Discovery App

AirCheck G3のディスカバリアプリケーションは、ネットワーク上のデバイスのインベントリとその属性を作成します：デバイスの種類、名前、アドレス、インターフェース、VLAN、リソース、その他の接続または関連するデバイスを確認できます。このアプリでは、ネットワークデバイスの識別と解析が可能で、Wi-Fi、パス解析、接続テストなどの他のアプリを使用してさらに解析するための出発点として機能します。

ディスカバリ各章の内容

この章では、ディスカバリプロセスとアプリ画面の仕組み、ディスカバリデータの例、ディスカバリ設定の詳細について説明します。

ディスカバリの紹介

ディスカバリは、ネットワーク・コンポーネントの詳細を検出、分類、表示します。ディスカバリによって提供される情報には、以下のものがあります:

- IP、BSSID、MACアドレス
- デバイス名
- デバイスの接続性
- SNMPデータ
- ネットワークの問題
- インターフェースの詳細と統計情報

ARPおよびPingスイープ、SNMP、DNS、mDNS、netBIOSクエリによってデバイスを検出、およびパッシブ・トラフィック監視を提供します。ディスカバリは、検出された各デバイスを分類し、最大2,000台のデバイスを報告することができます。

また、ディスカバリアプリは、**警告**や**失敗**状態など、検出されたデバイスの問題を検出することができます。

AirCheck G3の検出プロセスは、ユニットの電源がオンになると開始されます。

ネットワーク接続（**Wi-Fi、テストまたは管理**）が確立されると、アクティブな検出プロセスが開始されます。

ディスカバリ通知アイコン  は、アクティブなディスカバリの進行状況を示します。このアイコン  は、ディスカバリに有効なポートが1つも接続されていないか、または自動テストが実行されているため、現在アクティブなディスカバリに利用できるリンクがないことを示します。

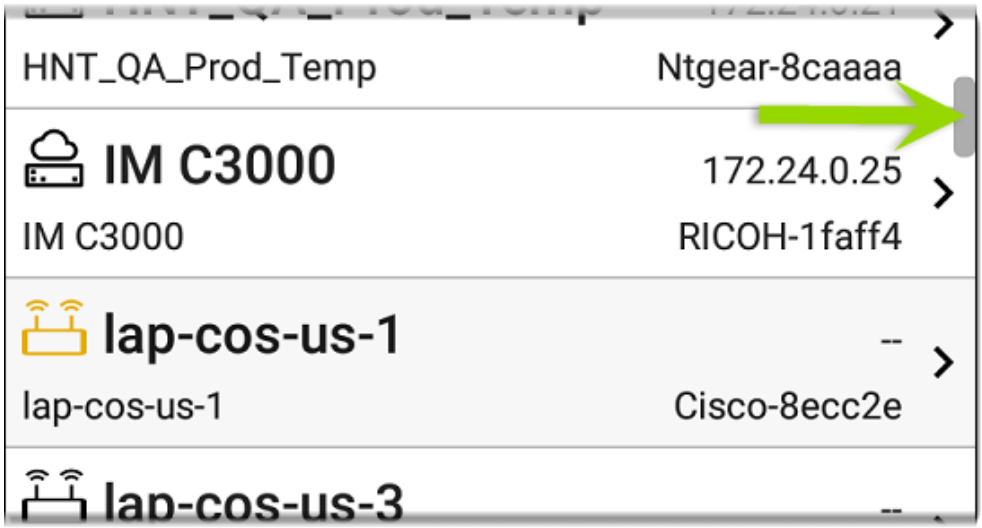
ディスカバリアプリは一貫してネットワークトラフィックを監視していますが、アクティブなディスカバリプロセスはデフォルトで90分ごとに再実行されます。**ディスカバリ設定**で任意の更新周期を選択することができます。

ディスカバリのメイン画面

ディスカバリのメイン画面には、AirCheck G3が検出したすべてのデバイスが表示されます。

自動テストや他のAirCheck G3画面と同様に、ディスカバリのアイコンは色が変わり、**警告**や**失敗**の状態を表します。また、ディスカバリでは、警告や失敗ではない問題関連の情報を示す**青色**と、以前の問題が解決されたことを示す**緑色**でデバイスアイコンを表示します。（**問題設定**を参照して、問題の有効調整としきい値の設定します。）

ディスカバリ画面をはじめ、長いリスト表示があるアプリの画面は、高速スクロールに対応しています。リストの右側にあるスクロールバーハンドルをタッチしてドラッグすると、上下に素早くスクロールすることができます。



ディスカバリのメイン画面では、リストアップされたデバイスのフィルタリングとソート、左側のナビゲーションドロワーを開いて設定を行い、

デバイスのカードをタップしてその詳細を表示することができます。

ディスカバリ リストカード

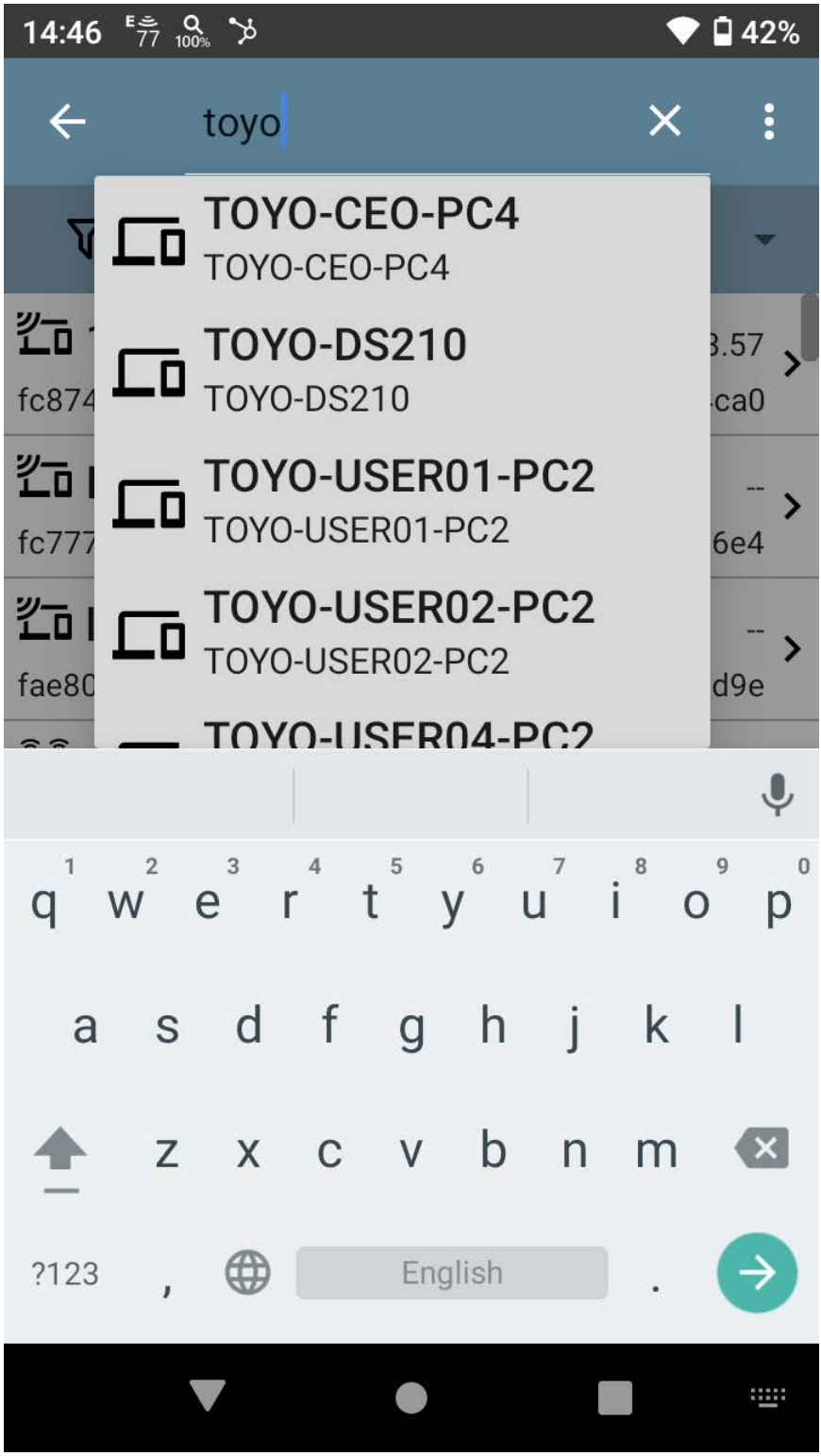
各デバイスカードに表示される情報は、選択したソート要素やAirCheck G3が検出できたデータによって異なります。

カードの左下のフィールドは、ディスカバリ リストで現在ソートされている項目を表示します。上の画像では、リストはMACアドレスでソートされていることがわかります。
ソートの詳細は、ディスカバリ リストのソートを参照してください。

ディスカバリ リストの検索

ディスカバリのメイン画面には、検索機能があります。画面上部の検索アイコン をタップすると、

検出されたデバイスを検索することができます。



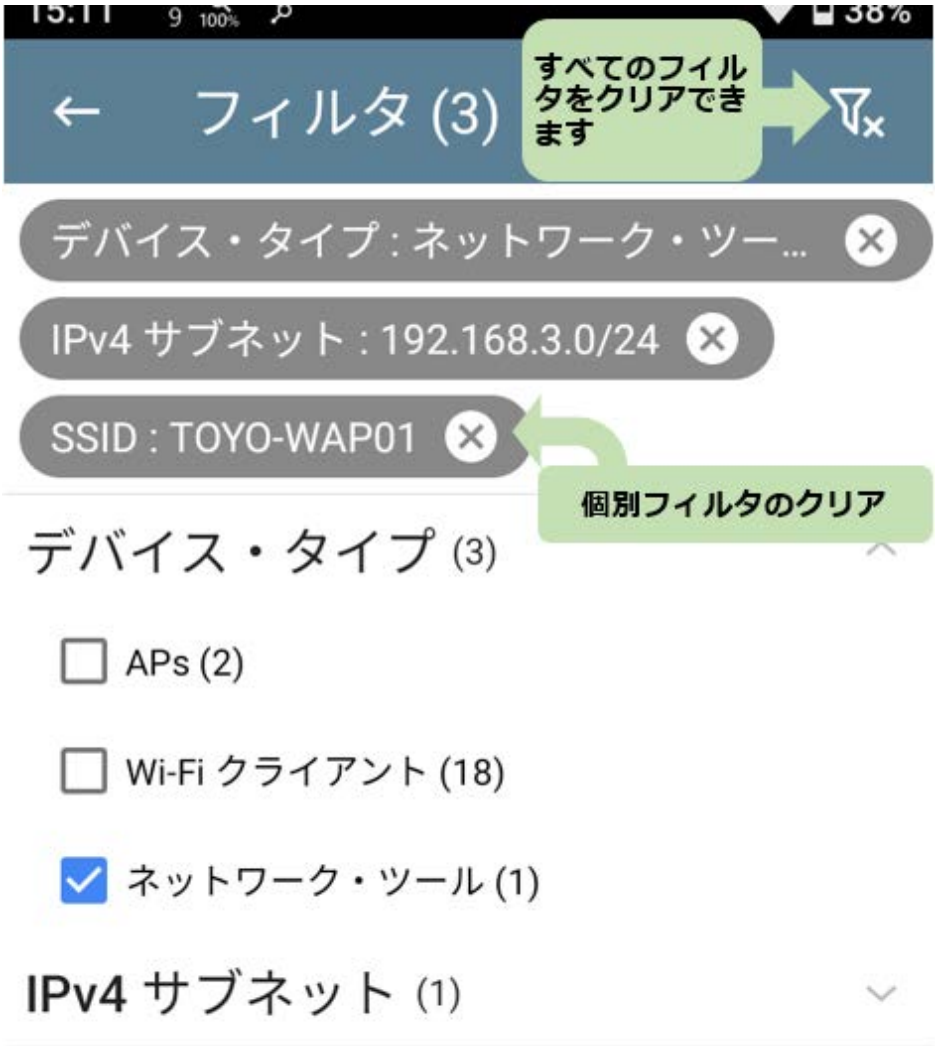
ディスカバリ リストのフィルタリング

ディスカバリのメイン画面の左上付近にあるフィルタボタンをタップすると、リストに表示するデバイスを制御するフィルタを設定できます。

フィルタ画面では、各カテゴリーで検出されたデバイスまたはドメインの数が表示されます。カテゴリー名をタップすると、チェックボックスでフィルタを選択できます。

ディスカバリのメイン画面では、選択したフィルタパラメーターに該当するデバイスまたはIDのみを表示します。

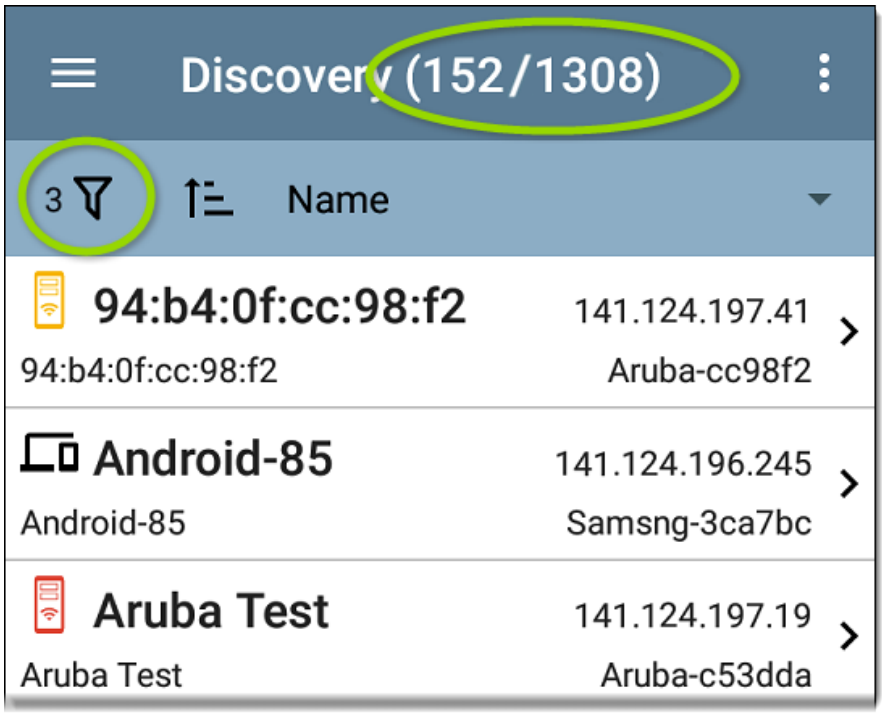
フィルタを選択すると、そのアクティブなフィルタがフィルタ画面の上部に表示されます。



- 各フィルタの右側にある×ボタンをタップするとクリアできます。

- 右上のフィルタクリアのアイコンをタップすると、すべてのフィルタがクリアされます。

フィルタを選択すると、フィルタ画面にその設定でフィルタリングされた結果が表示されます。例えば、上の画像では、ユーザーは**ネットワーク・ツール**のデバイスタイプを選択しています。その結果、検出されたネットワーク・ツールのあるサブネット、アドレス、Wi-Fiバンドなどだけがフィルタリストで選択可能な状態になります。



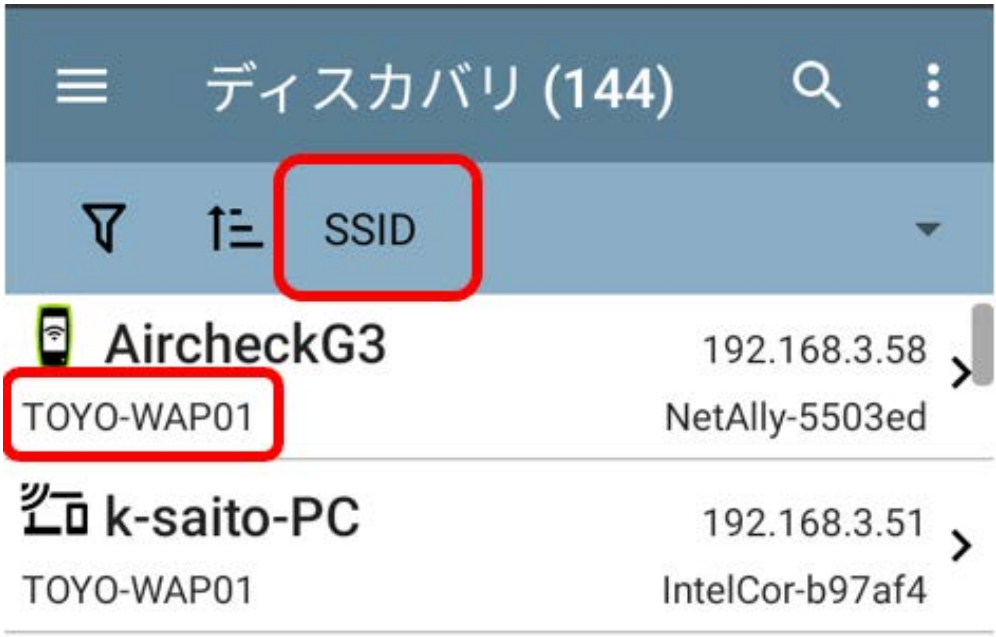
ディスカバリのメイン画面に戻ると、画面タイトルに、検出されたデバイスのうちフィルタリングされたデバイスの数が表示されます（上の画像では、1308台のうち152台がフィルタリングされています）。

フィルタアイコンの左側に、有効なフィルタの数が表示されます。(上の画像では3つのフィルタが有効です)

ディスカバリ リストのソート

ソートバーまたは下矢印をタップすると、ソートのドロップダウンメニューが表示されます。

ソートオプションを選択すると、選択した項目に基づいてデバイスを並べることができます。



選択したソートオプションはデバイスリストの上のソートバーに表示され、各デバイスのソート項目はデバイスタイプのアイコンの下に表示されます。上の画像では、「**TOYO-WAP01**」SSIDに関連するすべてのデバイスが一緒にソートされます。同じSSIDの個々のデバイスは、数字とアルファベットでソートされます。

ソート順アイコン をタップすると、ソート順を通常順と逆順に切り替えることができます。

デバイスはグループごとに分類されます。解決済みの名前を持つものが一番上に表示され（通常の順序）、次にIPv4、IPv6、MACアドレスのみを持つデバイスがそれぞれ下に表示されます。

通常のソート順を逆にすると、グループ内のデバイスが逆になりますが、グループの順番は変わりません。

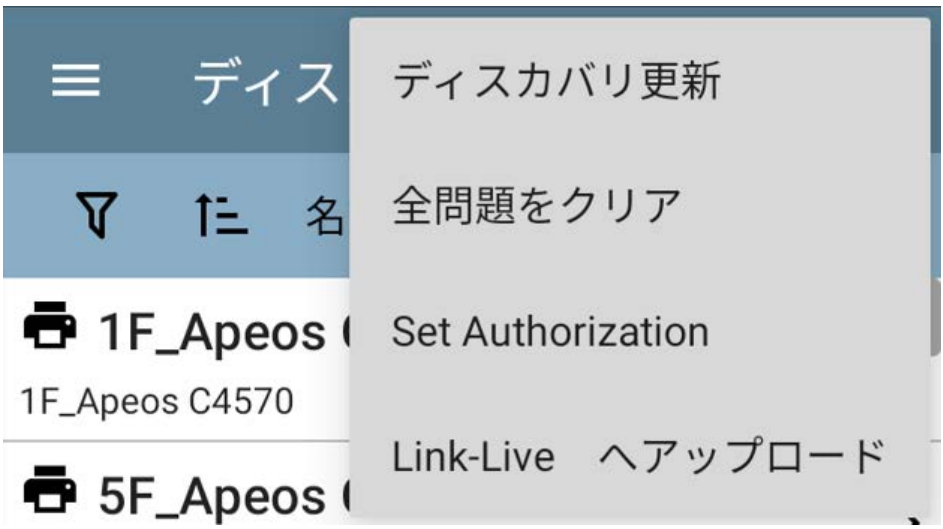
セキュリティ監査 – バッチ認可

バッチ認証では、AirCheck　G3のフィルタリングを拡張して、デバイスを以下のセキュリティ・カテゴリーに整理することができます：

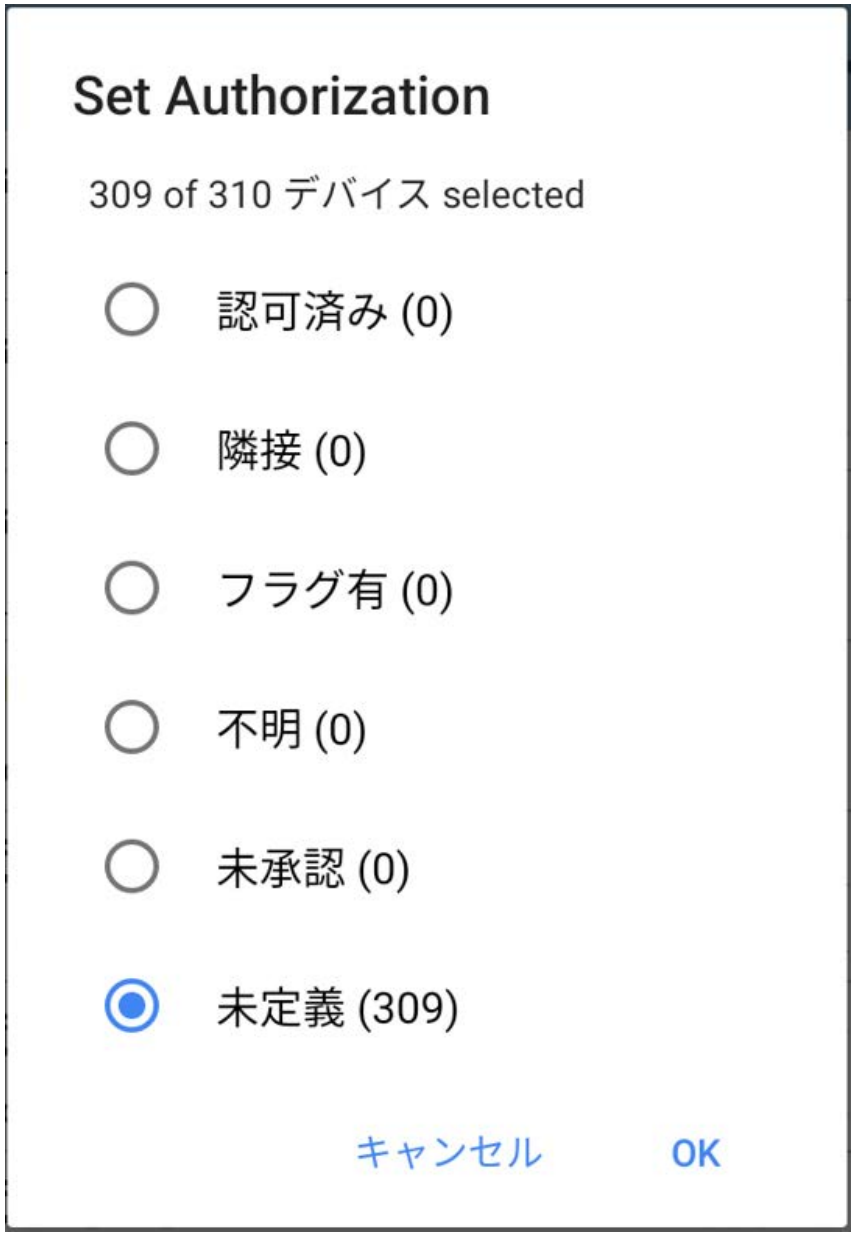
- **認可済み**：ネットワークでの使用が許可されたデバイスの場合
- **隣接**：近隣の組織が所有・管理するデバイスの場合
- **フラグ有**：特定のデバイスを可視化する場合
- **不明**：識別・分類されていないデバイスの場合
- **未認証**：ネットワーク上に存在すべきでなく、セキュリティリスクをもたらす可能性のあるデバイスの場合
- **未定義**：デフォルトで未設定 認可の状態

一度分類すると、認証の種類に応じてフィルタリングすることで、ネットワーク上の新しいデバイスを即座に特定することができます。新しいデバイスは**未定義**として識別されます。

バッチ認証機能を使用するには、分類したいデバイスを特定するフィルタを作成します。 例えば、ビル内の他のオフィスで使用されているSSIDをフィルタリングすることができます。検出されたデバイスのリストをフィルタリングした後、オーバーフローメニューを選択します。

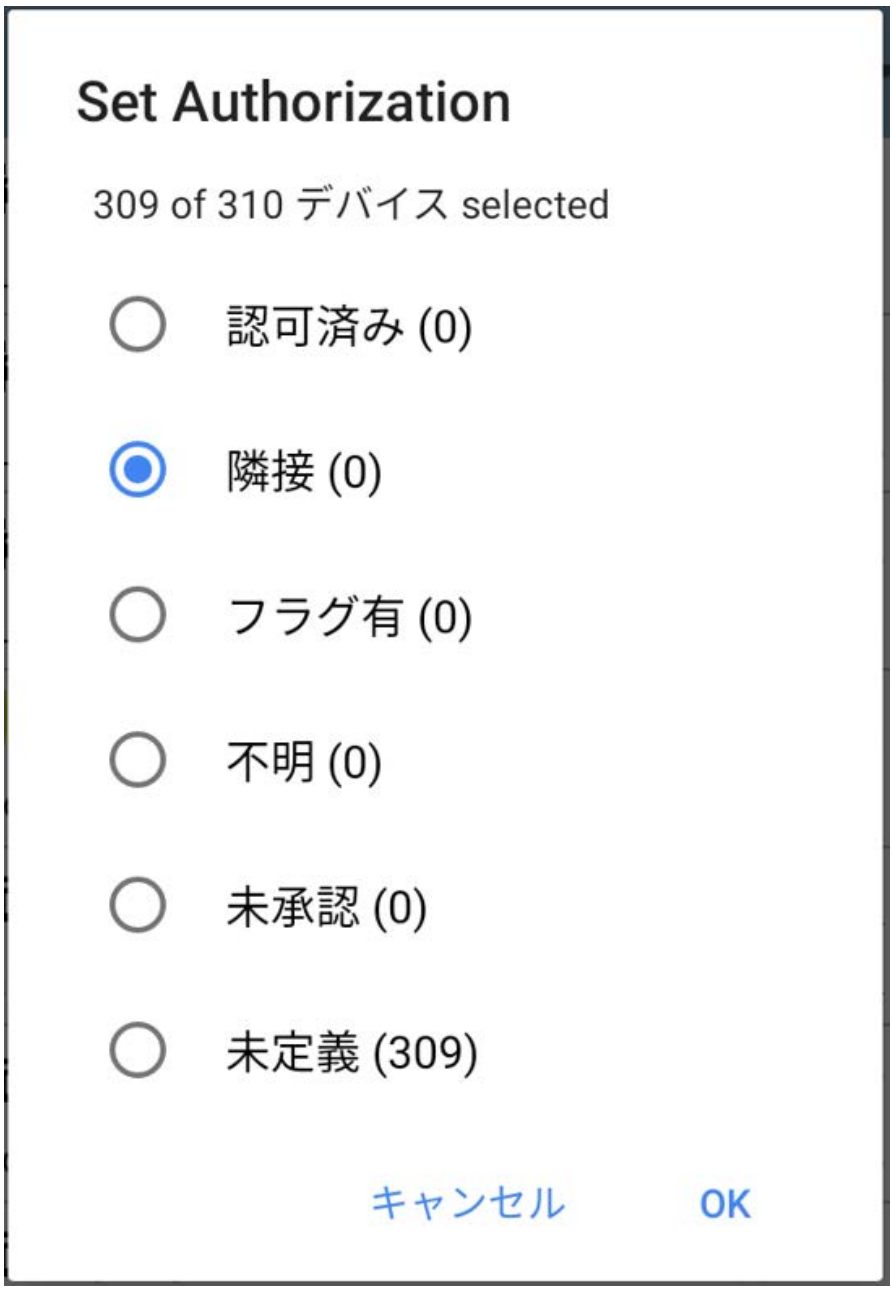


Set Authorizationを選択すると、これらのデバイスが現在どのように分類されているか、また各カテゴリーに属するデバイスの数が表示されます。



NOTE: この画面での初期選択は、カウント数が最も多いカテゴリーがデフォルトとなります。他のカテゴリのカウントが0でない場合、OKを選択すると、すべてのデバイスの認証設定が選択したカテゴリに変更されます。

適切なセキュリティカテゴリを選択します。例のように、これらのデバイスが他のオフィスに属している場合、「**隣接**」を選択し、「**OK**」ボタンをタップします。



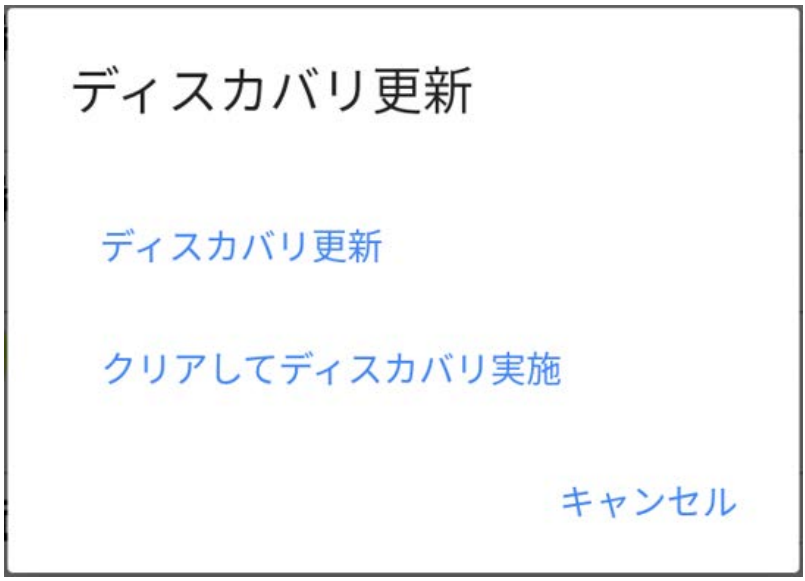
カテゴリーを明確に識別できるようになりました。

他拠点のデバイスは、以下のように識別されます。

NOTE: バッチ認証は、機器のデフォルトのMACアドレスに対して行われます。複数のMACを持つ機器では、デフォルトのMACアドレスにのみ認証が設定されます。未知のスイッチやオフネット機器など、検出されたMACアドレスを持たない機器は、認証設定を行うことはできません。

ディスカバリ更新

ディスカバリのメイン画面の右上にあるアクションオーバーフローアイコン ⋮ をタップし、**ディスカバリ更新**を選択すると、アクティブなディスカバリプロセスがリフレッシュされます。



ディスカバリ更新：すでに検出されたデバイスをクリアすることなく、アクティブな検出プロセスを再スタートします。

クリアしてディスカバリ実施：蓄積された結果をクリアし、ディスカバリプロセスを再スタートします。

ディスカバリ結果をLink-Liveにアップロード

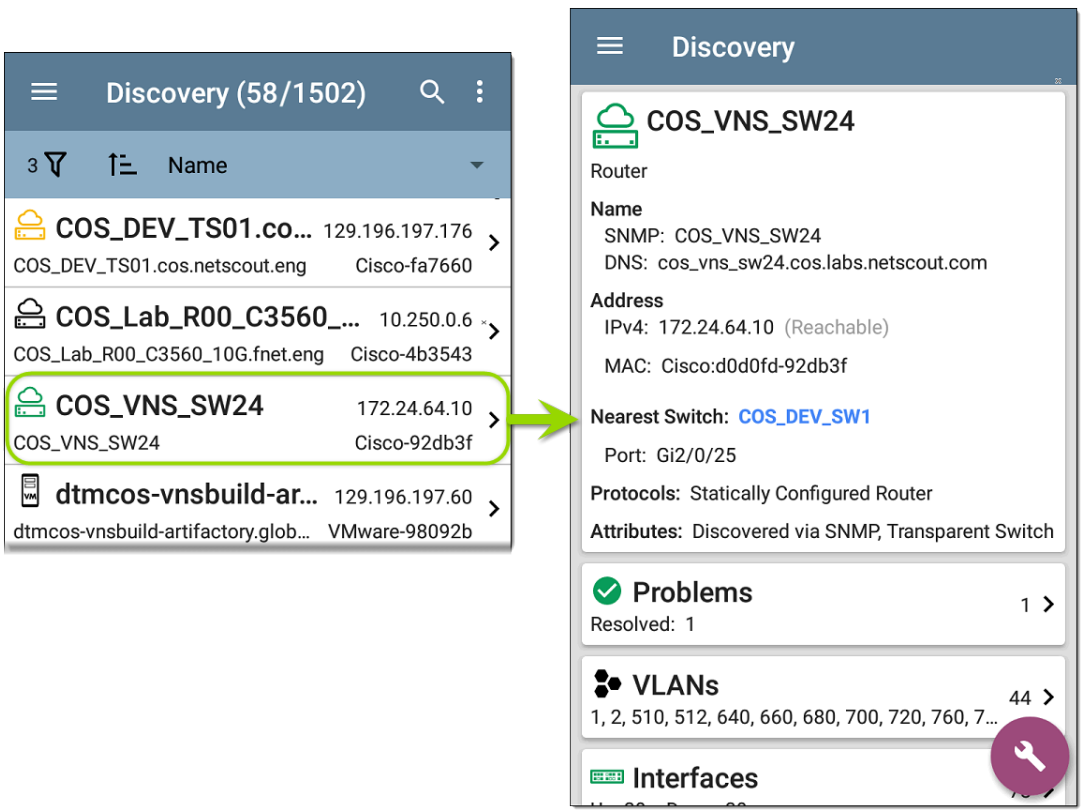
ディスカバリのメイン画面の右上にあるアクションオーバーフローアイコン  をタップし、**Link-Liveへアップロード**を選択すると、現在のディスカバリ結果がLink-Liveの解析ページ  に送信されます。


9:41
56%
Link-Live
by NetAlly
解析名
20230307-094027
コメント
TOYO test
Job コメント
test
解析ファイルに保存

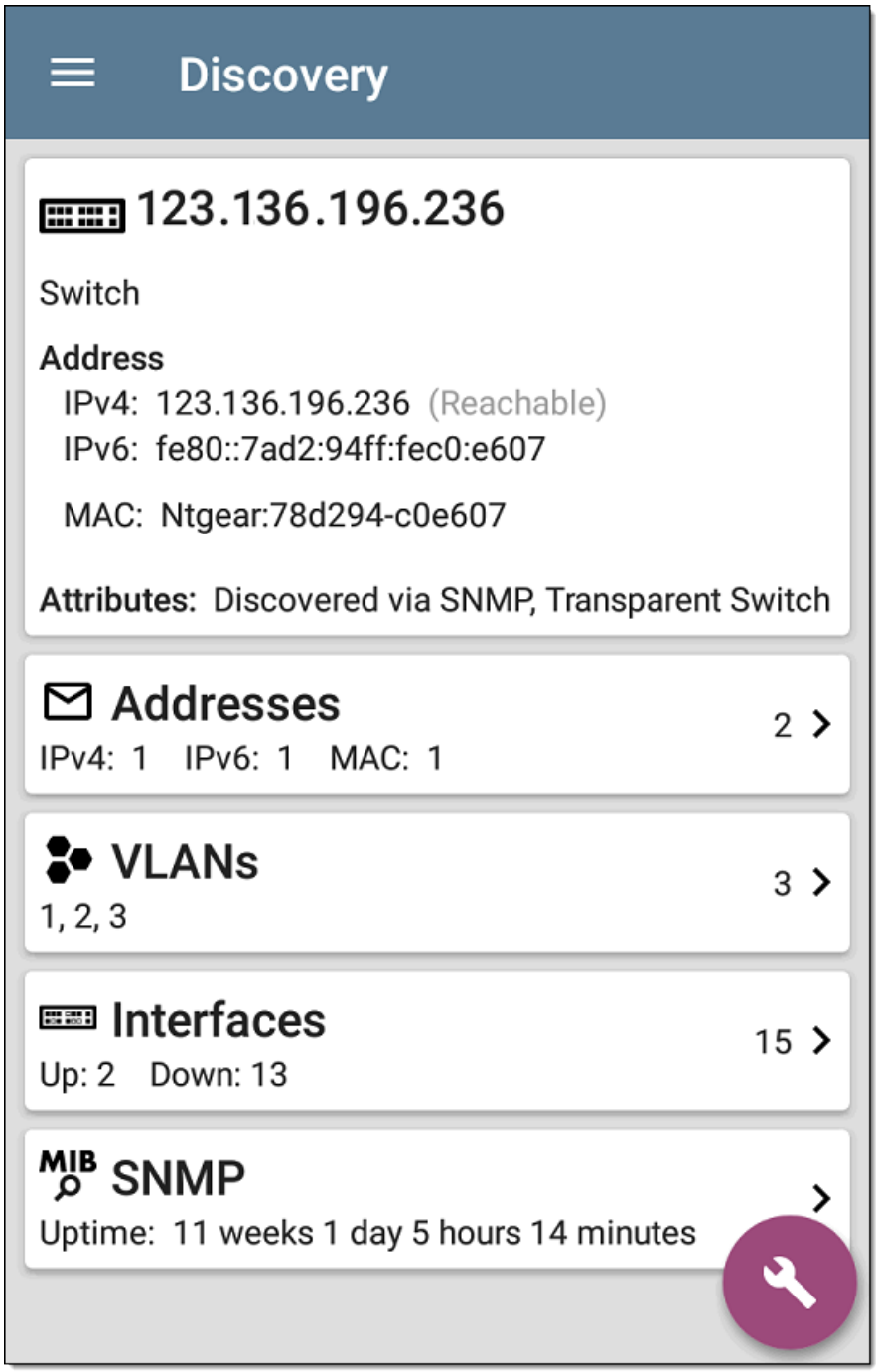
ディスカバリの詳細画面

ディスカバリのメイン画面で、いずれかのデバイスカードをタップすると、デバイスの詳細が表示されます。

以下の例では、ルーターカードとその詳細画面を呼び出しています。



詳細画面で利用できるデータとアクションは、AirCheck G3が検出できたデバイスのタイプ、接続、およびデータによって大きく異なります。つまり、詳細画面には、各デバイスの検出可能な情報のみが表示されます。



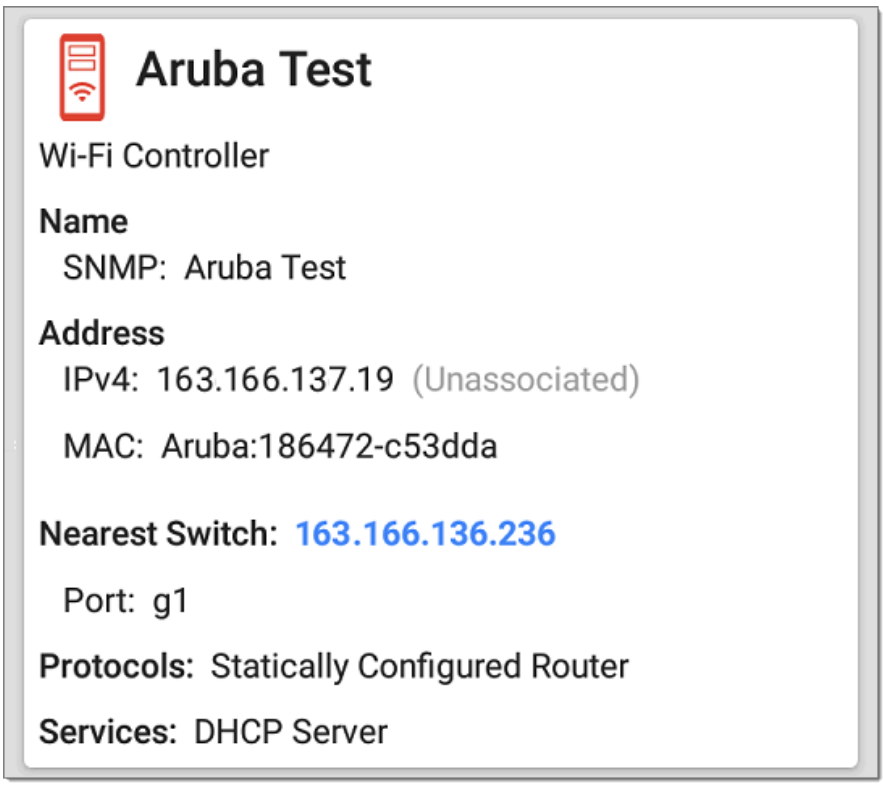
上図の「Switch」画面では、ディスカバリはスイッチのIPアドレスを見つけることができましたが、名前は見つけられませんでした。

各詳細画面には、選択したデバイスに関する追加情報、AirCheck G3によって検出された問題、および接続された他のネットワーク要素または対応するネットワーク要素のカウントが表示されます。

AirCheck G3が検出できる様々なデバイスの詳細については、**デバイスタイプ**を参照してください。

カードの詳細

詳細画面の一番上のカードは、選択したデバイスの検出されたデータをまとめたものです。



カードの上部には、デバイスの種類とアイコンが表示されます（上の画像の例では、**失敗**または**エラー**のステータスを持つWi-Fiコントローラです）。

上部の詳細画面カードに表示される残りのフィールドは、デバイスの種類とAirCheck G3がデバイスについて検出できるものによって異なります。

ディスカバリの詳細画面では、青色のリンク先の名前またはアドレスをタップすると、リンク先のデバイスのディスカバリ画面を開くことができます。

> **NOTE**: 下線のないリンクは同じアプリ（この場合はディスカバリ）で開き、下線のあるリンクは別のアプリで開きます .

上の画面イメージのリンクと下線のあるCisco MACアドレスは、Wi-FiアプリのAP詳細画面を開き、Lightweight APに関連する他の無線属性を表示することができます。近接のスイッチとWi-Fiコントローラのリンクは、これらのデバイスのディスカバリアプリの詳細画面を開きます。

カード詳細のデータフィールド

デバイスの詳細画面では、デバイスの種類とAirCheck G3が検出できた情報に応じて、以下のフィールドがカードに表示される場合があります:

名前：検出されたデバイスのホスト名。このセクションでは、検出されたユーザー定義、DNS、mDNS、SNMP、NetBIOS、AP、および仮想マシン名を表示できます。

アドレス：デバイスのIPv4、IPv6、BSSID、および/またはMACアドレスを検出します。このセクションでは、各タイプのデフォルト（最初に検出された）アドレスが表示されます。より多くのアドレスが利用可能な場合は、アドレスカードを選択します。

認可：このフィールドは、ユーザーによって割り当てられたデバイスの認証ステータスを表示します。

802.11：無線データ

チャネル：デバイスが動作しているWi-Fiチャネル

タイプ：デバイスがサポートする802.11メディアタイプ

近接スイッチ：デバイスに最も近いと特定されたスイッチの名前またはアドレス

ポート：デバイスが接続されている物理ポート

VLAN ID：デバイスが所属するVLANのID

プロトコル：パケット解析により検出された、機器またはネットワークで動作するルーティングプロトコル

サーバ：DHCPやDNSなど、このデバイスが提供するネットワークサービス

属性：その他、検出されたデバイスの属性

Wi-Fi コントローラ：Lightweight APのWi-Fiコントローラーの名前とアドレス

AP：接続先のアクセスポイント

SSID：機器が動作しているネットワークの名称

セキュリティ：APのセキュリティタイプ

ハイパーバイザ：仮想マシンが動作しているハイパーバイザーの名前

仮想マシン：仮想マシンの名前

ゲストOS：仮想マシン上で動作するOS

メモリ予約：仮想マシンに確保されたメモリ量

最終検出：AirCheck G3が直近でデバイスを検出した時間

下位のデバイス詳細カード

デバイスの詳細画面の下のカードをタップすると、より詳細な特性が表示され、選択したデバイスの特定の問題、アドレス、インターフェイスなどにドリルダウンすることができます。

以下、ソート一覧オプションでアドレスなどでソートができます。

このトピックの残りの部分では、各タイプの詳細画面の例と、追加解析のオプションについて説明します。

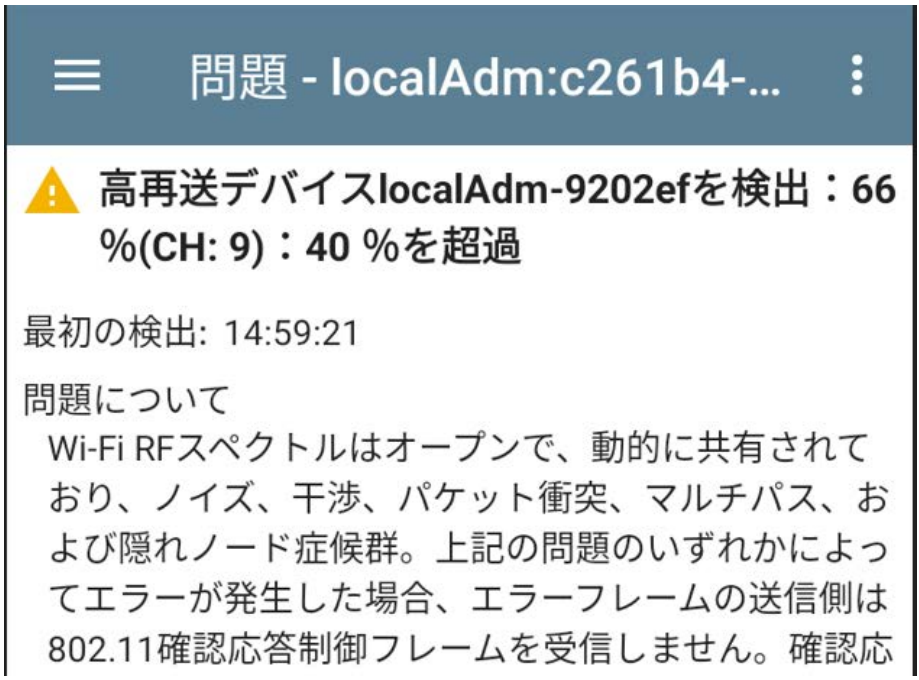
問題

問題カードには、最も深刻度の高い問題のアイコンの色と、デバイスまたはネットワークコンポーネントの**警告**、**失敗**または**エラー**、**情報**、および**解決**された状態の検出数が表示されます。

問題カードをタップすると、問題の一覧画面が表示されます（ただし、問題が1つしか検出されない場合は、一覧画面をスキップして問題の詳細説明が表示されます）。

ソートフィールドをタップすると、リストを深刻度順、または問題が最初に検出された時間順で並べ替えることができます。

問題一覧画面で、問題の行をタップすると、詳細な説明が表示されます。

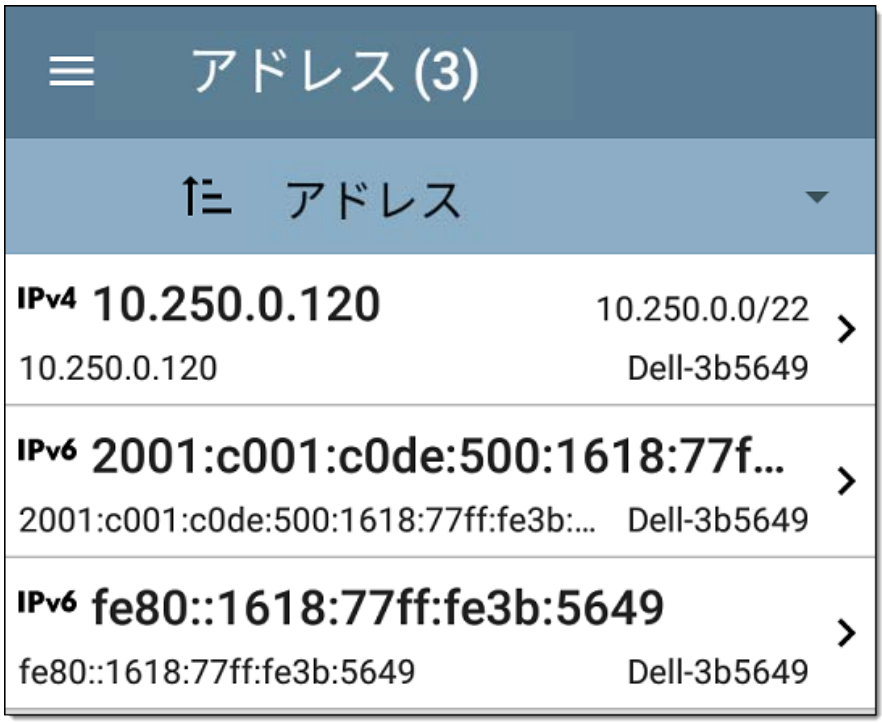


問題をクリアするには、問題リストまたは説明画面の右上にあるアクションオーバーフローボタン ⋮ をタップし、**全問題をクリア**をタップします。

問題設定を参照して、ユニットによって検出および表示される問題を設定してください。

アドレス

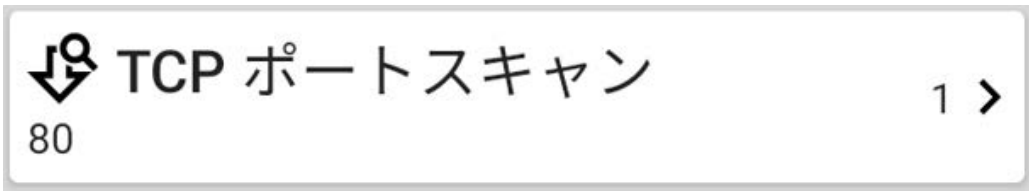
アドレスカードには、検出された各タイプのアドレス（IPv4、IPv6、MAC、BSSID）の数が表示されます。タップしてアドレスと関連情報を表示します。



アドレス一覧画面では、一覧の順番を並べ替えたり、検出されたアドレスをタップしてさらに調べることができます。

TCPポートスキャン

デバイスまたはIPアドレスに対してTCPポートスキャン（**ディスカバリFAB**から）を実行した場合、デバイスの詳細画面にTCPポートスキャンカードが表示されます。



このカードは、開いているポート番号の一覧と、開いているポートの総量を表示します。カードをタップすると、**TCPポートスキャン**画面が表示されます。

この画面は、**ディスカバリのフローティングアクションメニュー**からも開くことができます。

TCPポートスキャン結果画面の上部には、テスト対象機器の名称またはIPアドレスと、以下の項目が表示されます:

IPアドレス：スキャンされたデバイスのIPアドレス

インターフェース：TCPポートスキャン設定で設定した、テスト実行元のテストポートまたは管理ポート

スキャンリスト： テストしたポート番号のリスト

結果

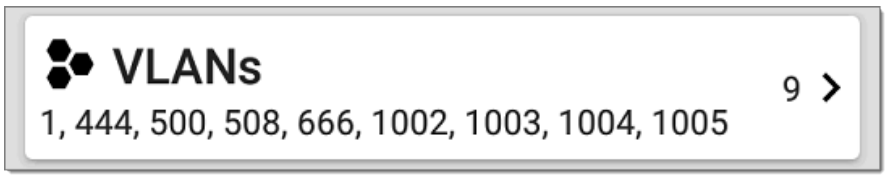
ステータス：ポートスキャンの現在のステータス

ポート/説明：検出されたすべてのオープンポートの一覧とその説明

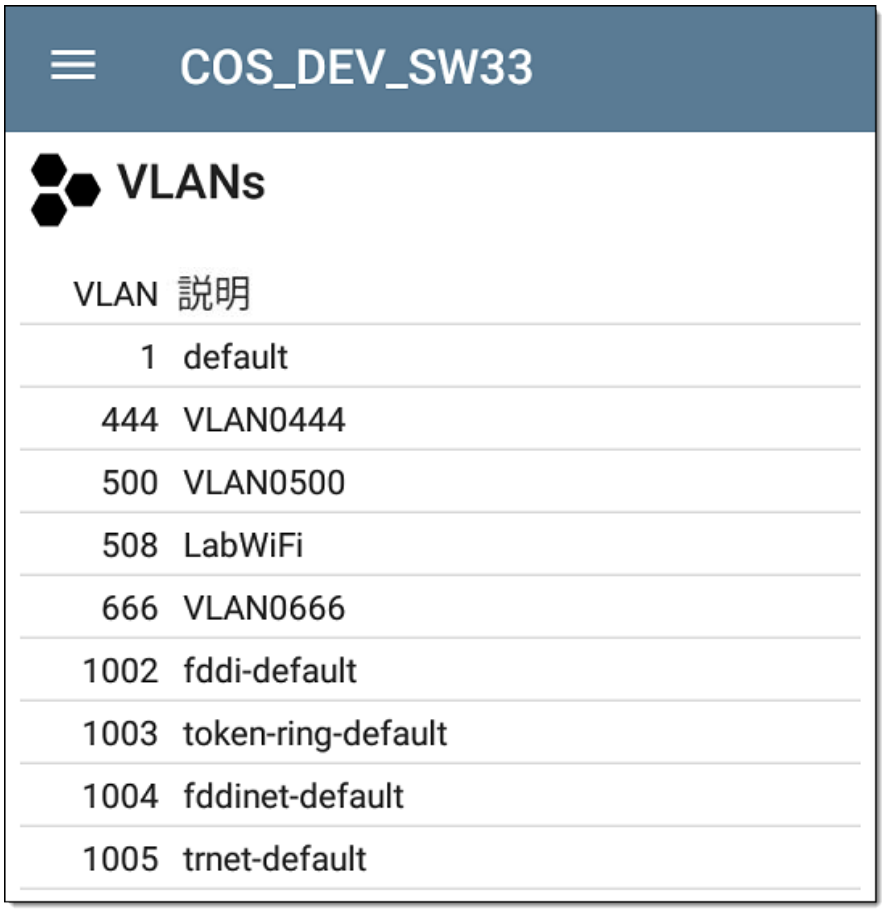
TCPポートスキャン設定を参照してください。

VLANs

VLANsカードには、ユニットが使用している、または設定されているVLAN IDが表示されます。



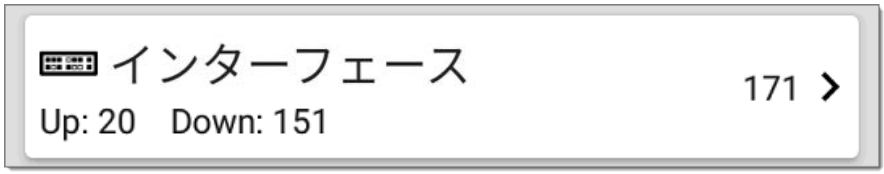
VLANが検出または設定されていない場合、このカードは表示されません。カードをタップすると、VLANs画面が表示されます。



VLANsの詳細画面では、各VLAN IDとともに説明文も表示されます。

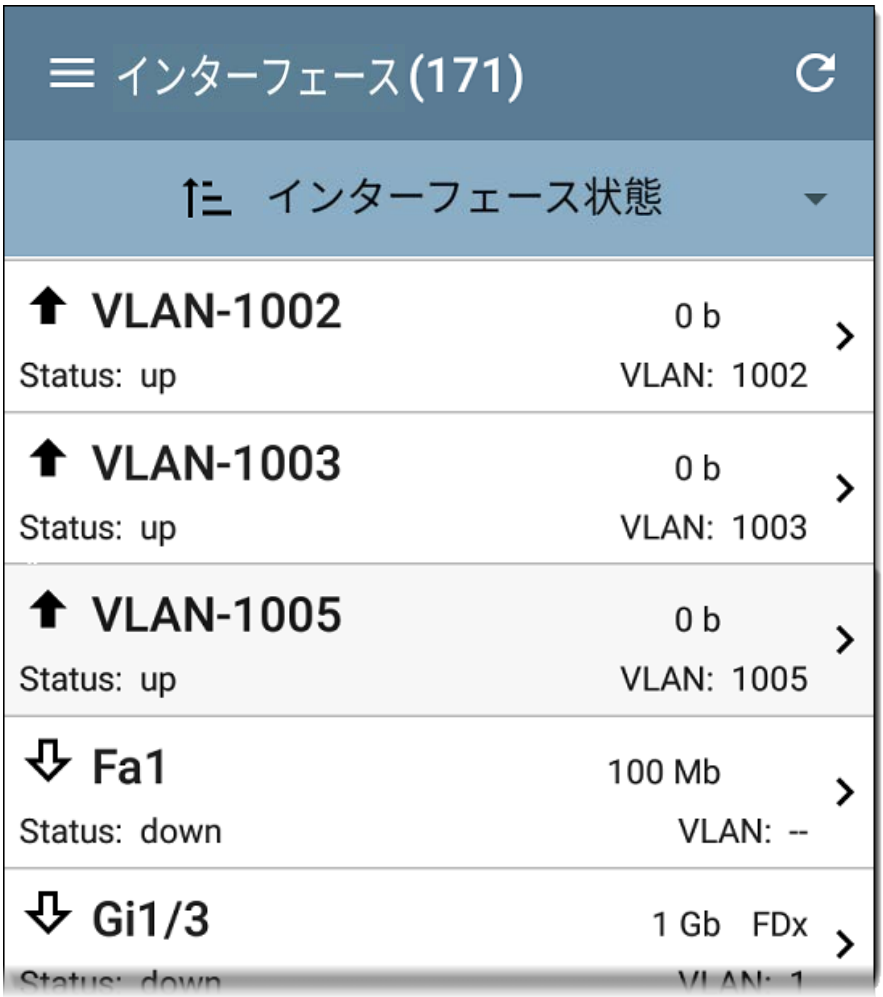
インターフェース

インターフェースはSNMPで検出されます。



インターフェースカードには、UpとDownのインターフェイスの数と、右側のインターフェイスの総数が表示されます。

カードをタップすると、インターフェースのリストが表示されます。



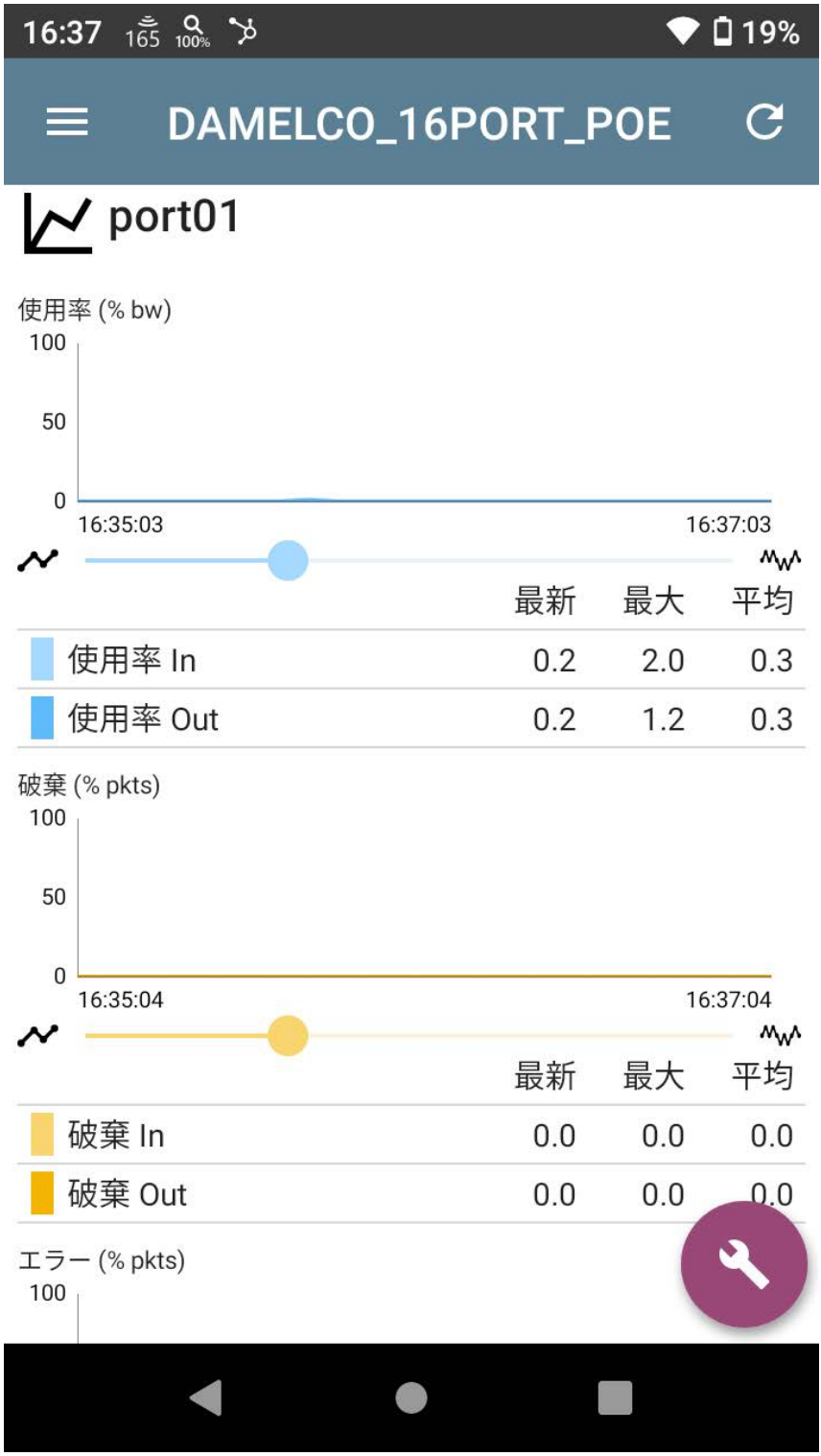
他のディスカバリ リスト画面と同様に、インターフェースリストにはいくつかのソートオプションがあり、選択したソートオプションは表示される情報の種類に影響します。上の画像は、**インターフェース状態**(上または下)でソートして表示したものです。下の画像は、**MACアドレス**順に並べたもので、各インターフェイスのMACアドレスが表示されます。

インターフェースの行をタップすると、選択したインターフェースの新しいディスカバリ詳細画面が表示されます。

インターフェースの詳細画面には、インターフェースの説明と、ステータス、接続デバイスとポート、アドレスに関する情報が表示されます。

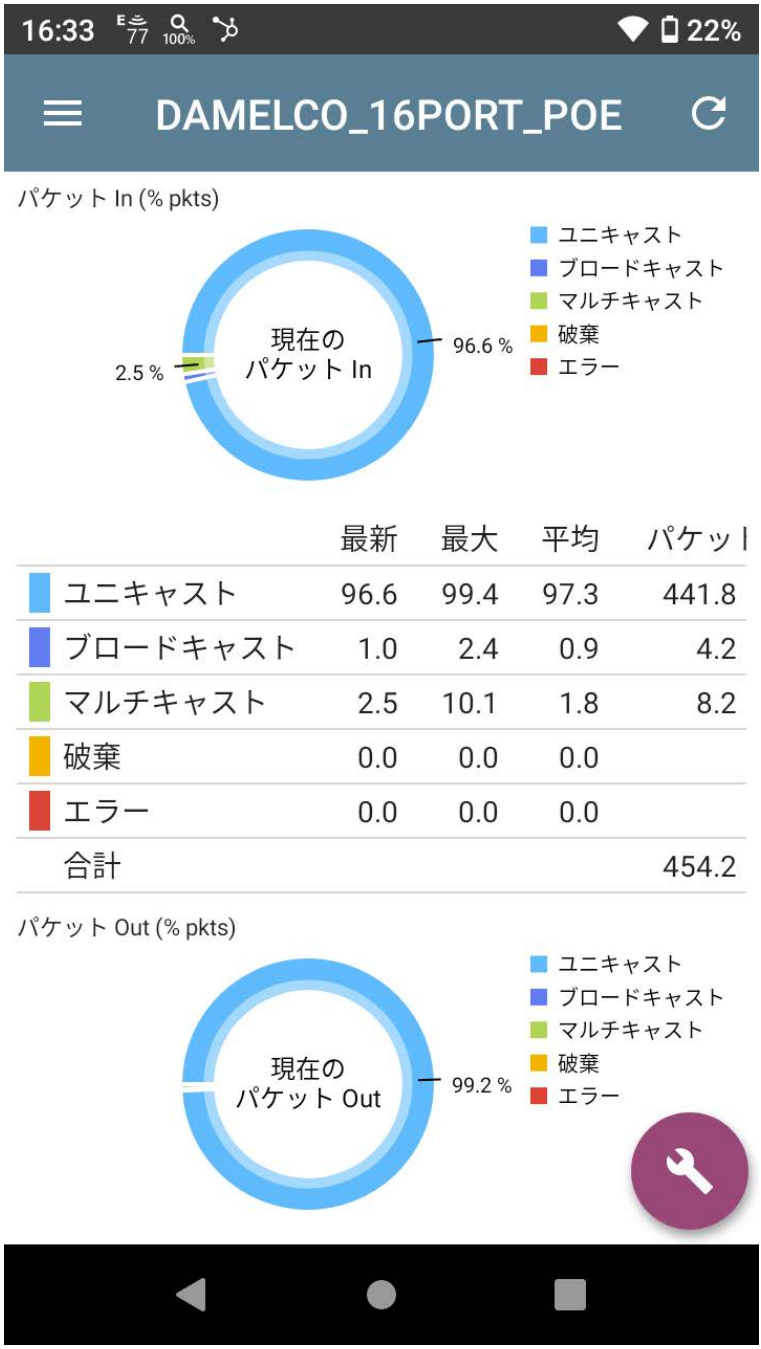
MTU：最大伝送単位、インターフェースポートに設定されている最大パケットフレームサイズ

この画面で下の統計カードをタップすると、インターフェイスの検出VLANとデバイス、およびインターフェイスの統計グラフを確認できます。



統計画面では、使用率、パケット廃棄数、パケットエラー数のリアルタイムなトレンドグラフが表示されます。

トレンドグラフの下には、インターフェースへのパケット転送量とインターフェースからのパケット転送量の円グラフが表示されます。



SNMP

このカードは、SNMPで収集したデバイスの詳細と、デバイスへのSNMP接続を表示します。

SNMPカードには、**SNMP Uptime**が表示されます。カードをタップすると、SNMPの詳細が表示されます。

SNMP システムグループ：これらのデータフィールドは、システムグループやその他の主要なデバイスのバージョン情報から収集されます。

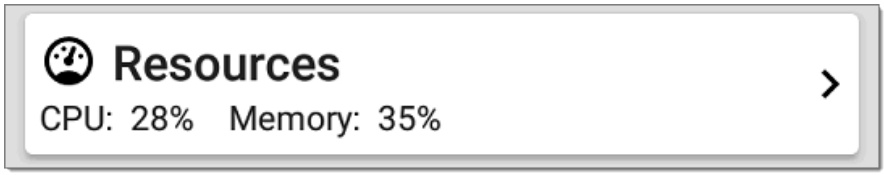
SNMP：デバイスがサポートするSNMPバージョン、エンジン ID（v3の場合）、および AirCheck G3がデバイスと現在どのように通信しているか、使用中のコミュニティ ストリングを含む資格情報とともに説明します。

接続デバイスs

接続デバイスsカードは、**不明な(非管理)スイッチ**の詳細画面に表示されます。AirCheck G3は、接続されているスイッチを直接識別できない場合がありますが、それに接続されているデバイスは、スイッチが動作している場所に関する手がかりを提供します。

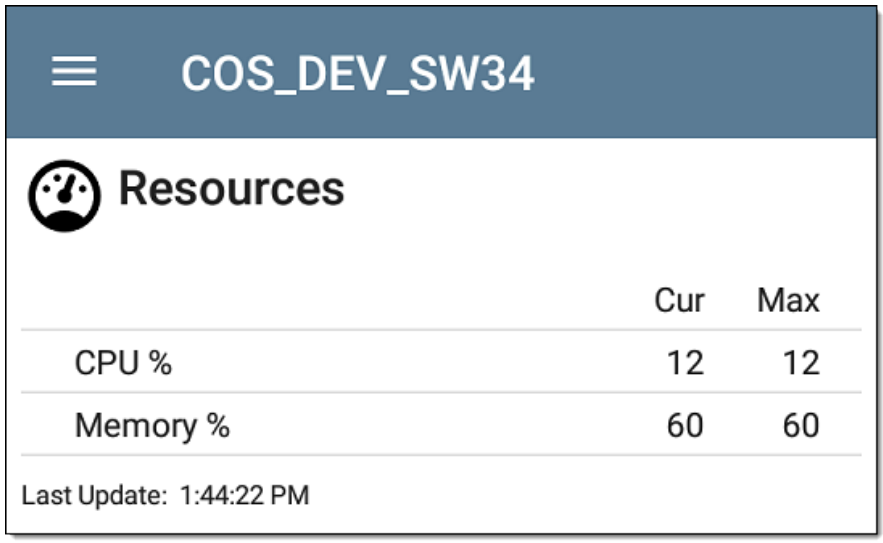
接続デバイスsカードには、不明なスイッチに接続されている、検出されたデバイスの数が表示されます。カードをタップすると、接続されたデバイスを含む検出リスト画面が開きます。

Resources



リソースカードは、デバイスのCPU、メモリ、ストレージの使用率のパーセンテージを表示します。この情報は、SNMP経由で収集されます。

カードをタップすると、現在および最大リソース使用率の測定値が表示されます。

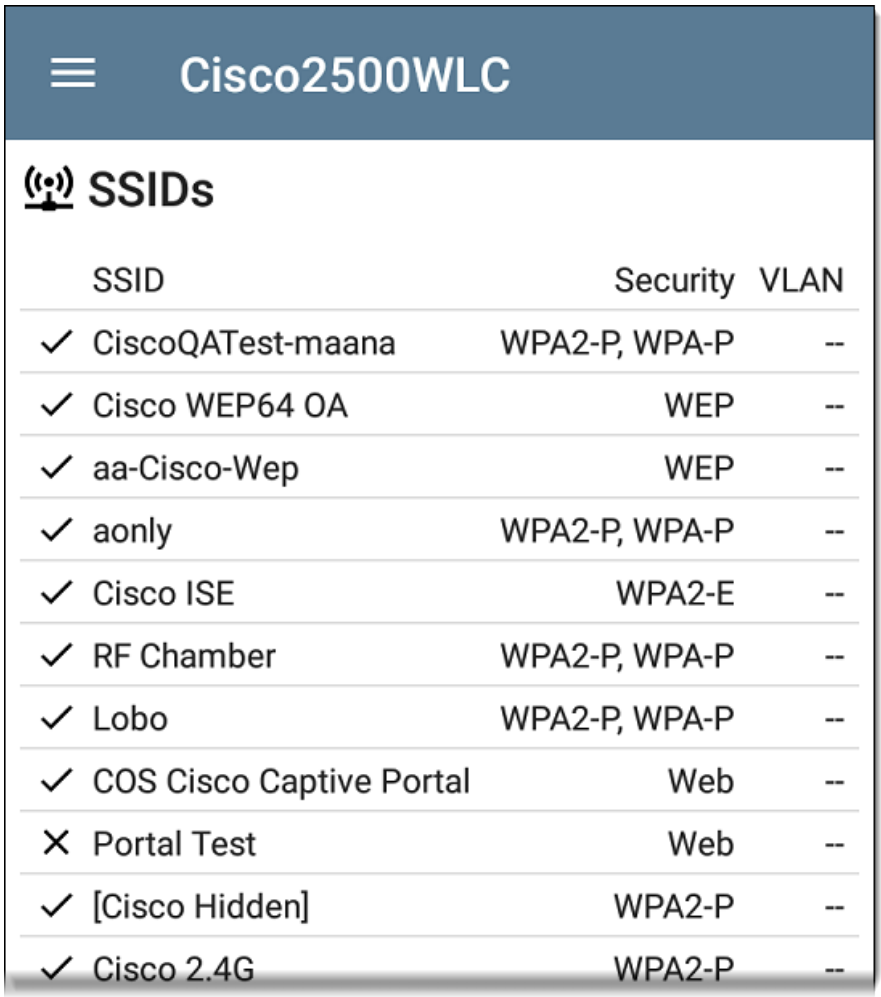


デフォルトでは、CPU、メモリ、またはストレージの使用率が90%を超えると、AirCheck G3は**警告**ステータスを表示します。 問題の検出やしきい値は、ディスカバリのナビゲーションドロワーからアクセスする**問題設定**で調整できます。

SSIDs

SSIDsカードは、**Wi-Fiコントローラー**の詳細に表示されます。この情報は、SNMPで収集されます。

このカードは、SNMPから収集したSSIDの数を表示します。カードをタップすると、SSIDの一覧が表示されます。



SSIDsの画面では、各SSIDのセキュリティタイプ、VLANが表示されます。左側にチェックマークがあるSSIDは有効、×があるSSIDは無効です。

ディスカバリのフローティングアクションボタン

詳細画面のフローティングアクションボタン（FAB）は、デバイスの種類や利用可能な接続に応じた追加アクションを提供します。

詳細画面から
パス解析、Ping/TCP、キャプチャなど他のNetAllyアプリを開くと、新しいアプリにデバイス名やアドレスが自動入力されます。このように、ディスカバリアプリとWi-Fiアプリの両方が便利なショートカットを提供し、他のテストアプリで宛先アドレスやホスト名の入力を省略できます。

- TCPポートスキャンをタップすると、ディスカバリアプリでTCPポートスキャン画面が表示されます。
- ブラウズを選択すると、Google Chromiumが開きます。

- テストターゲットを追加をタップすると、現在選択されているデバイスに一致する新しい自動テスト宛先が作成されます。テストの種類を選択するダイアログが表示され、自動テストアプリが起動し、新しく追加されたターゲットの設定が表示され、さらにカスタマイズすることができます。
- MACアドレスまたはBSSIDを持つデバイスの場合、名前と認可をタップすると、カスタムユーザ名と認証ステータスを割り当てることができるダイアログが表示されます。
- **その他**をタップすると、追加のフローティングアクションボタンのセカンダリリストが表示されます。**戻る**をタップすると、元のリストに戻ります。
- TelnetまたはSSHは、JuiceSSHアプリを開きます。

デバイスアドレスの自動入力

FABから他のアプリを開くと、トップ詳細カードにデフォルトでアドレスと名前が入力されます。

例えば、下の詳細画面に表示されているルーターは、複数のIPv4アドレスとMACアドレスを持っています（アドレスカードをタップすることで確認できます）。

FABを開いてパス解析など別のアプリを選択した場合、パス解析アプリでは詳細画面の上部に記載されたアドレスと名前のみが入力されます。


DAMELCO_16PORT_POE
スイッチ, SNMP Agent
名前
SNMP: DAMELCO_16PORT_POE
パス解析
アドレス
IPv4: 192.168.3.212 (到達)
Ping/TCP
PING TCP
MAC: Buffalo:106f3f-978f9b
TCP ポートスキャン
近接スイッチ: ~ Unknown Switch 1 ~
属性: SNMP経由で検出, Transpar
ブラウズ
VLANs
1
テストターゲットを追加
インターフェース
名前と認可
Up: 2 Down: 0
その他
MIB SNMP
Uptime: 13 weeks 1 日 10 時間 39 分

別のアドレスで別の画面やアプリを開くには、アドレスカードを開き、別のアドレスを選択してその詳細画面を表示します。

デバイスタイプ

ディスカバアプリは、このセクションで説明するタイプのデバイスをリストアップして解析します。デバイスの種類、検出方法、および構成された設定によって、AirCheck G3で異なるデータを利用できる場合があります。

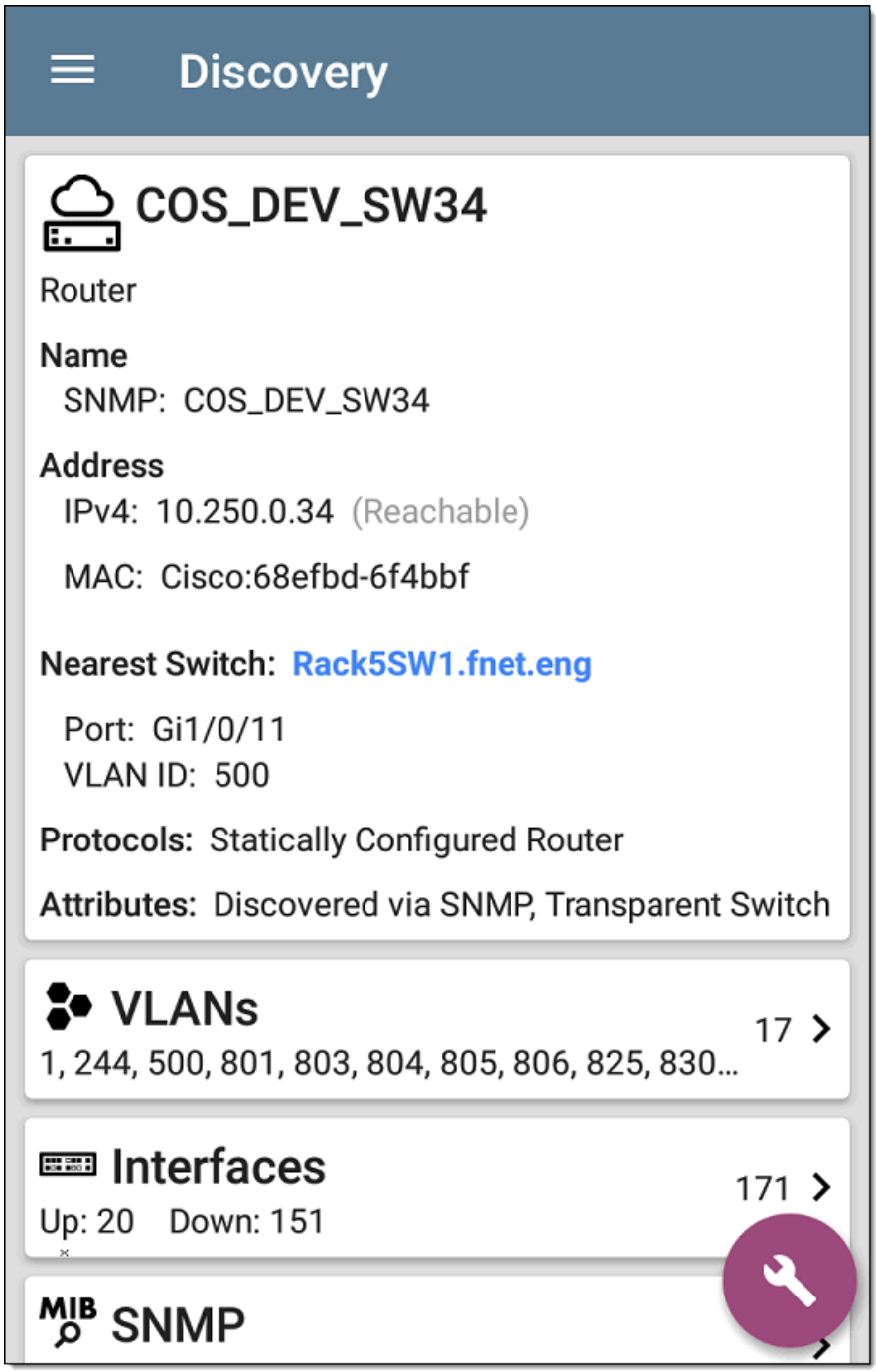
SNMPの設定および**他のデバイスを介して検出されたデバイス**、**ディスカバリ設定**を参照してください。

各詳細カードや画面の説明については、**ディスカバリの詳細画面**を参照してください。

このセクションの残りの部分の画像は、ディスカバリが各デバイスタイプに対して表示するデータの一例を示しています。

ルータ

AirCheck G3は、トラフィックを監視し、ホストにクエリを実行して、IPルーターを検出します。



スイッチ

スイッチは、トラフィックの監視とホストのクエリによっても検出されます。

Unknown Switches

不明なスイッチは、周囲のスイッチを通過するトラフィックを解析することで間接的に検出されます。AirCheck G3は、スイッチを特定することはできませんが、その空間のデバイスMACアドレスを通じて、ネットワーク上でスイッチがアクティブになっている場所を感知することができます。

AirCheck G3は、検出されたスイッチに番号を付けます。(これらの番号は、検出プロセスが実行されるたびに変更される場合があります)。

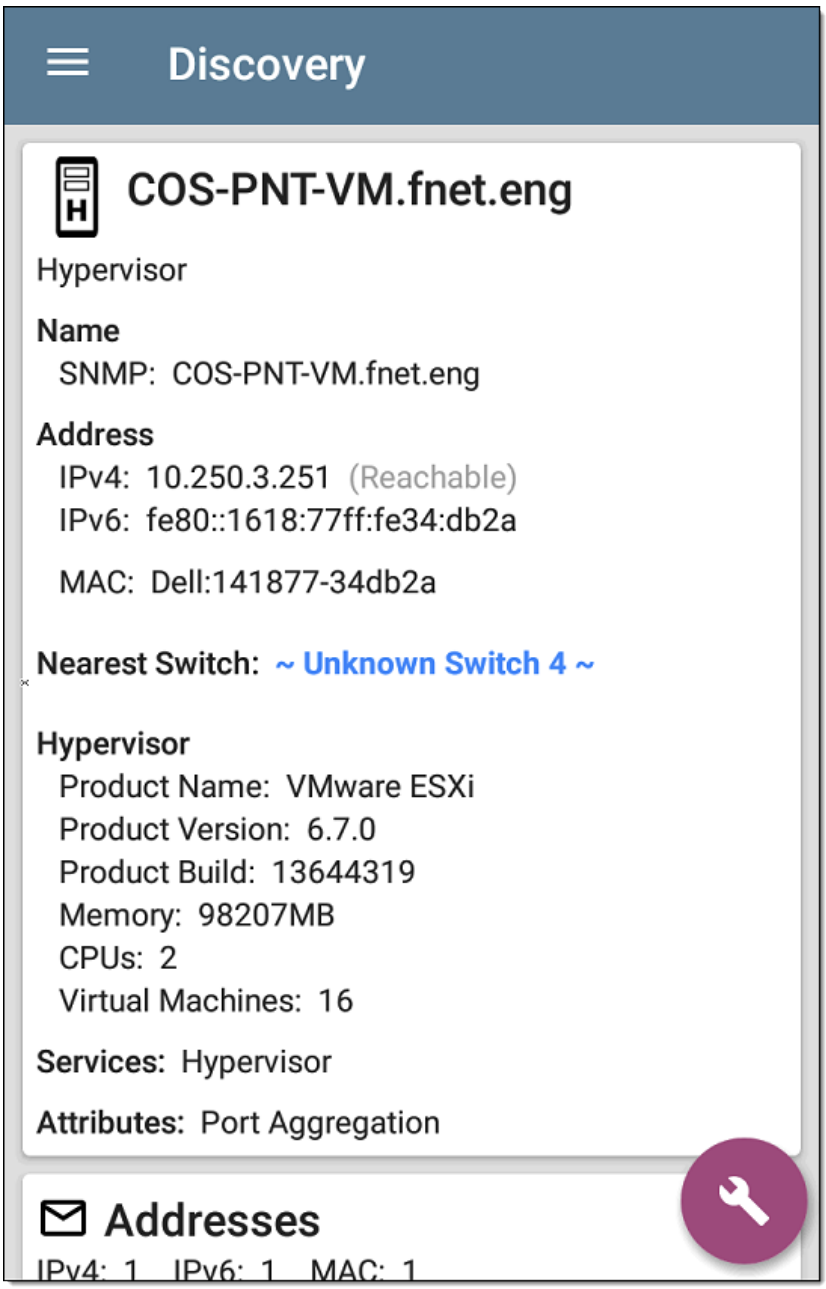
Unknown Switchの詳細画面には、スイッチに接続されているデバイスの数が表示されます。**接続デバイスs**カードをタップすると、接続されているデバイスが表示され、不明なスイッチの場所に関する手がかりとなる場合があります。

ネットワークサーバ

ネットワークサーバには、NetBIOSサーバ、DHCPサーバ、DNSサーバなどが含まれます。

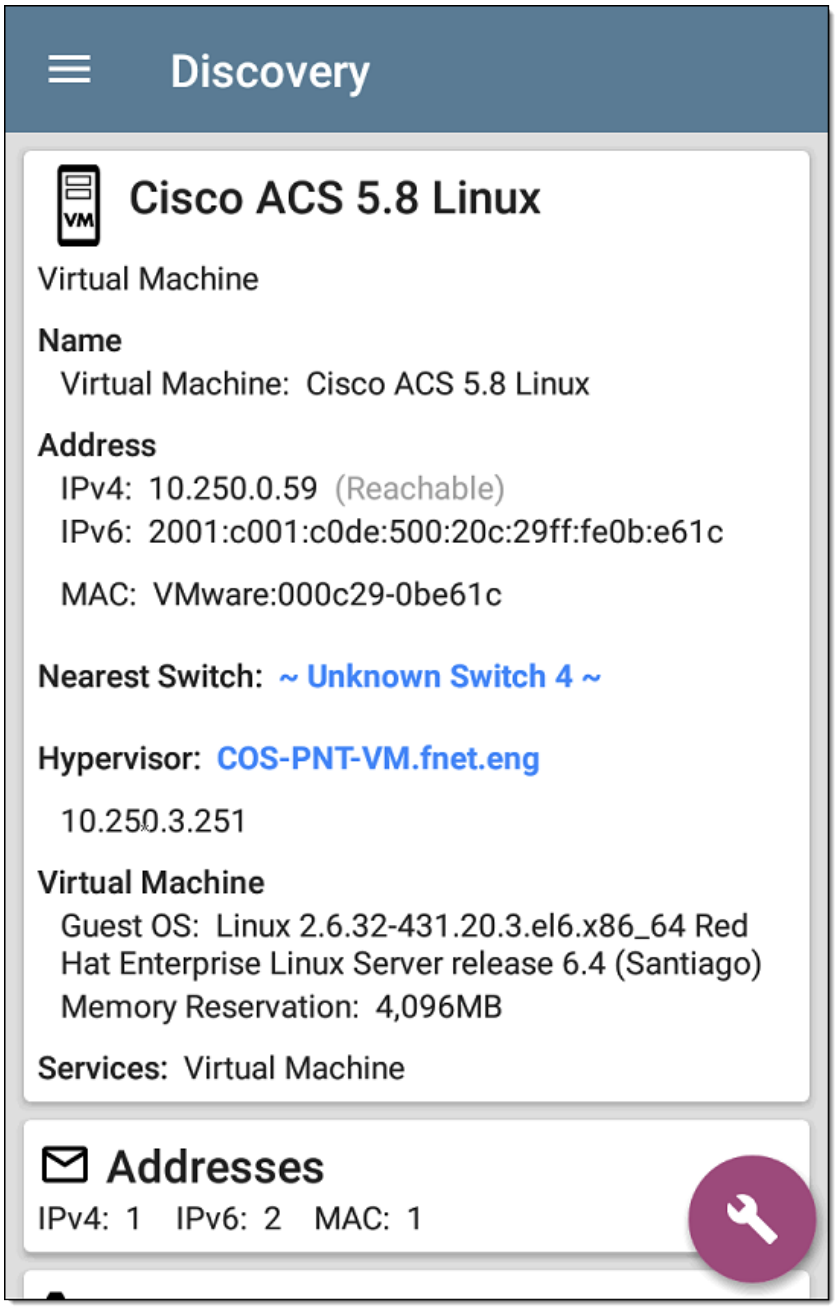
ハイパーバイザー

VMwareハイパーバイザーは、SNMPを介して検出されます。AirCheck G3がハイパーバイザーを検出し、ハイパーバイザーとして分類するには、ハイパーバイザーのSNMPエージェントが有効である必要があります。



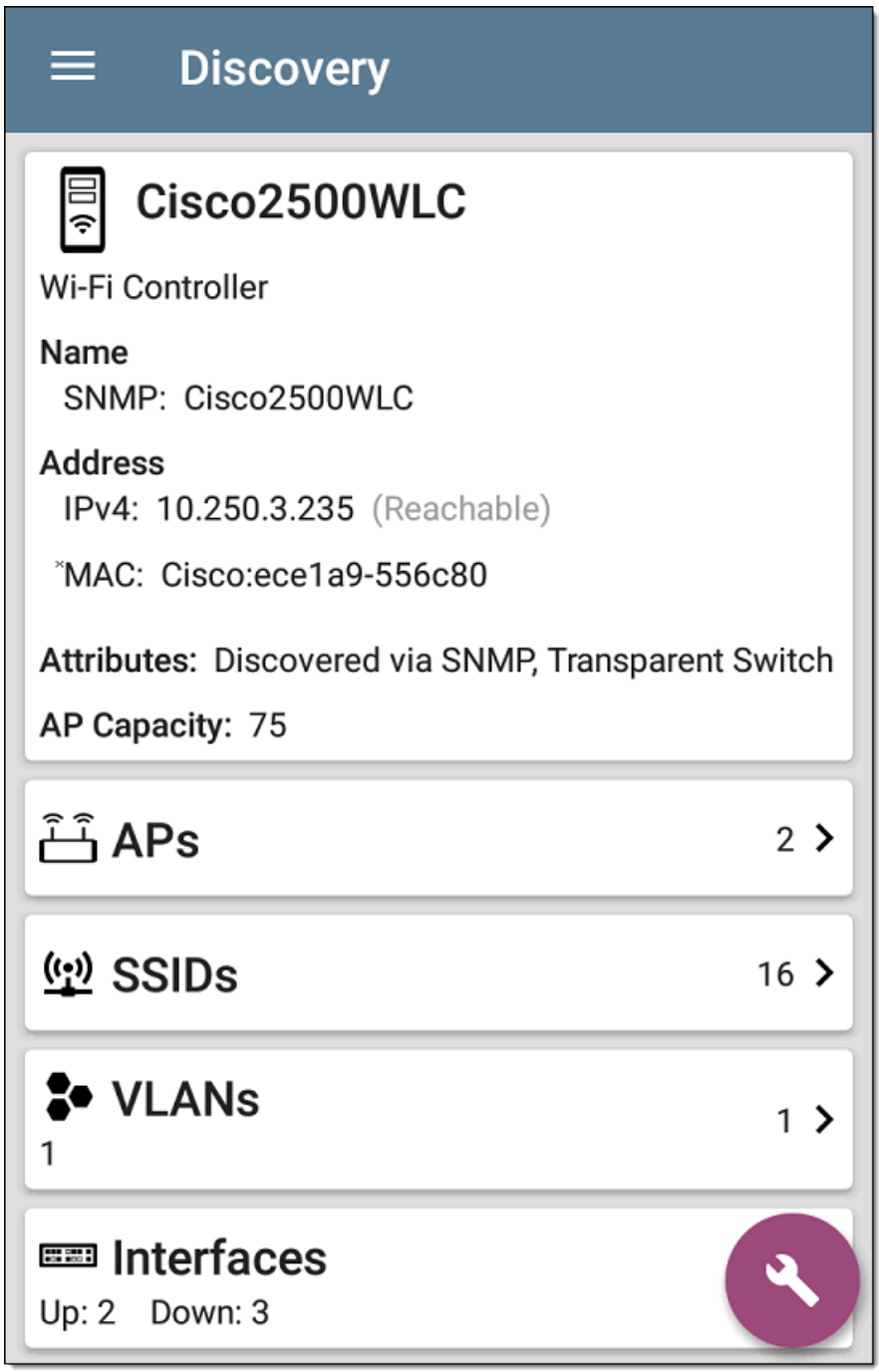
仮想マシン

VMwareの仮想マシンは、SNMP対応のVMwareハイパーバイザーのVMwareクライアントテーブルから発見されます。また、デバイスは、VMware MACを持つ場合、仮想マシンとして分類されます。



Wi-Fi コントローラー

AirCheck G3は、CiscoやAruba Wi-Fiコントローラーを含む、SNMP対応のWi-Fiコントローラーを検出できます。



アクセスポイント(APs)

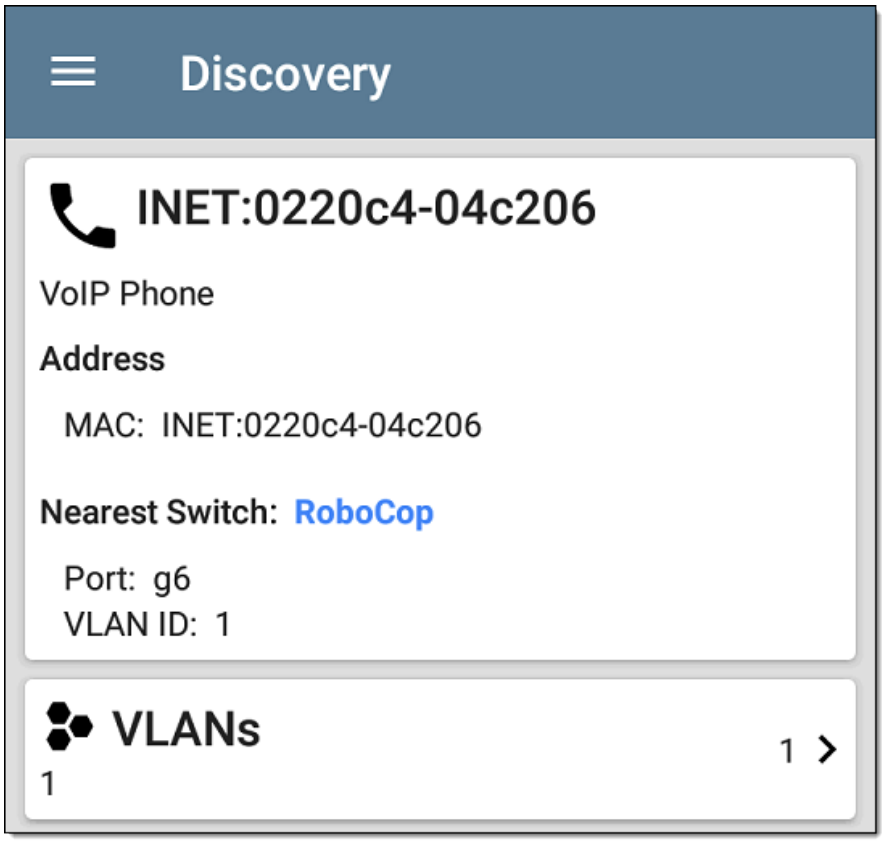
AirCheck G3は、管理ポートまたはテストポートを介したリンク接続により、無線パケット解析とSNMPクエリを通じてAPを検出します。

Wi-Fi クライアント

ワイヤレスクライアントは、管理ポートまたはテストポートを介したリンク接続で、ワイヤレスパケット解析とSNMPクエリによって発見されます。

VoIP Phones

VoIP ディスカバリは、ネットワークのVoIPとレイヤー2/3のコンフィギュレーションを可視化します。



プリンタ

AirCheck G3は、SNMP Printer MIB を介してIPプリンターを識別し、診断要求とクエリによってIPXプリンターを識別します。

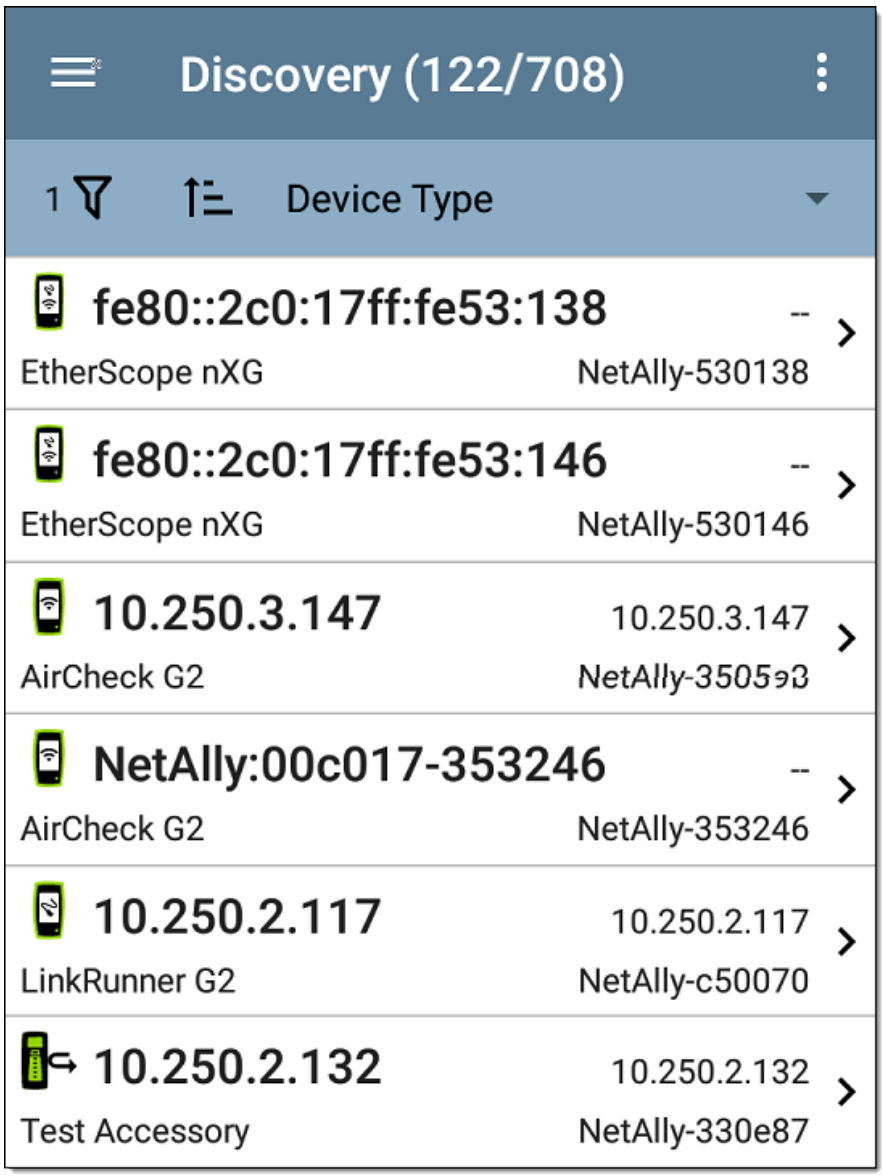
SNMP Agent

SNMPエージェントは、SNMPクエリを使用して検出されます。**SNMPの設定**を参照してください。

> **NOTE**: AirCheck G3がデバイス上のSNMPエージェントを検出できない場合、デバイスが管理サブネットなどの別のサブネットに接続されている可能性があります。サブネットを**拡張レンジ**に追加することで、この問題を解決します。

NetAlly ツール

AirCheck G3は、AirCheck G3、AirCheck G2、LinkRunner(ATとG2)、およびテストアクセサリなど、他の NetAllyネットワークテスターも識別できます。

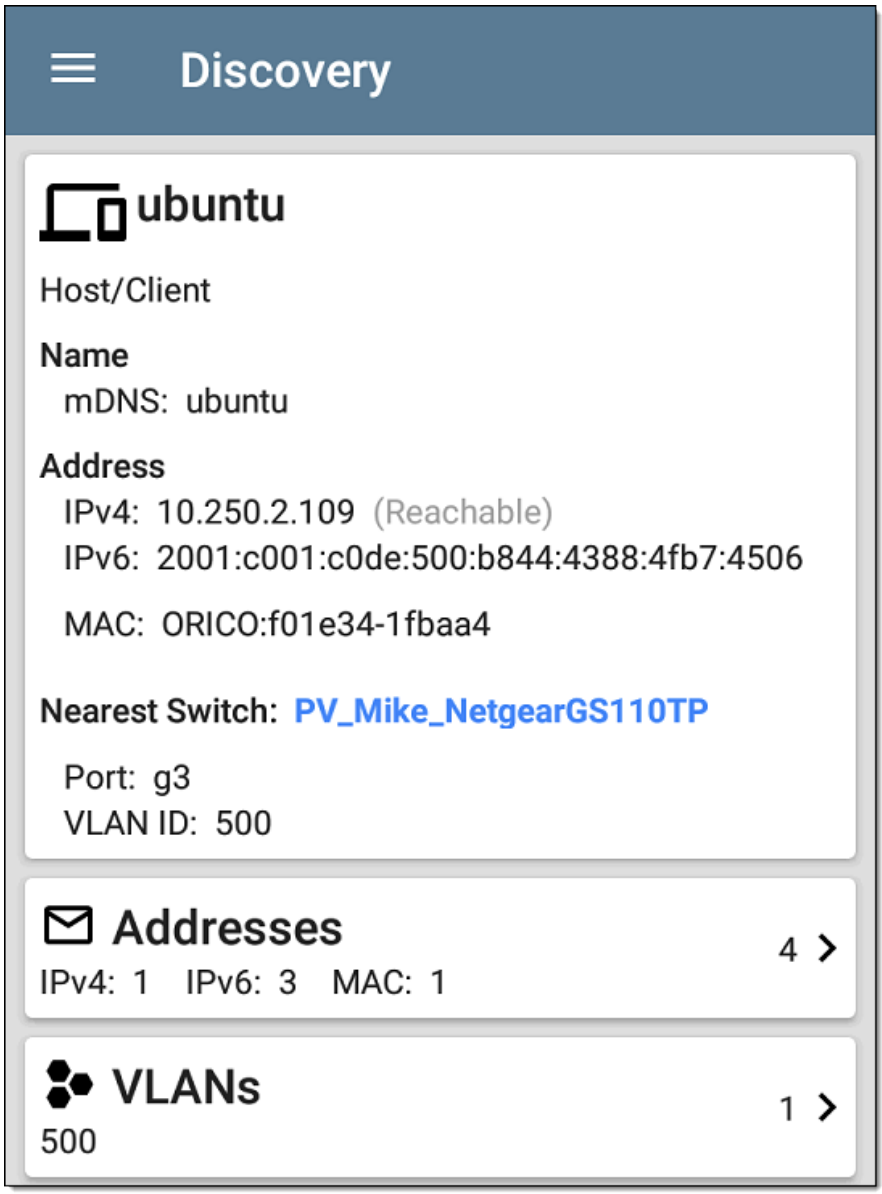


上の画像は、メインのディスカバリ リストに表示されるいくつかのNetAllyツールです。

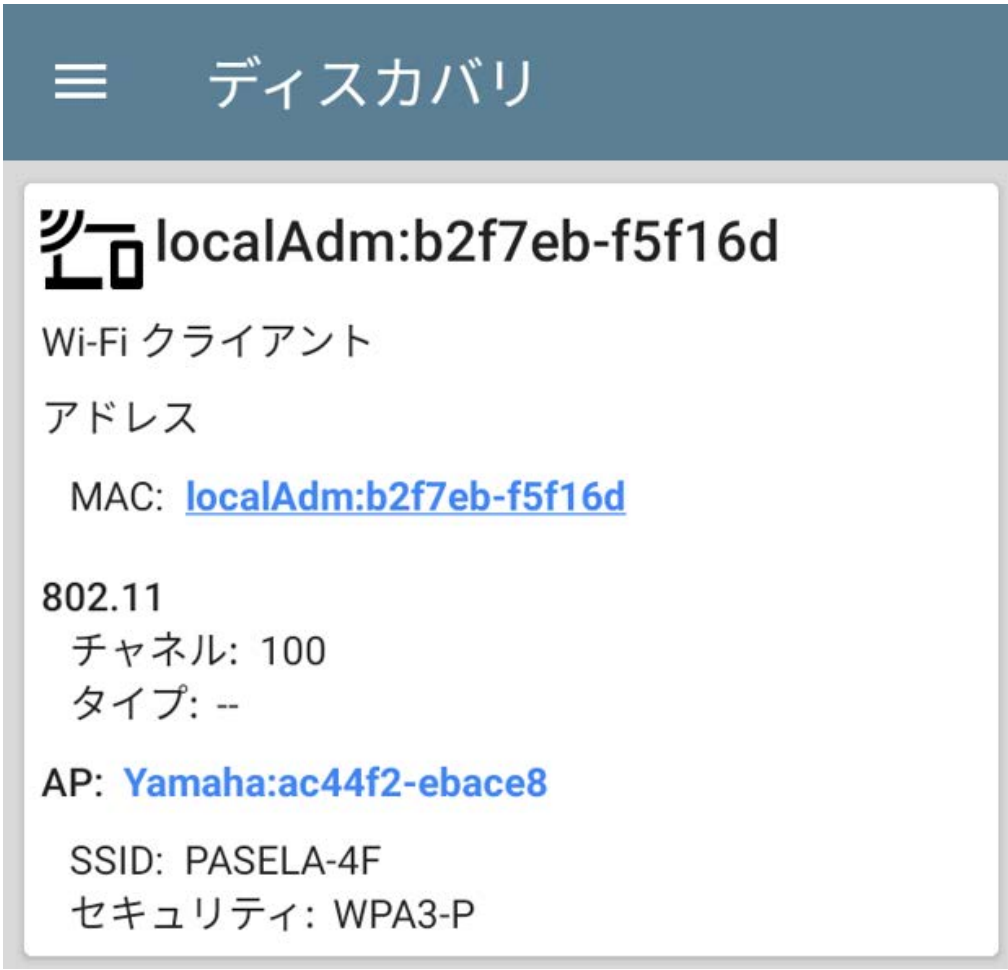
AirCheck G3は、各ツールについて収集できるすべての情報を詳細画面に表示します。

Hosts/Clients

その他のホストやクライアントは、トラフィックの監視や問合せによって検出されます。ホストが他のカテゴリー（スイッチ、ルーター、VoIPデバイスなど）に属すると特定できない場合は、Host/Clientトに分類されます。



NOTE: LocalAdmで始まるMACアドレスは、不正な追跡を防ぐために、アドレスがローカルにランダム化されていることを示します。


ディスカバリ
localAdm:b2f7eb-f5f16d
Wi-Fi クライアント
アドレス
MAC: localAdm:b2f7eb-f5f16d
802.11
チャネル: 100
タイプ: --
AP: Yamaha:ac44f2-ebace8
SSID: PASELA-4F
セキュリティ: WPA3-P

ディスカバリ設定

ディスカバリ設定には、SNMP設定、コミュニティ・ストリングとその順序、クレデンシャルセット、ポート、拡張レンジ、プロセス間隔が含まれます。

左側のナビゲーションドロワーをスライドさせるか、メニューアイコン をタップし、**ディスカバリ設定**を選択することで、ディスカバリ設定画面にアクセスできます。

(ここをタップすると、**問題設定**、**TCPポートスキャン**に移動できます。)

ディスカバリ設定の調整:

1. ディスカバリ設定画面で、必要に応じてこのトピックで説明する各フィールドをタップして、必要な設定を選択または入力します。

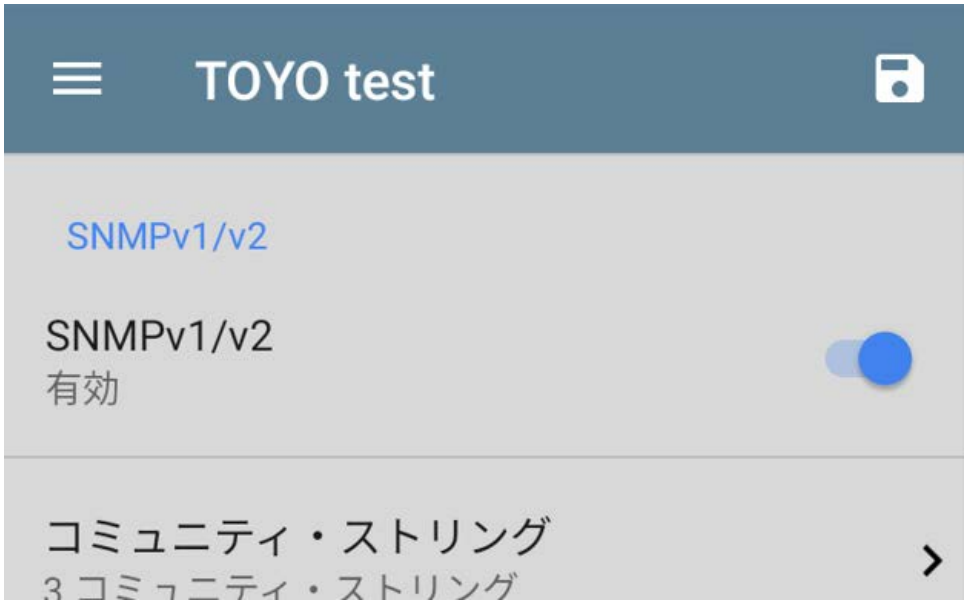
2. 設定が終わったら、戻るボタン  をタップして、メインのディスカバリ リスト画面に戻ります。
3. 次に、アクションオーバーフローメニュー  から**ディスカバリ更新**を選択し、新しい設定を適用します。

設定画面で保存ボタン  をタップすると、設定されたディスカバリの設定をロード、保存、インポート、エクスポートすることができます。

- **読み込み**：過去に保存したディスカバリの設定を開きます。
- **名前を付けて保存**：現在の設定を既存の名前または新しいカスタム名で保存します。
- **インポート**：過去にエクスポートした設定ファイルをインポートします。
- **エクスポート**：現在の設定のエクスポートファイルを作成し、内部または接続した外部ストレージに保存します。

設定を保存すると、入力したカスタム名がディスカバリ設定画面のタイトルに表示されます。

下の画像では、ユーザーが「TOYO test」という名前のカスタム設定を保存したため、ディスカバリ設定画面のタイトルが置き換えられています。



SNMPの設定

SNMP管理対象機器のMIB（Management Information Base）には、機器構成、インターフェース構成や統計情報、SNMPテーブル（ホストリソースやルートテーブルなど）、VLAN詳細などの情報が含まれています。
ディスカバリプロセスにより、AirCheck G3はMIBを照会して、デバイスのタイプ、ポート、接続されているサブネット、およびその他のデータを特定します。

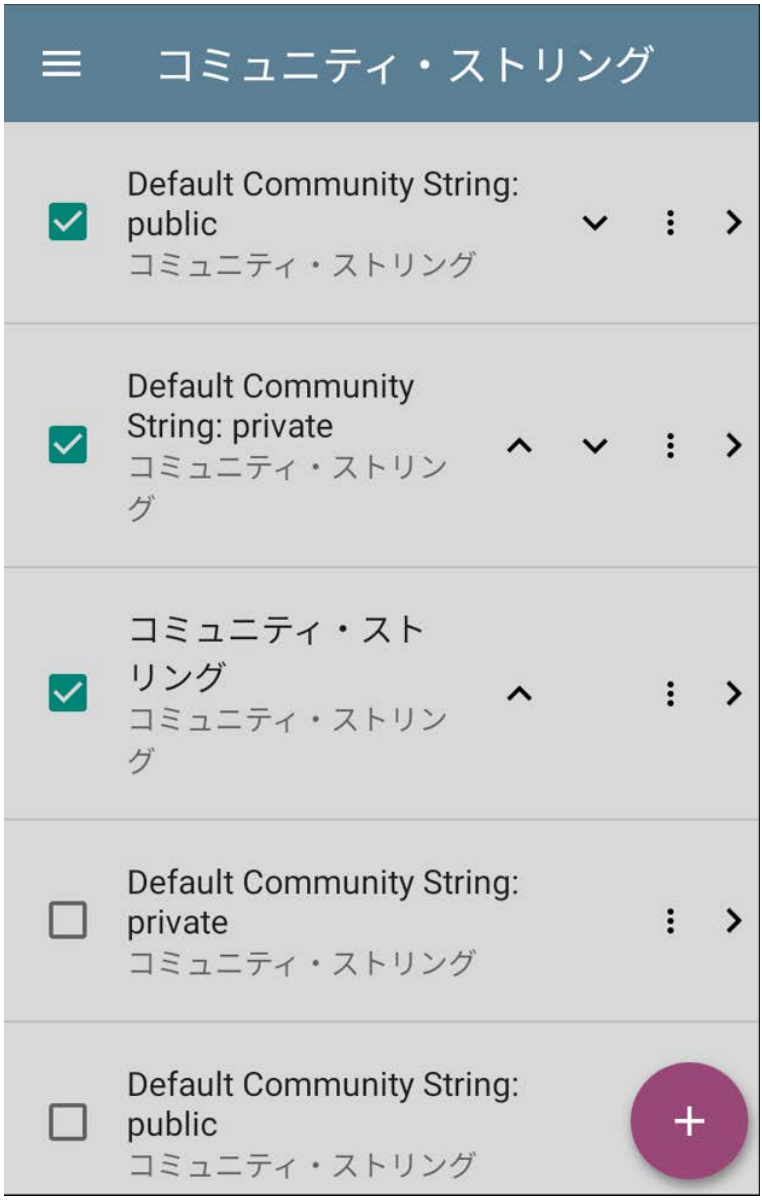
SNMPクレデンシャルは、スイッチやルーターなどの相互接続デバイスのSNMPエージェントと通信するために必要です。
ディスカバリ設定では、AirCheck G3がこれらのデバイスとの通信に使用するSNMPコミュニティ・ストリングと認証情報セットを入力することができます。

SNMPv1/v2

トグルボタンをタップすると、SNMPv1およびv2クエリの**有効**/**無効**を切り替えることができます。この設定はデフォルトで有効になっており、次の設定で設定されたコミュニティ・ストリングが使用されます。

コミュニティ・ストリング

このフィールドをタップすると、コミュニティ・ストリングの一覧画面が表示され、コミュニティ・ストリングの追加、編集、削除ができます。



AirCheck G3は、チェックした文字列をこの画面に表示している順序で使用します。ある文字列を使用して問い合わせた機器から応答がない場合、次の文字列を送信します。

NOTE: この画面とディスカバリ設定の他の画面は、自動テストプロファイルグループ画面と似た動作をします。

コミュニティ・ストリング画面では、以下の操作を行うことができます:

- 現在のディスカバリ設定で使用する文字列を含める、または除外するためのボックスをチェックまたはチェックを外します。
- 上下の矢印  をタップすると、AirCheck G3が文字列を使用してデバイスに問い合わせる順序を変更できます。
- アクションオーバーフローアイコン をタップすると、コミュニティ・ストリングを複製または削除ができます。
  注意：ストリングを削除すると、保存されているすべてのディスカバリ設定から削除されます。現在のディスカバリ設定のみからストリングを削除するには、そのチェックを外すだけです。
- FAB  をタップすると、新しいコミュニティ・ストリングが追加できます。
- コミュニティ・ストリングの行をタップすると、文字列とその説明を編集することができます。
  TIPS：クエリに失敗するたびに検出時間が長くなるため、検出時間を最短にするには、使用しないコミュニティ・ストリングのチェックを外すか削除します。

また、コミュニティ・ストリングを最も使用される順番に並べることができます。

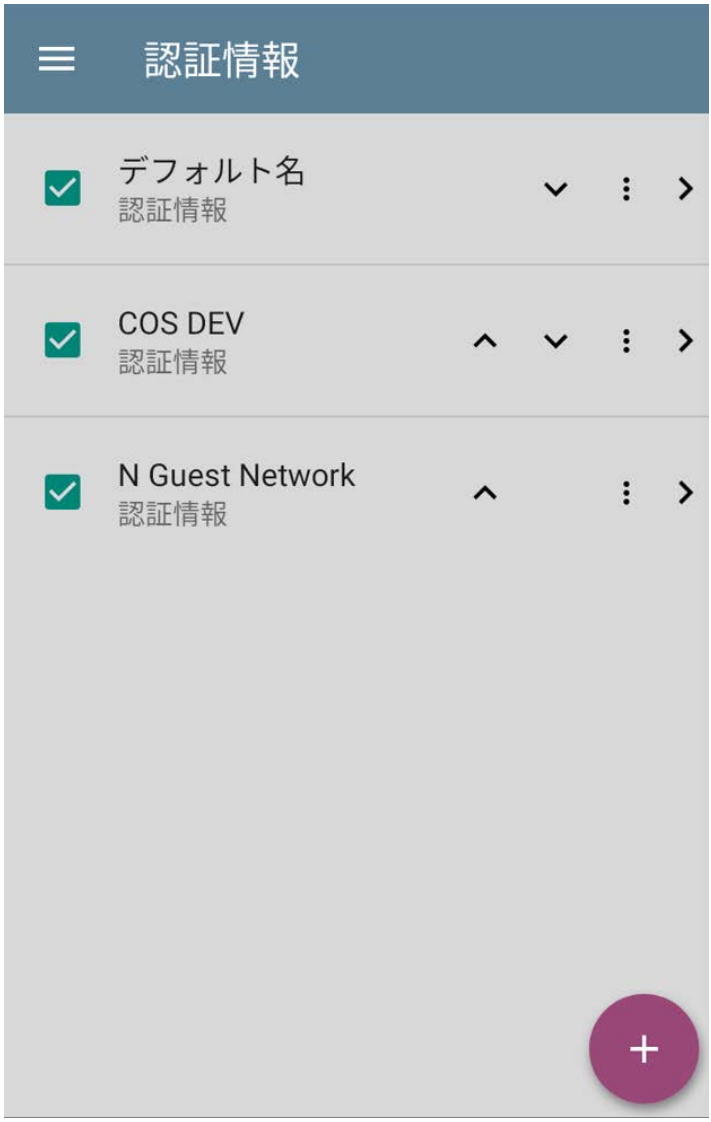
SNMPv3

SNMPv3クエリを有効または無効にするには、トグルボタンをタップします。この設定はデフォルトで有効になっており、次の設定で設定された認証情報を使用します。

> **NOTE**: この設定を有効にしても、SNMPv3の認証情報が構成されていない場合、AirCheck G3はすべてのSNMPv3エージェントのエンジンIDを検出します。これは、デバイスがSNMPv3をサポートしているかどうかを検出するのに適した方法です。

認証情報

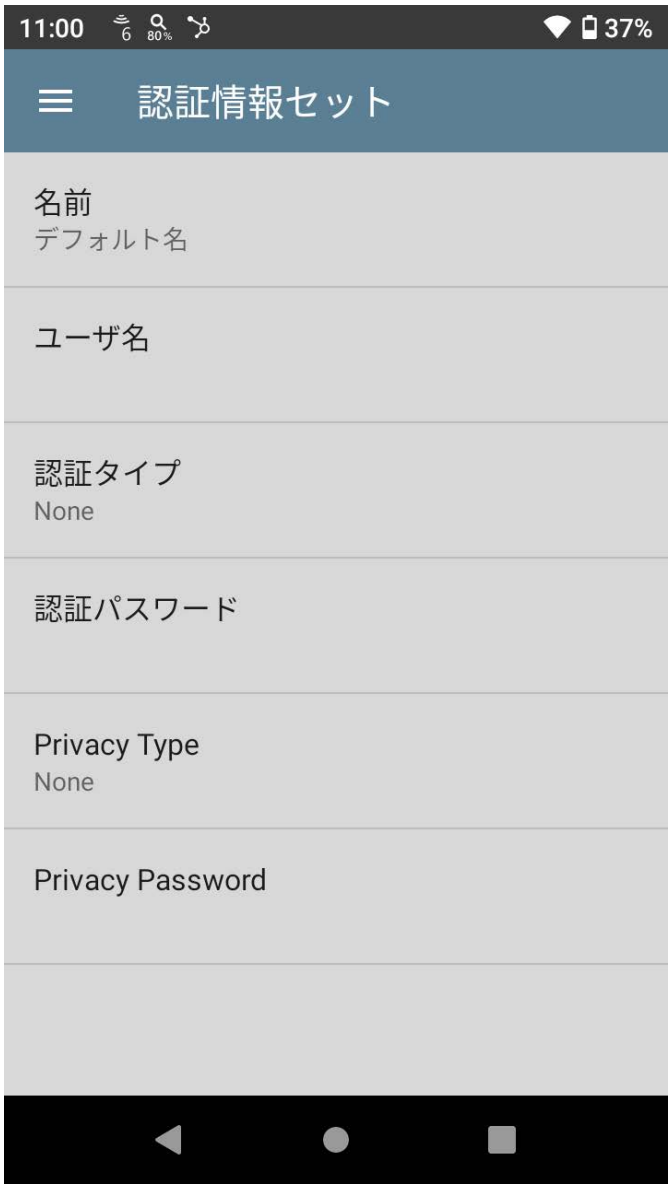
このフィールドをタップすると、認証情報の一覧画面が表示されます。



この画面のインタフェースは、上記のコミュニティ・ストリング画面と同様に機能します。AirCheck G3は、表示された順序で認証情報を使用します。

- 現在のディスカバリ構成で使用する認証情報のセットを含める、または除外するために、ボックスをチェックまたはチェックを外します。
- 行をタップして、その資格情報を編集します。

- FAB (+) をタップすると、新しい認証情報が追加できます。



認証情報セット画面で、各フィールドをタップして必要な認証情報を選択または入力します。

名前

名前フィールドをタップして、認証情報セットのカスタム名を入力します。

ユーザ名

タップし、SNMPv3のユーザ名を入力します。

認証タイプとパスワード

AirCheck G3のディスカバリは、2種類のSNMPv3認証をサポートしています。**HMAC-SHA**と**HMAC-MD5**です。認証が必要な場合は、適切なパスワードを入力します。

Privacy Type と Password

AirCheck G3のディスカバリは、4つのプライバシータイプに対応しています。
CBC-DES、**AES-128**、**AES-192**、および**AES-256**です。必要に応じて、適切な**Privacy Password**を入力します。

利用ディスカバリ・ポート

利用ディスカバリ・ポートをタップして、ディスカバリがデータ収集に使用するポートを選択します。アクティブなネットワークリンクが利用可能な場合にのみ、ディスカバリは有効なポートを介して実行されます。

ディスカバリでは、デフォルトですべてのポートを使用します。使用するポートを制限する場合は、チェックを外してください。

拡張レンジ

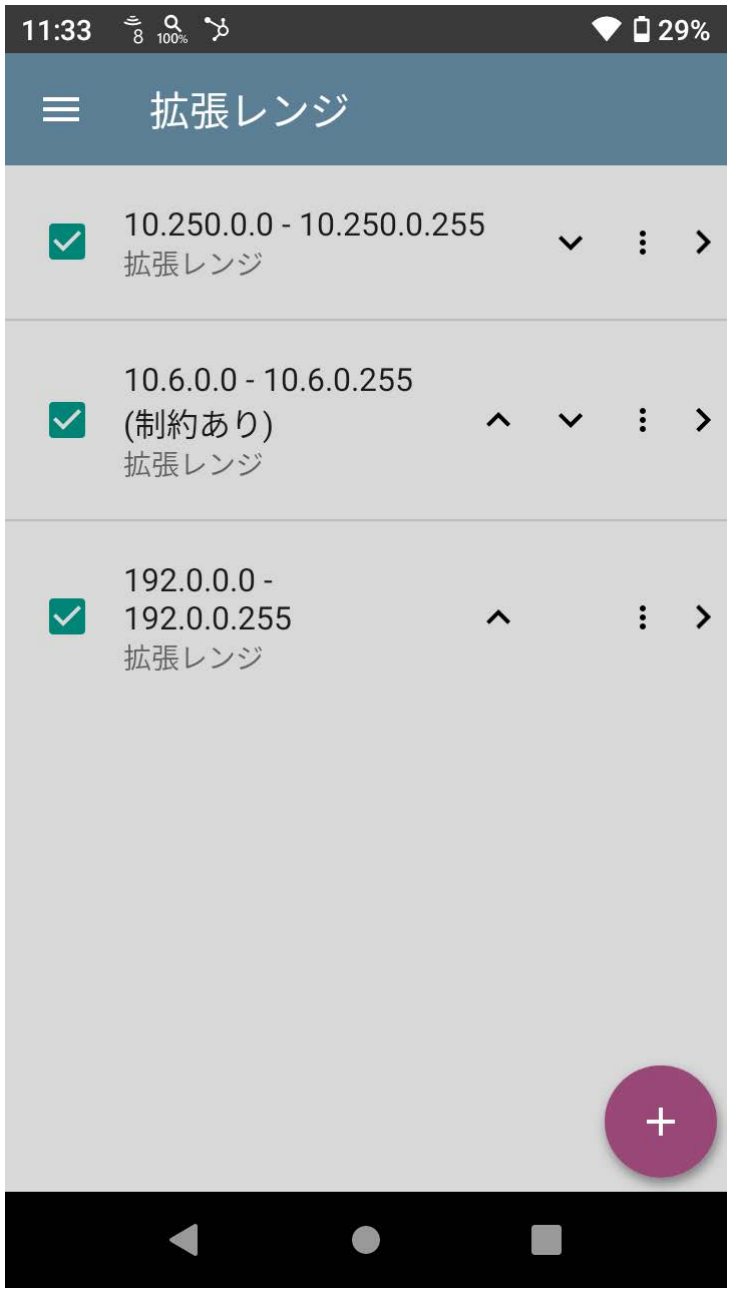
拡張レンジ画面では、ディスカバリプロセスを実行させる非ローカルサブネットのアドレスを入力することができます。ディスカバリは、直接接続されているかオフネットであるかにかかわらず、有効な拡張レンジのすべてのデバイスを検索します。AirCheck G3は、直接接続されていないサブネットではPingスイープを、接続されているサブネットではARPスイープを実行します。

SNMPエージェントがホスト（PCやサーバー）のサブネットとは別のサブネットにある場合、検出のために追加のネットワークを設定する必要があります:

- 検出したいリモートサブネットのネットワークアドレス。「ホスト（PCやサーバー）ネットワーク」
- リモートサブネットにあるスイッチとルーターのSNMPエージェントのネットワークアドレス。例：管理サブネット

SNMP認証情報セットと拡張レンジの両方を設定し、ネットワークポートの接続に関係なく、AirCheck G3が常に管理サブネットを検出するようにします。

フィールドをタップすると、拡張レンジ一覧画面が表示されます。



- 現在のディスカバリ設定から拡張レンジを含める、または除外するために、ボックスをチェックまたはオフにします。

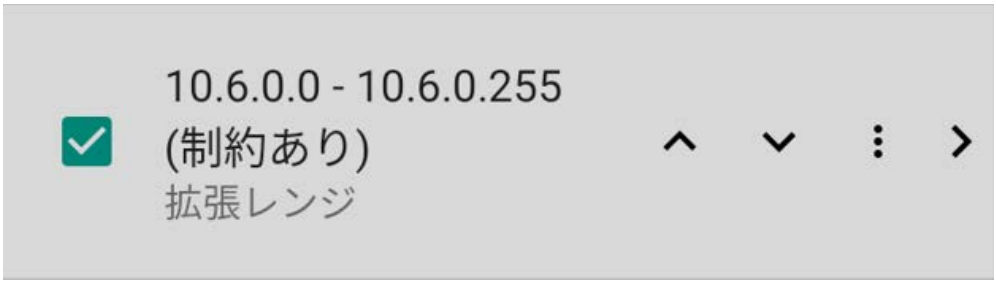
チェックされていない拡張レンジは、現在の設定におけるデフォルトのディスカバリ動作には影響しませんが、他のディスカバリ設定（コミュニティ・ストリングや認証情報など）で使用されることがあります。

- 拡張レンジの行をタップすると、そのアドレスとサブネットを編集することができます。
- FAB + をタップすると、新しい拡張レンジが追加できます。

アクティブと制約のあるサブネット

設定された各拡張レンジについて、トグルボタンをタップすると、Activeから**制約あり**に切り替えることができます。検出は、アクティブなレンジで実行されます。範囲を制限に設定すると、

そのネットワークまたはサブネットでの検出プロセスが無効になり、AirCheck G3は制限された範囲内のデバイスと通信しないことになります。



- 制約のあるレンジは、拡張レンジ画面での表示順序にかかわらず、優先されます。
- 設定されたActive拡張レンジの一部を**制約あり**にすることができます。
- また、Activeレンジの一部であるかどうかにかかわらず、単一のデバイスを制限することができます。カバーされないようにしたい単一のデバイスを入力するには、**アドレス**フィールドにそのIPアドレスを入力し、**サブネットマスク**フィールドを255.255.255.255に設定してください。

- ## アドレス

アドレス欄をタップして、IPアドレスの範囲を入力または選択します。

ドロップダウンメニューをタップして、以前に検出されたサブネットを選択します。**アドレス**フィールドには、選択した内容が自動的に入力されます。

サブネットマスク

このフィールドをタップして、サブネットマスクを選択します。すでに発見されているサブネットを選択した場合、サブネットマスクも事前に入力されます。

他のデバイスを介して検出されたデバイス

デフォルトでは、AirCheck G3は他のデバイスのSNMPテーブルからデバイスを検出します。

ここに記載されているデバイスタイプのSNMPテーブルからデバイスを自動的に検出しないようにするには、それらのボックスのチェックを外します。

ルータとサブネット

ルータとサブネットのチェックボックスを有効にすると、検出されたルーターが検出結果に含まれます。さらに、ディスカバリが検出されたルーターへのSNMPアクセス権を持っている場合、そのルーティングテーブルが読み取られ、ネクストホップ・ルーターがディスカバリ リストに追加されます。

ルーティングテーブルにローカルサブネットがある場合は、それらもサブネットリストに追加されます。このプロセスは、追加されたルーターで利用可能なすべてのSNMP認証情報が試されるまで続けられます。

NOTE: 検出されたサブネットはサブネットリストに追加されるだけで、検出されたすべてのサブネットをスイープするわけではありません。特定のサブネットでディスカバリを実行するには、上記の**拡張レンジ**を参照してください。

このプロセスを使用して検出したいルーターが他のサイトにあるが、このサイトからのローカルネクストホップリンクがない場合、そのサイトのルーターの1つを**ディスカバリ**に追加することができます。その後、そのルーターからプロセスが実行され、そのサイト上のルーターも同様に見つけます。ルーターのサブネット、またはルーターのIPアドレスと/32のマスクを**拡張レンジ**に追加します。

スイッチ

スイッチのチェックボックスが有効な場合、他の機器のSNMPネイバーテーブルで検出したスイッチを**ディスカバリ** リストに追加します。

たとえば、AirCheck G3が1つのスイッチのCDPおよびLLDPキャッシュを読み取っているとき、そのスイッチには他のスイッチが含まれていることがあります。このオプションを有効にすると、AirCheck G3は、検出範囲内にない場合でも、これらの他のスイッチを追加します。

> **NOTE**: 別のサイトのスイッチを検出するには、そのサイトのスイッチの1つをディスカバリ 拡張レンジに追加します。

VoIP デバイス

VoIP デバイスのチェックボックスが有効な場合、サブネットに関係なく、他のデバイスのSNMPテーブルで見つけたVoIPデバイスを追加します。これらは通常、スイッチのLLDP-MEDテーブルで見つかります。スイッチのオプションを有効にすると、すべてのVoIPデバイスを見つけることができる可能性が高くなります。

Wi-Fi クライアント

Wi-Fiクライアントのチェックボックスを有効にすると、APと無線LANコントローラーのSNMPテーブルで検出した無線クライアントを追加します。スイッチと一緒にこのオプションを有効にすることで、すべてのWi-Fiクライアントを見つけることができるようになります。

NOTE: ここでWi-Fiクライアントを有効にすると、Wi-Fi解析が無線送信パケットで検出したものしか表示しないため、Wi-Fi解析アプリに表示されないWi-Fi機器がディスカバリに表示される場合があります。

仮想マシン

仮想マシンのチェックボックスが有効な場合、他のデバイスのSNMPテーブルで検出された仮想マシンが追加されます。これらは通常、[ESXホスト] > [SNMPテーブル]で見つかります。ESXホストのサブネットを**拡張レンジ**に追加すると、仮想マシンを見つけるのに役立ちます。

更新周期

この設定は、ディスカバリプロセスの実行間隔を制御します。デフォルトでは、ディスカバリは90分ごとに実行されます。**更新周期**フィールドをタップして、別の間隔（最大8時間）を選択します。

マニュアルオプションを選択すると、通常の自動ディスカバリがオフになり、メインのディスカバリー覧画面からディスカバリを選択した場合のみプロセスがリフレッシュされます。

デバイス 健全な間隔

ディスカバリは、自動的に一連のネットワークヘルステストを実行し、検出されたすべてのインタフェースとデバイスリソースについて、高い使用率、廃棄、エラーなどのネットワーク問題を検索します。

選択した時間、更新周期は、デバイスヘルステストの各実行間の最小時間です。このフィールドをタップすると、デバイスヘルステストを無効にしたり、間隔をデフォルトの10分から30分または60分に変更することができます。

デバイスのヘルステストを無効にすると、ディスカバリで検出できる問題の種類に影響します。

問題設定も参照してください。

ARP スイープ・レート

ARP スイープ・レートフィールドをタップして、1秒あたりのARPリクエスト数を5～100の間で選択します。

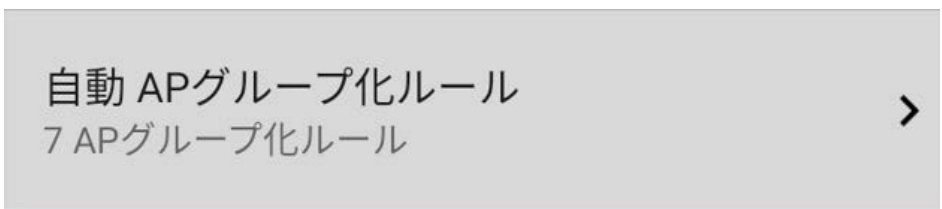
この設定により、AirCheck G3が、あまりにも多くのARPが送信されていると感知したポートをシャットダウンするのを防ぐことができます。

SNMP クエリ遅延

この機能は、ARPキャッシュ、IPアドレス・テーブル、ルーティング・テーブル、FDBテーブルなど、SNMPエージェントのCPUスパイクの原因となる主要なテーブルへのSNMPクエリ間でAirCheck G3が待機する時間を制御します。

デフォルトのSNMPクエリ遅延は、**遅延なし**です。主要なラージテーブルにクエリを実行する場合、AirCheck G3は応答が受信されるとすぐ、さらにデータを要求します。必要に応じて、1秒または5秒の遅延を選択することができます。

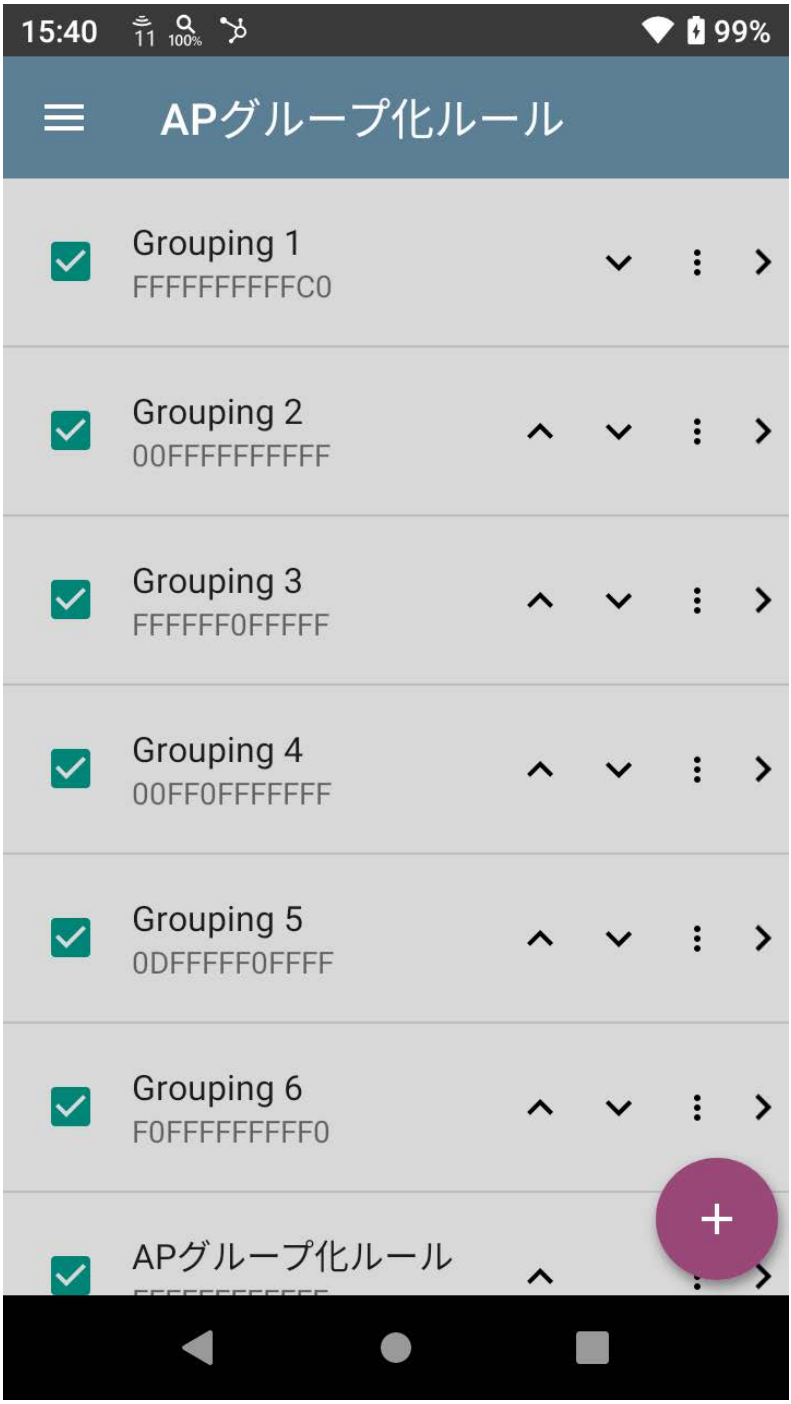
自動 APグループ化ルール



この機能により、AirCheck G3がBSSIDをアクセスポイントにグループ化する方法を制御するAPグループ化ルールを調整し、APタイプや環境に応じて適切にグループ化されるようにします。

例えば、異なるAPからのBSSIDが不正確にグループ化されている場合、グループ化の原因となっているルールを無効にすることができます。APメーカーが、6つのデフォルトルールのいずれにも当てはまらないBSSIDバリエーションスキームを使用している場合、新しいルールを追加することができます。

設定をタップすると、APグループ化ルールのリスト画面が表示されます。下の画像は、AirCheck G3の6つのデフォルトのAPグルーピング・ルールを示しています。すべてのデフォルトのグループ化ルールの**プリフィックス・フィルタ**は、000000-000000に設定されています。



AirCheck G3の他の設定リスト画面と同様に、この画面からグループ化ルールの有効・無効、追加、削除、編集を行うことができます。

- 現在のディスカバリ設定で使用するルールを含める、または除外するために、ボックスをチェックまたはチェックを外します。
- アクションオーバーフローアイコン ⋮ をタップすると、ルールの複製または削除ができます。
  注意：ルールを削除すると、保存されているすべてのディスカバリ設定からそのルールが削除されます。現在のディスカバリ設定で使用されているものからルールを削除するには、そのチェックを外すだけです。

- FAB ＋ をタップすると、新しいルールが追加できます。
- 任意のルールの行をタップして編集することができます。

名前

必要であれば、デフォルトまたは新規のルールのカスタム名を入力します。プリフィックス・フィルタを使用する場合は、APの製造者名をルールの名前にするのがベストプラクティスとなります。

プリフィックス・フィルタ

プリフィックス・フィルタを使用して、特定のAPメーカーのBSSIDスキームのルール、つまり1つのAPメーカーのプリフィックスだけのルールを作成します。デフォルトのルールには、すべてデフォルトのプリフィックス・フィルタである000000-000000が含まれています。

プリフィックス・フィルタが0でない場合、フィルタ・マスク（後述）が適用される前に、その2バイト目と3バイト目が検出されたBSSIDと比較されます。この2バイトが正確に一致しないと、2つのBSSIDは一緒にグループ化されません。この動作により、マスクが1つのメーカーにのみ適用されるため、かなりオープンなフィルタ・マスクを指定することができます。

例えば、BSSIDがすべてb83861で始まるCisco APがあるとします。プリフィックス・フィルタに003861-000000を指定することで、グループ化ルールをこれらのAPだけに限定することができます。

フィルタ・マスク

フィルタ・マスクは、APのグループ分けを決定する際に、BSSIDのどの部分を比較するかを指定します。

例えば、デフォルトのルール、**Grouping 1**のフィルタ・マスクはFFFFFF-FFFFFC0なので、下位6ビットだけが異なるBSSIDはすべてグループ化されます。

問題設定

問題設定は、ディスカバリアプリとWi-Fiアプリの両方で検出・表示される問題や、パケット破棄や使用率など有効な問題のしきい値を決定します。

左側のナビゲーションドロワーをスライドさせるか、ディスカバリアプリのメニューアイコン ☰ をタップし、**問題設定**を選択すると、問題設定画面にアクセスできます。

（ここをタップすると、**ディスカバリ設定**に移動することができます。）

問題は、**ネットワーク**または**Wi-Fi**に分類されます。

NOTE: ここで設定されたWi-Fi問題は、Wi-Fiアプリで検出・表示される問題も制御します。

ディスカバリ設定と同様に、この画面で保存ボタン をタップすることで、設定した問題設定の保存、読み込み、インポート、エクスポートが可能です。

それぞれの行をタップすると、問題の種類を有効または無効にし、必要に応じてしきい値を設定することができます。

初期設定では、すべての問題タイプが有効になっています。右側のトグルボタンをタップすると、それぞれを無効にすることができます。

各問題の右側にある赤、黄、青の情報アイコンをタップすると、詳細な説明と推奨される対処法を読むことができます。赤いアイコンは**失敗**、黄色は**警告**を表します。**青いアイコン**は情報提供です。

設定が終わったら、戻るボタンをタップして、ディスカバリのメイン画面に戻ります。

TCPポートスキャン設定

TCPポートスキャン機能は、ディスカバリ詳細画面のFABから、現在のデバイスのオープン・ポートをチェックします。AirCheck G3は同時に多くのポートをスキャンし、開いているポートの番号を報告します。

左側のナビゲーションドロワーをスライドさせるか、ディスカバリアプリのメニューアイコン☰をタップして、TCPポートスキャン設定にアクセスします。

TCPポートスキャンを選択してください。

インターフェース：フィールドをタップして、ポートスキャンの実行元となる AirCheck G3のポートを選択します。

スキャンリスト：この設定は、ポートスキャン中にどのポート番号がテストされるかを一覧表示します。フィールドをタップして、異なるポート番号または範囲をカンマで区切って入力します。

タイムアウト・スレッショルド：この値は、AirCheck G3が各ポートからの応答を待機する時間を制御します。スキャンリスト内のすべてのポートがこの応答時間を経過すると、スキャンは終了し、TCP ポートスキャンの結果画面が表示されます。

しきい値内で応答したポートをリストします。

TCPポートスキャンも参照してください。