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.

Upstream Target Rate

1 Mbps

10 Mbps

100 Mbps

999.8 Mbps

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 CyberScope 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.

Thresholds	
Upstream	
Frame Loss Threshold	Disabled
Jitter Threshold	20 ms
Latency Threshold	100 ms
Downstream	
Frame Loss Threshold	0.2 %

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.

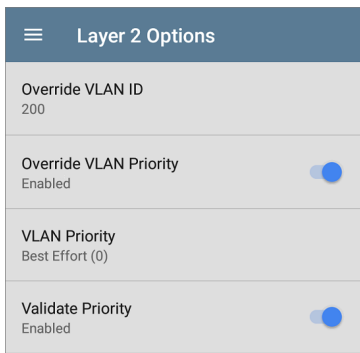
Latency Threshold: Latency is the amount of time it takes for a packet to go from the source to the endpoint and endpoint to source in milliseconds. The default threshold is 100 ms.

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.

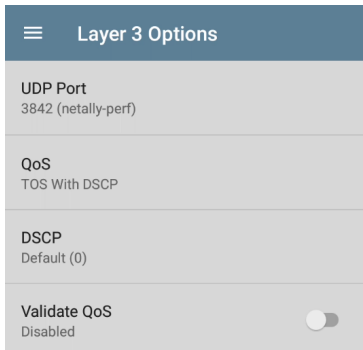
VLAN Priority: This setting only appears if the **Override VLAN Priority** setting above is Enabled. Tap to select a VLAN Priority.

Validate Priority: Tap the toggle button to enable the CyberScope to validate the selected VLAN priority. When the Validate Priority option is enabled, CyberScope 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.



Layer 3 Options	
UDP Port	3842 (netally-perf)
QoS	TOS With DSCP
DSCP	Default (0)
Validate QoS	Disabled <input type="checkbox"/>

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 CyberScope 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.

Configuring Performance Endpoints

CyberScope can run a Performance Test to any of the following Endpoints:

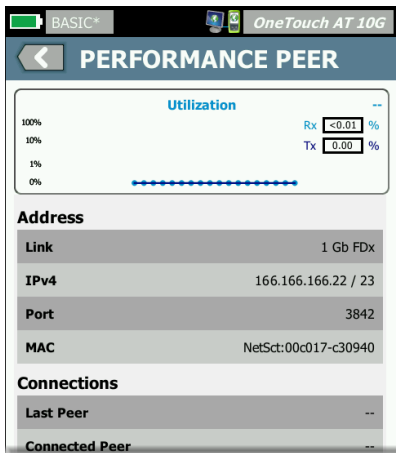
- Another CyberScope (Peer)
- A OneTouch AT 10G (Peer)
- A LinkRunner G2 or LinkRunner AT (Reflector)
- NPT Reflector Software (Reflector)

See our website NetAlly.com for more information about [OneTouch](#) and [LinkRunner](#) and to download the free NPT Reflector PC application.

CyberScope Performance Peer


To run an CyberScope as a Performance Peer, see the [Running as a Performance Peer](#) topic.

OneTouch 10G Performance Peer



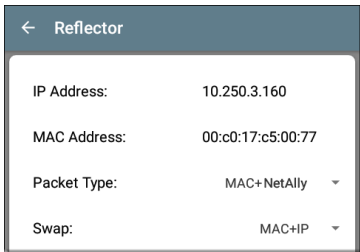
Follow these steps to set up a OneTouch 10G Performance Peer:

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 CyberScope.
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 CyberScope'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 CyberScope'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

Reflector	
IP Address:	192.168.001.090
MAC Address:	00-C0-17-B6-86-0C
Packet Type:	MAC+NetAlly
Swap:	MAC+IP

Reflector Mode



Configure


1000
FDx

Start

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 CyberScope'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 Link-live.com/downloads. (Select Cyber-Scope 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 CyberScope'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
START
⚙️
⋮




New Performance Test

Duration: 10 minutes

Started: 11:16:22 PM

Status: Test failed, thresholds exceeded (6)


	Throughput	Loss	Latency	Jitter
--	------------	------	---------	--------



LinkRunner G2 Reflector

>


	1 Mbps	<0.001 %	60 us	<1 us
--	--------	----------	-------	-------



EtherScope Peer

>

● ↑	939.4 Kbps	6.1 %	56 us	<1 us
● ↓	939.4 Kbps	6.1 %	55 us	1 us



PC NPT Reflector

>

	1 Mbps	0 %	223 us	105 us
--	--------	-----	--------	--------

Performance results update every five seconds if you are using only Reflector endpoints, and/or an CyberScope 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

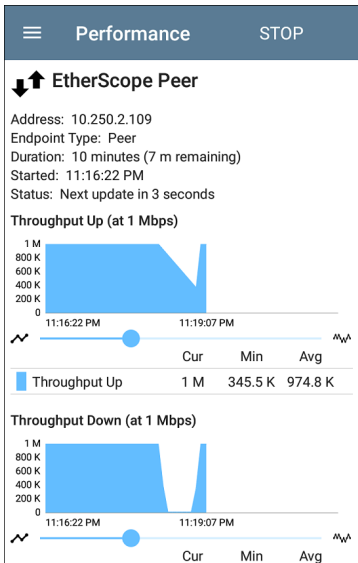
Started: Time at which the test began

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

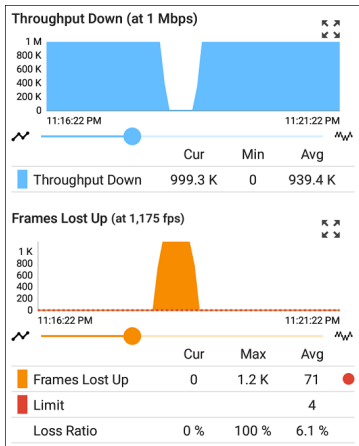
Rerunning Tests from Detailed Results

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.

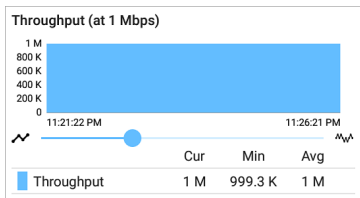
Graph Legends

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 (at 1,175 fps)



	Cur	Max	Avg
Frames Lost Up	0	5.9 K	279.8
Limit			18
Loss Ratio	0 %	100 %	4.8 %

Frames Lost Down (at 2,350 fps)



	Cur	Max	Avg
Frames Lost Down	0	11.7 K	559.5
Limit			35
Loss Ratio	0 %	100 %	4.8 %

Frames Lost (Up/Down): Frame loss is quantified by the number of frames received subtracted from the number of frames sent.

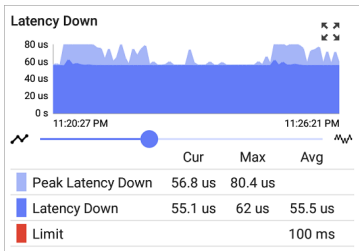
Limit: This is the Frame Loss Threshold for one interval. It is computed from the Frame Loss

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.

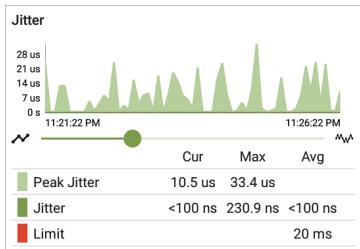
Latency



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. One-way latency measurements consist of the 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 latest results to the Results page  on Link-Live.com.


**Link-Live**


by NetAlly

**Comment****Job Comment****SAVE TO LINK-LIVE**

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**.

**Link-Live**
by NetAlly



Performance Result Filename


New Performance Test - 1 - LinkRunner

Comment

Enter Comment

Job Comment


Performance Main Offices

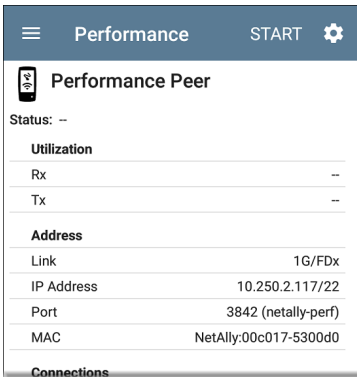
 **SAVE TO LINK-LIVE**

See the [Link-Live chapter](#) for more information.

Running CyberScope as a Performance Peer

In addition to running a Performance Test as the controlling source device, CyberScope can also act as a Peer for another CyberScope or a OneTouch AT 10G acting as the source and controller.

To access the CyberScope Performance Peer, tap the menu button  in the Performance app and select **Performance Peer**.



The screenshot shows the Performance app interface. At the top, there is a dark blue header with a menu icon (three horizontal lines), the word "Performance", the word "START", and a gear icon for settings. Below the header, there is a section titled "Performance Peer" with a small icon of a smartphone. Underneath, the status is shown as "Status: --". There are two sections: "Utilization" and "Address". The "Utilization" section has two rows: "Rx" and "Tx", both with "--" values. The "Address" section has four rows: "Link" with "1G/FDx", "IP Address" with "10.250.2.117/22", "Port" with "3842 (netally-perf)", and "MAC" with "NetAlly:00c017-5300d0". At the bottom, there is a section titled "Connections".

Utilization	
Rx	--
Tx	--

Address	
Link	1G/FDx
IP Address	10.250.2.117/22
Port	3842 (netally-perf)
MAC	NetAlly:00c017-5300d0

Connections

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.

Performance		STOP
	Performance Peer	
Status: Running		
Utilization		
Rx		1.02 %
Tx		1 %
Address		
Link		1G/FDx
IP Address		10.250.2.244/22
Port		3842 (netally-perf)
MAC		NetAlly:00c017-5300d0
Connections		
Last Peer		10.250.2.247
Connected Peer		10.250.2.247
Time Remaining		4 minutes 23 seconds

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 CyberScope to be entered into the controlling source device

Port: UDP Communication port in use by the peer

MAC: The CyberScope's MAC address

Connections

Last Peer: Address of the previous peer that was connected to the CyberScope

Connected Peer: Address of the peer that is currently connected to the CyberScope

Time Remaining: Amount of time left for the current test



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](https://netally.com/products/TestAccessory).

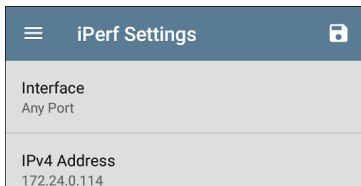
If you are using an iPerf server installed on a PC or other device as an endpoint, iPerf version 3 is required to run the CyberScope iPerf test. You can download iPerf server software from <https://iperf.fr>.


iPerf Settings

To run an iPerf test, you must configure your CyberScope 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

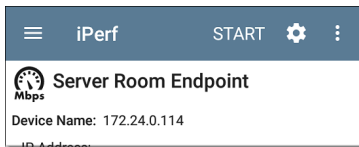
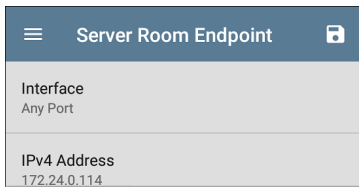
The iPerf app allows you to save a configuration of settings for running an iPerf test to the same endpoint later.



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."

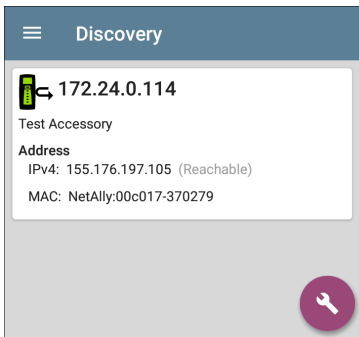



Test Accessories in Discovery

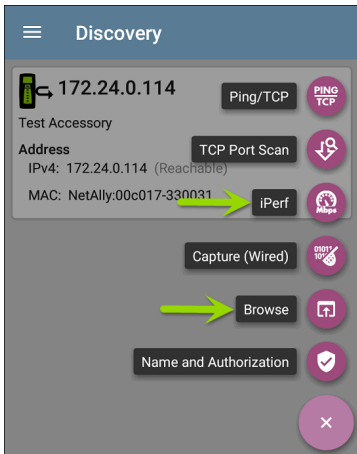
You can start an iPerf test from the Details screen for a Test Accessory in the [Discovery app](#) using the floating action button.

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.

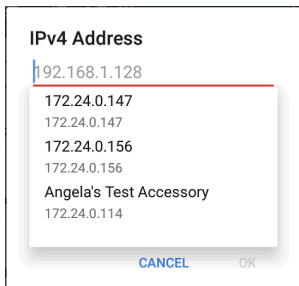
iPerf Settings 	
Interface	Any Port
IPv4 Address	172.24.0.114
Port	5201 (iperf3)
Duration	10 seconds
Protocol	TCP
Direction	Upstream/Downstream
Upstream Threshold	10 Mbps

Server Room Endpoint	
IPv4 Address	10.250.3.182
Port	5201 (iperf3)
Duration	10 seconds
Protocol	TCP
Direction	Upstream/Downstream
Upstream Threshold	10 Mbps
Downstream Threshold	10 Mbps

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 CyberScope 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 CyberScope has discovered through the [discovery process](#), as well as any Test Accessories that are claimed to the same [Link-Live](#) organization as your CyberScope.

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.

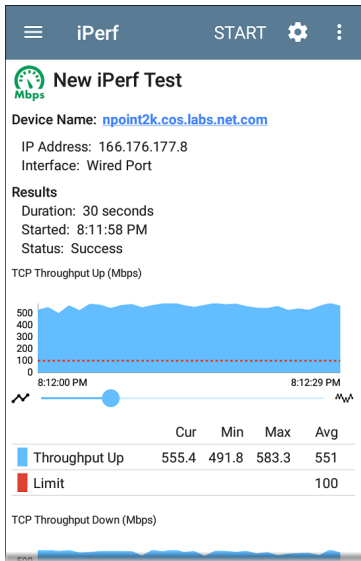
Upstream and Downstream Bandwidth: These fields only appear if the **UDP Protocol** is selected. They specify the desired target bandwidth for the iPerf Test using the UDP protocol.

Upstream and Downstream Thresholds: Thresholds are the values the CyberScope 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.

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 CyberScope Test Port from which the test is running.

Results

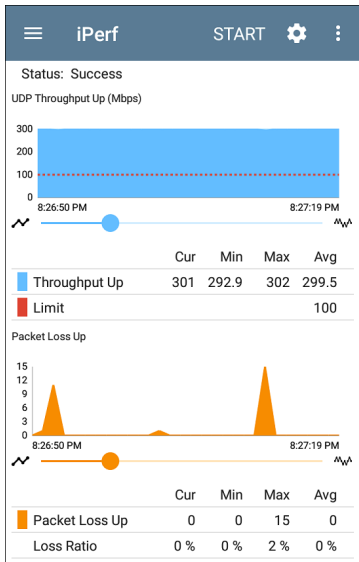
- **Duration:** Configured Duration from the iPerf settings
- **Started:** Time the test started
- **Status:** Success or failure status of the test.

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**.

**Link-Live**

by NetAlly

**Iperf Result Filename**

20190619_134743


Comment

Room 302

Job Comment

Union Hall

**SAVE 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**.

☰ Generator Settings	
Speed	Auto
Frame Size	64 Bytes
Duration	1 minute
Grading Type	Count
Error Threshold	0 (No errors)
Loss Threshold	0 (No loss)

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, and 10 Gbps to match the capacity of the media you want to test. (All settings are full duplex or full duplex forced.)
- **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 CyberScope 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, and 10 Gbps to match the capacity of the media you want to test. (All settings are full duplex or full duplex forced.)
- **Auto** lets the CyberScope automatically negotiate the speed.

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 CyberScope [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.)

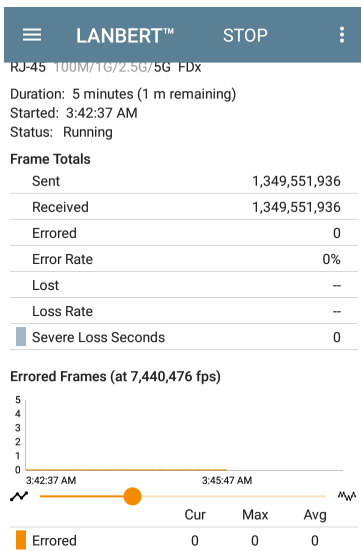
- A NetAlly EtherScope nXG or LinkRunner 10G with the LANBERT application running as the LANBERT Loopback. (Either device can function as the loopback relay and can collect data at the endpoint of the test.) See [LANBERT Settings](#) for instructions on setting up the loopback settings.

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.

**LANBERT Generator**
RJ-45 100M/1G/2.5G/5G/10G FDx
Duration: 1 minute
Started: 10:19:05 PM
Status: Success
Frame Totals

The following example shows an unsuccessful test for an RJ-45 connector that transmitted frames at 100 Mbps at full duplex.

**LANBERT Generator**
RJ-45 10M/100M HDx/FDx
Duration: 10 seconds
Started: 1:45:19 PM
Status: Thresholds exceeded (4)
No frames were received (5)
Frame Totals

- 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 display after the test ends.
- Severe Loss Seconds occur when the LANBERT generator detects $\geq 1\%$ 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).

**Link-Live**

by NetAlly




Comment

Job Comment



SAVE TO LINK-LIVE

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.



Cable Test App

CyberScope'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 CyberScope unit. Connect a cable to this port for testing and tracing with the tone function.

Cable Test Settings


The Cable Test app has limited settings. Tap the navigation menu icon  or swipe from the left-side drawer to open the Cable Test Settings.

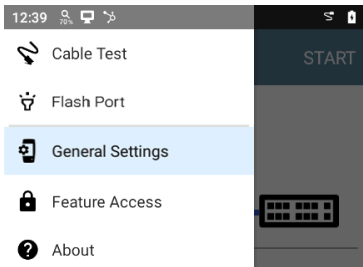
Flash Port


Tap this setting choice to activate the Flash Port function, which flashes port LEDs to help you locate cables and ports. See [Running Cable Test](#) for instructions on using this function.

Distance Unit

The **Distance Unit** setting is contained in the [General Settings](#) menu. The setting designates Feet or Meters.

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, and then tap **OK**.
4. Tap the Back button  at the bottom of the screen to return to the Cable Test screen.

Running Cable Test

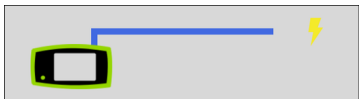
The Cable Test app has general tests for cables as well as a [toning function](#) and a [flash port function](#) to help you trace cables and ports. You can also [upload your results to Link-Live](#).

General Cable Tests

Refer to CyberScope'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.
- CyberScope 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.

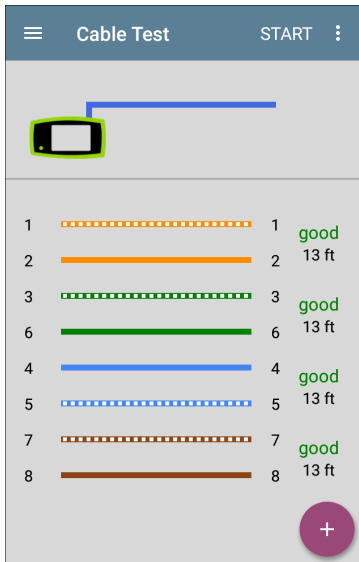
- Additionally, you cannot run a cable test or use the toning feature if the unit detects voltage on the connected cable. The lightning bolt icon on the Cable Test screen indicates detected voltage.



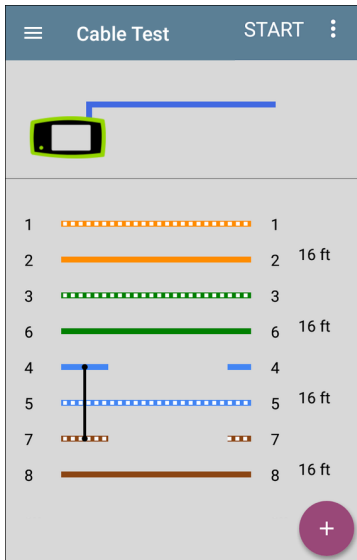
To start the cable test, tap **START** at the top right of the Cable Test app screen.

Open Cable TDR Testing

CyberScope 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 CyberScope 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.



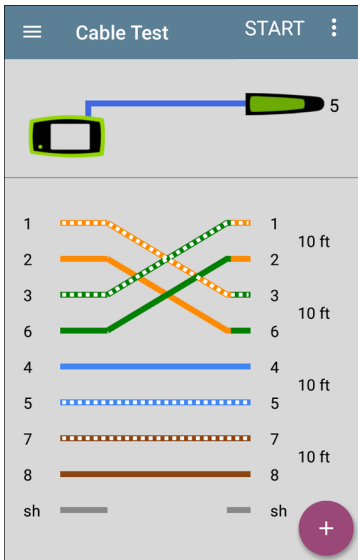
This unterminated cable test image shows a shorted cable between pins 4 and 7.

Terminated WireView Testing

Using a WireView accessory provides more detailed, per-wire results. A WireView #1 is included with your CyberScope. 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 CyberScope from detecting the WireView.




The image above indicates a crossover between pairs 1, 2 and 3, 6 and a WireView accessory number 5.

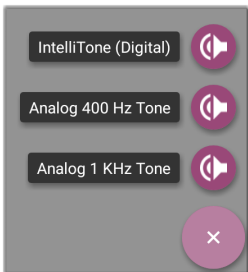
The last row of WireView results indicates whether the cable is shielded: an unbroken line between **sh** means a shielded cable is detected.



Toning Function

You can also trace a cable using a Fluke Networks IntelliTone™ Probe^{*}, an analog probe, or the Tone function.

1. Connect a cable into the left side RJ-45 port.
2. Tap the floating action button (FAB)  to display the tone menu:




* IntelliTone is a trademark of Fluke Networks.

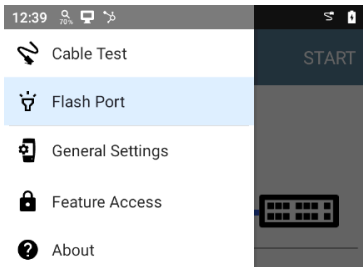
3. Select a Tone option from the menu. The CyberScope emits the tone through the cable, and the probe detects it, allowing you to trace the wire or locate it in a switch closet or rack.

Flash Port Function

Flash Port gives you the ability to make the LEDs blink on your unit's RJ-45 test port and on the switch to which your unit is connected. This helps make the connected port easier to locate on the switch.

To use the flash port feature:

1. Connect the left side RJ-45 port to an active network cable.
2. Tap the navigation menu icon  or swipe from the left-side drawer to open the Cable Test Settings.



3. Tap **Flash Port** to open the Flash Port screen. If the connection to the switch is good, a blue line connects a test unit icon to a switch icon.



Flash Port



Slow

Fast

- Use the slider to set the rate of the flash.

TIP: Some port LEDs may have trouble flashing at a very fast rate. Setting a rate slower than the maximum may work better.
- Tap the **Start** button. When the flash function begins, a green circle appears over the switch icon and flashes at the rate you set with the slider. The green circle, the LEDs on the top RJ-45 port of your test unit,



and the LEDs for the connected port on the switch all blink in unison.

Flash Port



6. When you finish using the Flash Port function, tap the **Stop** button.

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](https://link-live.com).

See the [Link-Live](#) for more information.



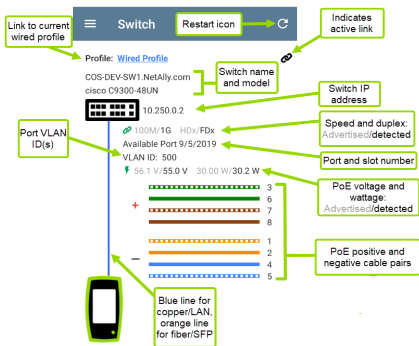
Switch App

The Switch application displays a summary of AutoTest's Wired Profile results from the Link, PoE, and Nearest Switch result screens. This gives you a fast way to display information about how your CyberScope is connected.



NOTE: This application is available on the [Apps screen](#), not the default Home screen. You can open Switch from the Apps screen or tap and hold the icon to move it to your Home screen.

Running Switch


Before running switch, use AutoTest to start a [wired profile](#) so that Switch has information when you need it. To run Switch, simply tap the Switch app icon. This opens the main Switch screen.



The main Switch screen has only a few controls and no settings.




- Tap the Restart icon  to update the switch information. The app displays results from the nearest switch for the wired AutoTest profile that was last run or is currently running.
 - A black Link icon  in the upper right corner of the screen appears when the tester is actively linked.
 - A "no cable" icon displays if no connection is available:



NOTE: Displayed results are retained even after the cable is disconnected. Just tap Restart  to capture and displays the newest information from the switch.

- To open the AutoTest profile, tap the Profile link:

Profile: [Wired Profile](#)

For detailed information, tap the AutoTest cards that display the Link icon , the PoE icon , or the Switch icon .

Specifications and Compliance

This chapter contains device specifications and required compliance information.

CyberScope 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

CyberScope 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	CyberScope-CE United States CyberScope-CE-E 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 (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:** $\pi/4$ -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)
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 CyberScope 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

CyberScope 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.



Complies with 47 CFR Part 15 requirements of the U.S. Federal Communications Commission.



Conforms to relevant Australian Safety and EMC standards.



Listed by the Canadian Standards Association.



Conforms to relevant European Union directives.



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-WNFQ268AXB
T, WA7-9377

Contains IC IDs

6158A-WNFQ268AXB
T, 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 compris 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 mêmes 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.



**European Union (EU)
Radiation Warning
Statement and Con-
formance 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 CyberScope-CE-E 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 CyberScope is in compliance with Radio Equipment Regulations 2017.

[Back to Title and Contents](#)

CyberScope User Guide

Index

A

About screen 80

Access

- points 496

- points, details 612

- remote 132

Active

- discovery ports 521

- subnets 524

- survey 662

Adding

- AirMapper comments 665

- profile groups 203

- profiles 192

- test targets 338

Address

- Discovery 525

- extended range 522

Addresses

- Discovery 465

- subnet 522

Adjustments, signal 96

Administrative password 181

Advanced

- 802.11ax capabilities 622

- authentication 228, 281

- Nmap parameters 414

- Wi-Fi connection 278

Air Quality profiles 385

- FAB 391-392

- results 387

AirMagnet 669

AirMapper

- active survey 655, 662

- app 643

- auto sampling survey 655

- change settings after start 653

- collecting data 655
- comments 665
- configuring 645
- connected survey 662
- deleting survey points 666
- export data 669
- hidden APs and SSIDs 654
- results, uploading 667
- settings 644
- settings, load and save 671
- survey 655
- Wi-Fi management port data 665

AllyCare

- code 737

Antenna

- directional 588
- dual-band flag 592
- external 585, 589
- internal 586

Apps 748

AirMapper 643

AutoTest 185

Cable Test 850

Capture 719, 864

configurations, saving 144

Discovery 431

Files 117

iPerf 816

LANBERT 833

Nmap 399

Path Analysis 672

Performance 761

Ping/TCP 709

screen and store 48

settings, loading 137

settings, saving 141

Spectrum 694

testing 184

- Wi-Fi 553
- APs 496
 - grouping rules 539
 - hidden 654
- ARP sweep rate 526
- Assigning device name 505
- Auditing
 - password 404
- Authentication 268
 - advanced 228, 281
- Authname file 514
- Authorization 505
 - batch 446
 - Wi-Fi 569
- Auto AP grouping rules 539
- Auto power off 55
- AutoTest
 - app 185
 - FTP test 368

- HTTP test 356
- importing/exporting profiles 206
- main screen 207
- periodic 209
- ping test 344
- profiles 185
- profiles, Air Quality 385
- Profiles, Wi-Fi;profiles
 - Wi-Fi;Wi-Fi
 - profiles 261
- Profiles, Wi-Fi;Profiles
 - Wi-Fi;Wi-Fi
 - profiles 265
- profiles, Wi-Fi;profiles
 - Wi-Fi;Wi-Fi
 - profiles 287
- profiles, wired 214, 234
- results, Wi-Fi 287
- results, wired profile 234

- settings, transferring 149
- settings, Wi-Fi profile 265
- settings, wired profile 218
- targets 337
- TCP connect test 351

B

- Batch authorization 446
- Battery charging 31
- Bluetooth 638
- BSSIDs 616
 - advanced 802.11 ax 622
 - Interworking 623
- Buttons 26
 - FAB 110

C

- Cable Test
 - app 850
 - open cable TDR test 854

- running 853
 - settings 851
 - terminated WireView test 857
 - toning function 859-860
- Camera 115
- Captive portals 60
- Capture
- running 725
 - settings 720
 - viewing 725
 - Wi-Fi filters 723
 - wired filters 722
- Certifications and compliance 880
- Certificate 270
- authority file 63
 - importing 272
- Changing
- AirMapper settings 653
 - device language 75

Changing administrative password 181

Channel utilization

 Air Quality profile 391

Channels

 channel test settings 282

 details 604

 map, Wi-Fi 593

 overlap, Wi-Fi 596

 Wi-Fi 602

Charging and power 31

 charge via PoE setting 99

 PoE 31

Chromium browser 113

Claiming your test unit 733

Cleaning 35

Clear

 Wi-Fi problems 568

Clients 629

 certificates 67

- Wi-Fi 537
- Colors, icons 207
- Comments, AirMapper 665
- Common
 - icons 109
 - tools 113
- Configuring
 - AirMapper 645
 - enterprise security 61
 - iPerf 822
 - LANBERT 834, 839
 - Performance endpoints 788
 - Performance source 771
 - saving configuration 141, 144
 - SNMP 527
- Connecting
 - devices, Discovery 477
 - TCP Connect test 351
 - Wi-Fi 57

- Wi-Fi advanced settings 278
- Wi-Fi profile 267
- Contact NetAlly 16
- Credentials, SNMP 522
- Custom
 - Discovery scripts 415
- Custom Signal Adjustments 96
- Customer support 16
- CyberScope
 - additional resources 16
 - feature access 160-161
 - features 26
 - models 22, 24
 - running as peer 812
 - specifications 869

D

- Defaults, app settings 137
- Deleting survey points 666

Details

APs 612

Bluetooth 641

BSSIDs 618

channels 604

client 631

Discovery

 Discovery 454

Performance results 800

SSIDs 609

Wi-Fi 572

Device

discovery 534

endpoint 775

health 537

language 75

Layer 2 686

names 505

names, assigning 505

- settings 52
- types, Discovery 488
- VoIP 536
- Wi-Fi, locating 582

Device types

- access points 496
- hosts/clients 502
- hypervisors 493
- network servers 492
- network tools 501
- printers 499
- routers 489
- SNMP agents 500
- switches 490-491
- virtual machines 494
- Wi-Fi clients 497
- Wi-Fi controllers 495, 498

DHCP

- settings 284

test 311-312

Differences between models 22, 24

Directional antenna 588

Discovery

addresses 465

app 431

connected devices 477

details screens 454

device types 488

FAB 481

filtering list 441

interfaces 470

main list screen 435

monitoring 544

Nmap settings 538

Nmap tests 483

ports 521

problem settings 547

problems 464

- refresh 451
 - resources 478
 - searching list 439
 - security auditing 446
 - settings 518
 - SNMP 476
 - sorting list 444
 - SSIDs 479
 - TCP port scan 467
 - Test Accessory 819
 - through other devices 534
 - VLANs 469
- Distance units 104
- DNS
- settings 284
 - test 326
 - tests 311
- Dual-band flag antenna 592

E

Ejecting storage media 124

Encryption 269

Endpoint

- configuring 788

- device 775

Enterprise security 61

Environmental specifications 878

Exporting

- AirMapper data 669

- AutoTest profiles 206

- logs 81

- Nmap settings 407

- settings 81, 145, 155

Extended ranges 522

External antenna 585, 589

F

FAB 110

- Air Quality profile 392

- BSSID 626

- clients 636

- Discovery 481

- Nmap 483

Factory defaults

- profiles 190

- resetting 157

Features

- permanently disabling 175

Files

- app 117

- authname 514

- certificate authority 63

- managing 117

- moving and copying 120

- sharing 70

- text, sharing to Link-Live 752

Filters

- Discovery list 441

- Wi-Fi 723

- Wi-Fi lists 561

- wired 722

Fingerprints 415

Flashlight 115

Floating action button (FAB) 110

FTP test, AutoTest 368

G

Gateway

- test 331

- test settings 284

- tests 311

General

- settings 92

- specifications 869

- Grading test results 328, 332, 347, 353, 360, 373, 413

- Graphs, trending 105

- Grouping rules, AP 539

- Groups, profile 190, 198

H

- Hidden SSIDs and APs 654

- Home screen 39

- Hosts/clients, discovery 502

- Hotspot 2.0 623

- HTTP

- Proxy 285

- test 356

- Hypervisors 493

I

- Icons

- colors 207

- common 109

Importing

- AutoTest profiles 206

- certificate 272

- client certificate 67

- Nmap settings 407

- settings 145, 155

Interfaces, Discovery 470

Internal antenna 586

Interval

- device health 537

- refresh 526

Interworking 623

iPerf

- app 816

- running 827

- settings 818

K

Kensington lock 29

L

LANBERT

- app 833

- generator settings 834

- loopback settings 839

- running 840

- settings 834

Language

- changing 75

- support 56

Layer 2 Devices 686

Layer 3 Hops 681

Legal notification 37

Limiting output 414

Link-Live

- app 731

- cloud service 731
 - exporting Nmap settings 408
 - features 739
 - getting started 733
 - introduction 731
 - job comment 745
 - notifications 748
 - private instance 738
 - remote setting 103
 - saving locally only 743
 - software updates 747
 - transferring settings 149
 - uploading results 392, 452, 667, 692,
703, 808, 831, 847, 863
 - uploading results, Wi-Fi 570
 - wired testing with pairing 755
- Link-Live Remote
- using 135
- LinkRunner AT (2000) 793

LinkRunner G2 791

LinkSprinter 755

List

 filtering, Discovery 441

 searching, Discovery 439

 sorting, Discovery 444

Loading

 AirMapper settings 671

 app settings 137

Local save 104

Locate

 Wi-Fi devices 582

Logs

 exporting 81

M

MAC, user-defined 96, 100

Machines, virtual 537

Maintenance and safety 34

Management

- files 117

- ports 83, 88

- settings 101

Map, channels 594

Micro SD card 28, 121

Models, differences between 22, 24

Monitoring, Discovery 544

N

Names, device 505

Navigation

- drawer 43, 78

- system 41

NetAlly

- contact 16

- support 16

Network

- servers 492

tools, discovery 501

Nmap

advanced settings 414

app 399

creating tests 406

Discovery 483

Discovery settings 538

editing parameters 410

examples 424

FAB 483

grading results 413

introduction 401

output 423

output, limiting 414

parameters 410

resources 402

run settings 419

running 417

scripts 401, 411

- settings 407

- tests 403

Notifications

- Link-Live 748

- panel 45

- system 45

NPT reflector software 795

O

OneTouch 10G 789

OneTouch AT 10G 812

Overlap, Wi-Fi channels 596

Over-the-air updates 127

P

Passive

- survey 655

Passpoint 623

Password

- administrative 181

- auditing 404
- Password, VNC 102
- Path Analysis
 - app 672
 - introduction 673
 - Layer 2 devices 686
 - Layer 3 hops 681
 - manual configuration 674
 - populating 674
 - results 678
 - running 677
 - settings 674
- Peer 788, 812
- Performance
 - app 761
 - configuring source 771
 - endpoint device 775
 - endpoints 788
 - introduction 763

- NPT reflector 795
- peer 788-789, 812
- reflector 788, 791, 793, 795
- results 798, 800
- running a test 797
- saving custom tests 766
- service 800
- settings 765

Periodic AutoTest 209, 211

Permanently disabling features 175

Ping

- TCP app 709
- TCP app, running 715
- TCP settings 710
- test 344

PoE

- charge battery setting 99
- charging 31
- test PoE before link 98

Portals, captive 60

Ports 26, 83

- Discovery 521

- management 88

- selecting 89

- TCP port scan 550

- test 84

Power

- auto power off 55

- powering on 33

- restart tester option 82

Preferences 104

Printers 499

Private instance, Link-Live 738

Problems

- Discovery 464

- settings 547

- Wi-Fi 568, 575

Product registration 16

Profiles

- adding 192
- adding groups 203
- Air Quality 385
- exporting 206
- groups 198
- importing 206
- managing 190
- Wi-Fi 265
- wired 214, 218, 234

Proxy, HTTP 285

R

- Range, extended 522
- Receive only setting 99
- Reflector 788
- Refresh
 - Discovery 451
 - Wi-Fi screens 568

- Refresh interval 526
- Regex 416
- Register your product 16
- Remote
 - access 132
 - Link-Live, using 135
 - VNC 134
- Remote Link-Live setting 103
- Reset
 - factory defaults 157
 - trending graphs 107
 - user name/authorization 514
- Resources
 - Nmap 402
 - Regex 416
- Resources, Discovery 478
- Restarting tester 82
- Restoring factory defaults 157
- Restricted subnets 524

Results

Air Quality profile 387

AutoTest wired profile 234

AutoTest, Wi-Fi 287

Cable Test, uploading 392, 863

iPerf, uploading 831

LANBERT, uploading 847

Nmap, grading 413

Nmap, output 423

Path Analysis 678, 692

Performance 798, 808

screen, test target 341

Spectrum 703

Wi-Fi, uploading 570

Reverse grading 328, 332, 347, 353, 360, 373

Routers 489, 535

Running

Capture 725

iPerf tests 827

- LANBERT test 840
- NetAlly devices as peers 812
- Nmap settings 419
- Path Analysis 677
- Performance test 797
- Periodic AutoTest 211
- Ping/TCP test 715

S

Safety and maintenance 34

Saving

- AirMapper settings 671
- app settings 141
- configuration 144
- iPerf settings 818
- locally only 104, 743
- Nmap settings 407
- Performance tests 766

Screen

- Discovery, main 435

- shot 73

Scripts

- Discovery, custom 415

- Nmap 411, 415

Scripts, Nmap 401

SD card, micro 28

Searching, Discovery list 439

Security

- auditing, batch authorization 446

- auditing, Discovery 446

- enterprise 61

Selecting, ports 89

Server

- network, discovery 492

Settings

- AirMapper 644

- app defaults 137

- Cable Test 851
- Capture app 720
- channel test 282
- connection 267
- default 137
- device 52
- DHCP, DNS, and gateway 284
- Discovery 518
- Discovery, TCP port scan 550
- exporting 81, 145, 155
- general 92
- importing 145, 155
- iPerf 818
- LANBERT 834
- Link-Live remote 103
- management 101
- managing 137
- Nmap 407
- Nmap, advanced 414

Path Analysis 674
Performance 765
periodic AutoTest 209
Ping/TCP app 710
preferences 104
problems, discovery 547
receive only 99
Spectrum 695, 705
TCP port scan 550
test app 137
transferring 149
VNC 101
Wi-Fi 93
Wi-Fi connection 267
Wi-Fi filters 723
Wi-Fi profile 265
Wi-Fi, advanced 278
wired filters 722
wired profile 218

- wired, general 97

Sharing

- files 70

- screen shot 73

- screens, Link-Live 749

- text files, Link-Live 752

Show internal storage 44, 515

Signal adjustments 96

SNMP

- agents 500

- configuration 527

- credential sets 522

- Discovery 476

- extended ranges 522

- query delay 533

Software

- manual updates 129

- updates 747

- updating 127, 130

Sorting

- Discovery list 444

- Wi-Fi lists 566

Specifications

- CyberScope 869

- environmental 878

- general 869

- wireless 870

Spectrum

- app 694

- changing settings 706

- frequency view 698

- real time view 701

- settings 695, 705

- view, changing 705

- waterfall view 700

SSH 113

SSIDs 607

- Discovery 479

- hidden 654
- Static IP test 312
- Statistics
 - BSSID 624
 - RF and traffic 577, 624, 633
- Status
 - bar 45
- Storage, media 124
- Store 48
- Subnet
 - addresses 522
 - mask 526
- Subnets 535
 - active v. restrictive 524
- Support 16
- Survey PRO 669
- Sweep rate, ARP 526
- Switches 490-491, 536

System

- navigation 41
- notifications 45
- status bar 45

T

Targets

- addresses 341
- AutoTest 337
- test 285
- test results 341

TCP

- connect test 351
- port scan settings 550
- port scan, Discovery 467
- test app 709

Telnet/SSH 113

Test

- Accessory 816

- app defaults 137
- apps 184
- DHCP 312
- DNS 326
- FTP 368
- gateway 331
- HTTP 356
- Ping/TCP 709
- ports 83-84
- static IP 312
- targets 285, 337
- targets, adding 338
- targets, managing 338
- targets, results 341
- TCP connect 351
- type, Nmap 415
- Test Accessory 755, 819
- Tests
 - creating Nmap tests 406

Nmap 403

Nmap Runner 417

Tips, user guide 18

Tools, common 113

Transfer, AutoTest settings 149

Trending graphs 105

reset 107

U

Unclaiming unit 736

Unit

claiming 733

restarting 82

Units, distance 104

Unknown switches 491

Unrecognized Fingerprints 415

Updating

manual 129

software 127, 747

Upload

results to Link-Live 392, 452, 667, 692,
703, 808, 831, 847, 863

Wi-Fi results 570

USB

drive 122

Type-C to USB cable 124

User guide tips 18

User-Defined MAC 96, 100

V

Viewing, Capture 725

Virtual machines 494, 537

VLANs, Discovery 469

VNC

password 102

remote 134

settings 101

VoIP

devices 536

phones 498

W

Web browser 113

Wi-Fi

app 553

APs 612

authorization 569

Bluetooth 638

BSSIDs 616

channels 602

channels map 593

clients 629

clients, discovery 497, 537

connecting to 57

connection, advanced 278

controllers, discovery 495

details screens 572

filtering 561

- list screens 557
- management port data, AirMapper 665
- problems, clearing 568
- problems, screen 575
- profiles 265
- refreshing 568
- RF and traffic statistics 577
- screens 556
- settings 93
- sorting 566
- SSIDs 607

Wired

- profiles 214, 218, 234
- testing with pairing 755

Wired, general settings 97

Wireless

- specifications 870