ワイヤレスアクティブテスト（ThousandEyes 利用）導入ガイド

目次

はじめに

ThousandEyes を使用した Cisco CW9172H アクセスポイントでのアクティブテストは、対応する各アクセスポイントを合成クライアントに変えることで、ネットワーク アシュアランスを変革します。この機能により、ワイヤレスクライアントの視点から、ネットワークエッジで直接エンドツーエンドのテストを実行できます。すべての顧客セグメントの組織が、実際のクライアントデバイスに依存することなく、ThousandEyes ダッシュボードを使用して、オンボーディング、接続、およびアプリケーションレベルのエクスペリエンスに関するリアルタイムの可視性を直接得ることができます。合成クライアントとして機能する各 CW9172H アクセスポイントを継続的にテストすることで、ネットワークパフォーマンスのベースラインに関する理解が得られます。これは、ファームウェアのアップグレードや設定変更などのメンテナンスウィンドウの前後で特に重要になります。

このプロアクティブなアプローチは、認証、DHCP、DNS などのコアサービスが、アップデート後も完全に動作可能な状態となるようにするという長年の課題を解決します。包括的な AP 間接続テストにより、IT チームは、ネットワークが事業運営に対応しているという確証を得ることができます。これにより、ダウンタイムのリスクが軽減され、問題解決が迅速に進められます。これらのメトリックは、迅速な根本原因の特定と、アクセスポイントからクラウドへのエンドツーエンドの可視性を実現します。しかも、追加のハードウェアは必要ありません。この機能により、お客様は先行して準備状況を把握し、平均解決時間（MTTR）を短縮して、シスコと競合他社の差別化につながる最適なユーザー体験を提供できます。

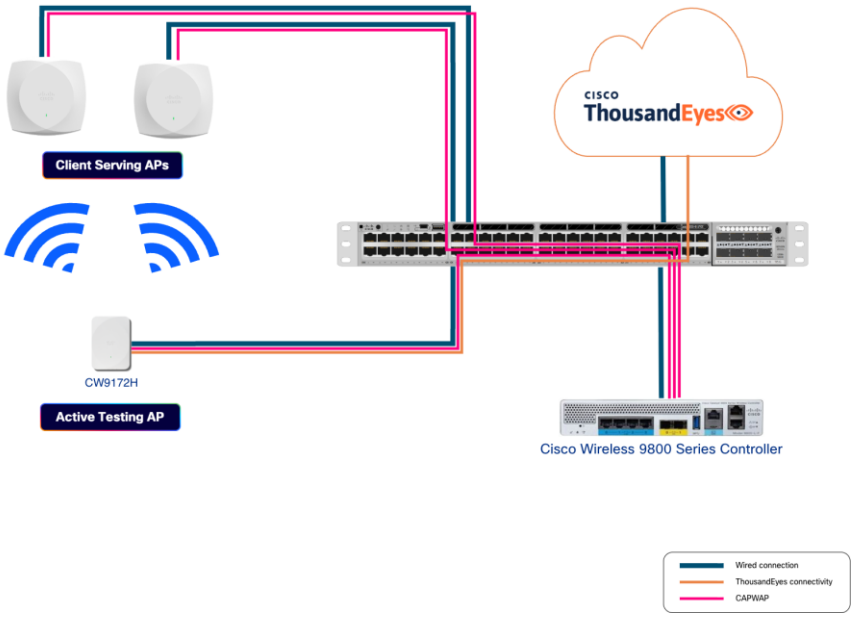

図 1.　　アーキテクチャの概要例

このドキュメントでは、Cisco Wireless 9800 ワイヤレス LAN コントローラと ThousandEyes の Web サイトの両方でのアクティブ テスト アクセス ポイントのインストール、設定、および操作について説明します。

要件

- 1 つ以上の **CW9172H アクセスポイント**
- Cisco IOS® XE 17.18.2 以降を実行する **Cisco Wireless 9800 ワイヤレス LAN コントローラ**
  - スイッチの組み込みワイヤレスコントローラを除くすべてのフォームファクタがサポートされています。
  - ローカルおよび FlexConnect モードがサポートされます。

- アクセスポイントごとに **1 つの Cisco Wireless Essentials ライセンス**
- アクセスポイントあたり 1 つの ThousandEyes Endpoint Agent Advantage ライセンス（別名：End User Monitoring Advantage）
- **ThousandEyes プラットフォームにアクセスするための ThousandEyes アカウント**
- ThousandEyes への **IP 到達可能性**（直接、ネットワークアドレス変換（NAT）、またはプロキシ）。アクティブテスト AP の有線管理 VLAN のみが ThousandEyes プラットフォームに到達できる必要があります。WLC は対象外です。必要なネットワーク接続のリストは、https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/installing/system-requirements#network-connections で確認できます。

サポートされるセキュリティタイプ

次のセキュリティタイプは、2.4 GHz、5 GHz、および 6 GHz でサポートされています。WPA2 および WPA3 はどちらも、PMF（無効化、任意、必須）を含めてサポートされています。ビーコン保護はサポートされていません。

表 1. サポートされるセキュリティタイプ

WLAN タイプ	**サポートされるタイプ**	**サポートされるタイプ**
AKM スイート	• 802.1X • PSK • FT-802.1X • FT-PSK • 802.1X-SHA256 • PSK-SHA256 • SAE • FT-SAE • OWE（OWE 移行モードを含む）	• SUITE-B • Suite-B-192 • SAE-EXT-KEY • FT-SAE-EXT-KEY
暗号	• CCMP-128	• GCMP-128 • CCMP-256 • GCMP-256
PHY モード/Wi-Fi バージョン	• HE（802.11ax / Wi-Fi 6 + 6E） • VHT（802.11ac / Wi-Fi 5） • HT（802.11n / Wi-Fi 4） • レガシー（802.11abg）。 Wi-Fi 6E までのすべての PHY モードをサポート	• EHT（802.11be または Wi-Fi 7）

サポートされている EAP タイプは次のとおりです。

- **PEAP**：ユーザー名とパスワードに加えて、サーバー側の証明書が必要です。この実装では、サーバー側の証明書は無視されます。
- **LEAP**：ユーザー名とパスワードに加えて、サーバー側の証明書が必要です。この実装では、サーバー側の証明書は無視されます。
- **EAP-FAST**：ユーザー名とパスワードに加えて、PAC のプロビジョニングが必要です。この実装では、PAC のプロビジョニングは自動的に行われます。
- **EAP-TLS**：両側に証明書があること。

制限事項

- 基本認証を使用する HTTP プロキシはサポートされていません。
- 非表示 SSID のテストはサポートされていません。
- ファブリックモードのアクティブ テスト AP はサポートされていません。ただし、AP を SDA ファブリックにオーバーザトップ（OTT）で展開して、ワイヤレスファブリックのテストに使用できます。

設計上の考慮事項

ソリューションの規模を決定する際は、サイト内のすべての AP が動作していることを確認する場合から、規模を問わず、サイトごとに 1 つのデータポイントのみを取得することを希望する場合まで、いくつもアプローチが考えられます。規模に関する質問への回答として単一の式を提供する代わりに、以下の質問と回答を参考にして、ビジネスニーズに適したアプローチを見つけてください。

アクティブテスト AP はいくつ必要ですか?

前述のとおり、適切なアプローチは具体的なビジネス要件によって異なります。ワイヤレス接続が運用にとって重要であり、最適なパフォーマンスを確保したい場合は、包括的なテストを実施することを推奨します。現在の推奨される比率は、クライアントサービスを提供する AP 5 個につき、アクティブテスト AP が 1 個です。サポートされる最大比率に制限はありませんが、1:10 を超えないことを推奨します。RSSI が次のしきい値を下回っている場合、アクティブテスト AP は AP（BSSID）に接続しません。

- 2.4 GHz：-73 dBm
- 5 GHz：-70 dBm
- 6 GHz：-68 dBm

アクティブテスト AP はどこに配置しますか?

ワイヤレスアクティブテストをウォール プレート アクセスポイント（CW9172H）に組み込んだ場合、実際のクライアントが体験する無線周波数（RF）環境を正確にシミュレーションできるため、最も正確で現実的な結果を提供しました。エンドユーザーデバイスは通常、天井レベルではなくフロアレベル近くに配置されるため、アクティブテスト AP は床の近く（デスクやブースの高さなど）に配置することを推奨します。

アクティブテスト AP は、壁に取り付けたり、必要に応じて入手可能なアクセサリ CW-ACC-DESK1-00 を使用してデスクトップに設置したりできます。

何をテストするのですか?

環境内の一般的なクライアントの動作をエミュレーションして、ビジネスに関連する最も重要なアプリケーションをテストすることを推奨します。たとえば、オフィス環境では生産性アプリケーションがこれに含まれますが、保管倉

庫では注文のピッキングや関連するアクティビティをサポートするロジスティクス アプリケーションが含まれることが考えられます。アクティブテスト AP ごとにサポートされるテストの数は最大 10 個であることに注意してください。ただし、次の記事に概説されているように、追加のテストを設定し、それらの優先順位を管理することはできます。https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/assign_tests_to_agents

設置および設定手順

ソリューションの設置および設定手順は次のとおりです。

1. ThousandEyes アカウントの作成
2. Cisco Wireless 9800 シリーズ ワイヤレス LAN コントローラの設定
3. ThousandEyes でのテストの設定
4. ThousandEyes でのワイヤレス アクティブ テスト データの活用

ThousandEyes アカウントの作成

すでに ThousandEyes アカウントをお持ちの場合は、そのアカウントを活用できます。それ以外の場合は、アカウントを作成する必要があります。アカウントプロセスの詳細については、
https://docs.thousandeyes.com/product-documentation/getting-started/getting-started-with-account-setup
を参照してください。

アカウントを作成したら、エンドポイントエージェントの接続文字列が必要です。ThousandEyes プラットフォームの [UI インストーラ（UI installer）] セクションで [接続文字列（Connection String）] をコピーできます（以下のスクリーンショットを参照）。

- エンドポイントエージェントがない場合は、[ダウンロード（Download）] ボタンをクリックして接続文字列を表示します。
- すでにエンドポイントエージェントがある場合は、[新しいエンドポイントエージェントの追加（Add New Endpoint Agent）] をクリックして接続文字列を表示できます。
- 接続文字列は、エージェントをインストールするアカウントグループを正確に識別するトークンとして機能します。

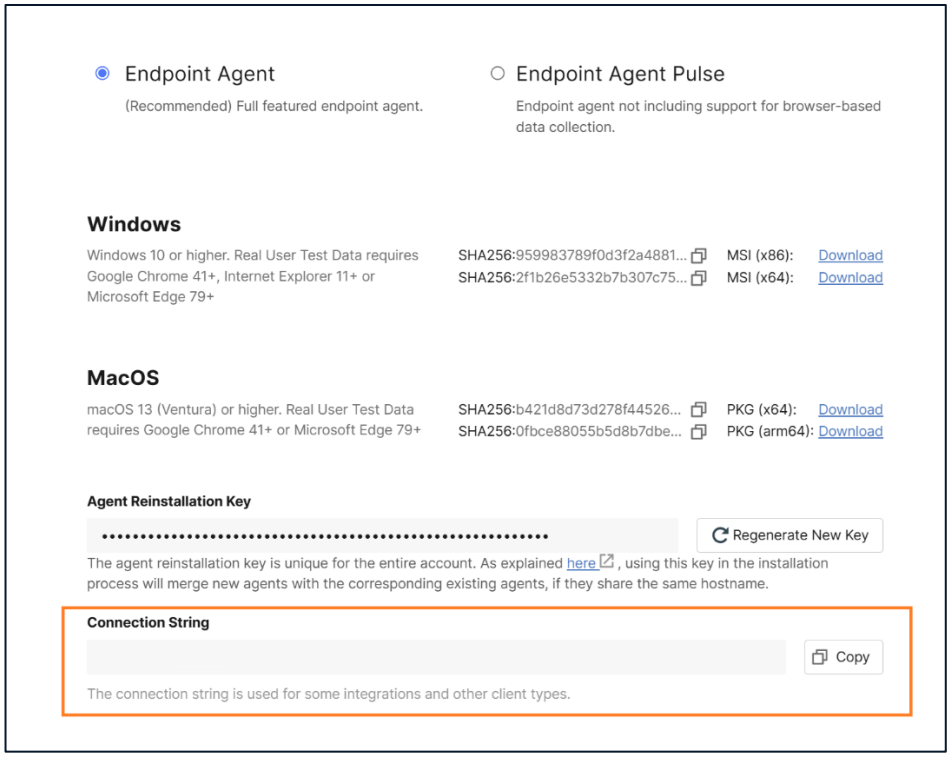

図 2.　　接続文字列の取得

Cisco Wireless 9800 シリーズ ワイヤレス LAN コントローラの設定

必要なイメージを実行している Cisco Wireless 9800 シリーズ ワイヤレス LAN コントローラ（WLC）を用意したら、次の手順に従って設定します。

グローバル コンフィギュレーション

WebUI：[設定（Configuration）] > [サービス（Services）] > [クラウドサービス（Cloud Services）] > [ThousandEyes] タブに移動し、以下を行います。

1. 有効にする（デフォルトで有効）
2. 前の手順で取得した接続文字列を貼り付ける

注：　TE ダウンロード URL は事前に定義され、デフォルトで入力されています。

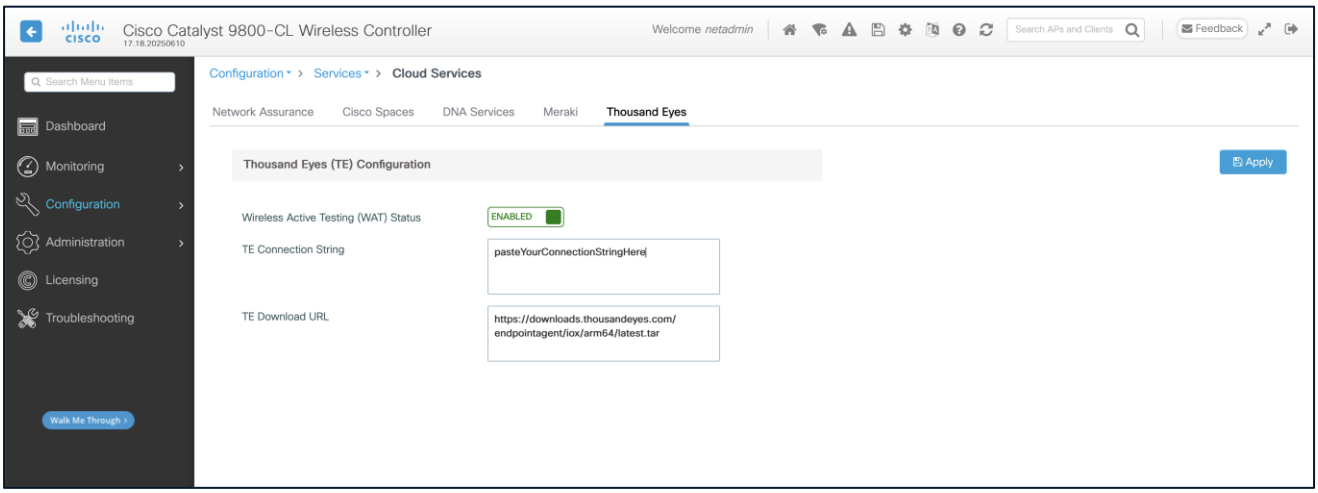

図 3.　　ワイヤレス アクティブ テストをグローバルに有効化する

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
wireless active testing !enabled by default
wireless active testing thousand-eyes connection-string <connection-string>
```

設定を確認するには、次のコマンドを実行することを推奨します。次に、出力例を示します。

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
show wireless active testing configuration


CW9800#show wireless active testing configuration
Wireless Active Testing (WAT) Management - Configuration
============================================================
Administrative State                          : Enabled

ThousandEyes Endpoint Agent
---------------------------
  Connection String                           : theconnectionstring
  Download URL                                :
https://downloads.thousandeyes.com/endpointagent/iox/arm64/latest.tar
```

無線プロファイルと RF タグ：AP 無線設定

AP がワイヤレス合成クライアントとして動作するには、無線プロファイルで特別な設定を行う必要があります。

テスト AP 専用の新しい無線プロファイルを作成します。これはテスト AP にのみ使用されます。

WebUI：[設定（Configuration）]、[タグとプロファイル（Tags & Profiles）]、[RF/無線（RF/Radio）]、[無線（Radio）] タブの順に選択し、テーブルで [無線プロファイル（Radio Profile）] をクリックし、[ワイヤレスアク

ティブテス無線の選択（Wireless Active Testing Radio Selection）] を有効にします。

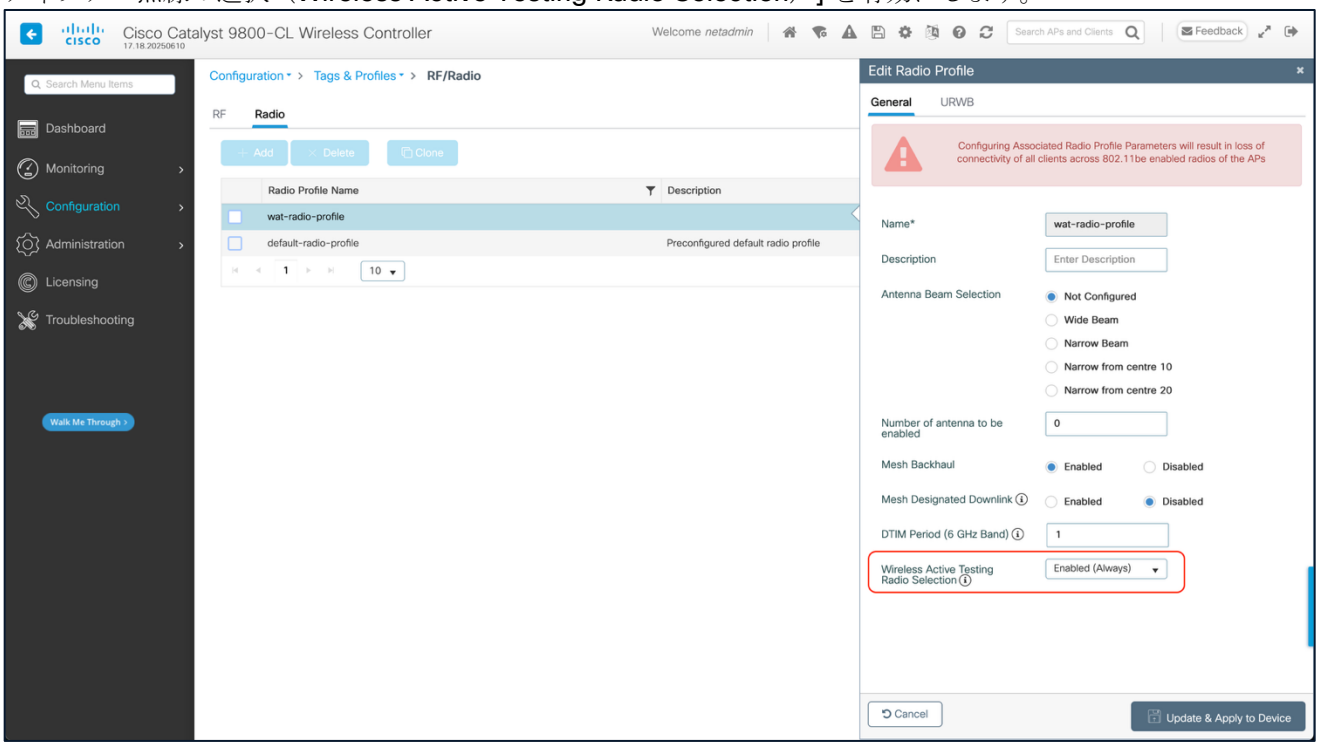

図 4.　　ワイヤレス アクティブ テスト無線の選択

最近作成された無線プロファイルを利用するため、テスト AP 専用の新しい RF タグも必要です。新しい RF タグを作成し、以下に示す各スロットについて、前の手順で作成した RF プロファイルを選択します。CW9172H には 3 つのスロットがあります。

1. **スロット 0**：2.4 GHz 無線
2. **スロット 1**：5 GHz 無線
3. **スロット 2**：6 GHz 無線

注：　上記に示されているスロット番号を完全に一致させることが重要です。

WebUI：[設定（Configuration）]、[タグとプロファイル（Tags & Profiles）]、[タグ（Tags）]、[RF] タブ **>新しい RF タグ**を作成 **>** 上記の各スロットについて、最近作成した**無線プロファイル**を選択します。

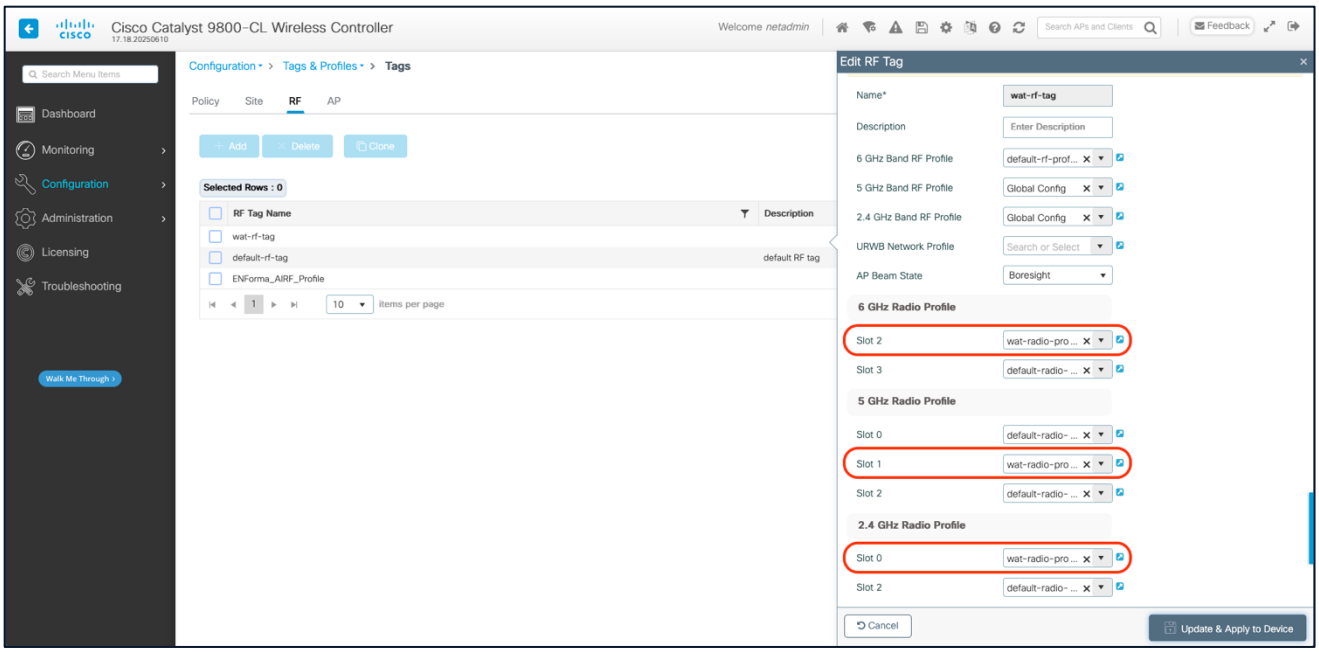

図 5.　　RF タグの設定

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
wireless profile radio <radio-profile-name>
 active testing radio-selection always

wireless tag rf <rf-tag-name>
 dot11 24ghz slot0 radio-profile <radio-profile-name>
 dot11 5ghz slot1 radio-profile <radio-profile-name>
 dot11 6ghz slot2 radio-profile <radio-profile-name>
```

設定を確認するには、次のコマンドを実行することを推奨します。次に、出力例を示します。

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
show wireless profile radio detailed <radio-profile-name>
show wireless tag rf detailed <rf-tag-name>

CW9800#show wireless profile radio detailed wat-radio-profile
Radio Profile name                              : wat-radio-profile
Description                                     :
Beam-Selection                                  : Not configured
Number of antenna to be enabled                 : 0
Mesh Backhaul                                   : Enabled
Mesh Designated Downlink                        : Disabled
DTIM period                                     : 1
```

```
URWB
  Role                                          : Not Configured
  Channel                                       : Not Configured
  Channel Width                                 : 80 MHz
  AES                                           : Fixed Key
  Key Control Rotation Timeout                  : 15
  Channel List                                  : Not Configured
  Point-to-Multi-Point
    RSSI Threshold                              : 0
    Auto Scan                                   : Disabled
    Cluster ID                                  : CiscoURWB
    Tower ID                                    :

Wireless Active Testing (WAT) Configuration
  WAT Admin State (Radio Selection)               : Enabled (Always)

CW9800#show wireless tag rf detailed wat-rf-tag

Tag Name                      : wat-rf-tag
Description                   :
---------------------------------------
6ghz RF Policy                : default-rf-profile-6ghz
5ghz RF Policy                : Global Config
2.4ghz RF Policy              : Global Config
2.4ghz slot 0 Radio Profile   : wat-radio-profile
5ghz slot 0 Radio Profile     : wat-radio-profile
6ghz slot 1 Radio Profile     : default-radio-profile
2.4ghz slot 2 Radio Profile   : default-radio-profile
6ghz slot 2 Radio Profile     : wat-radio-profile
6ghz slot 3 Radio Profile     : default-radio-profile
AP Beam State                 : Boresight
URWB Profile                  :
```

ポリシータグ：WLAN/SSID 設定

アクティブテスト AP では、通常の AP と同じポリシータグを使用することを推奨します。これにより、ThousandEyes ダッシュボードでの設定が容易になります。ただし、そうしないことも選択できます。テスト用 AP（CW9172H）は、SSID がポリシータグに含まれていても、SSID をブロードキャストしません。

現在テストできるセキュリティタイプは、「サポートされているセキュリティタイプ」セクションに一覧表示されています。

WebUI：[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [WLANs]

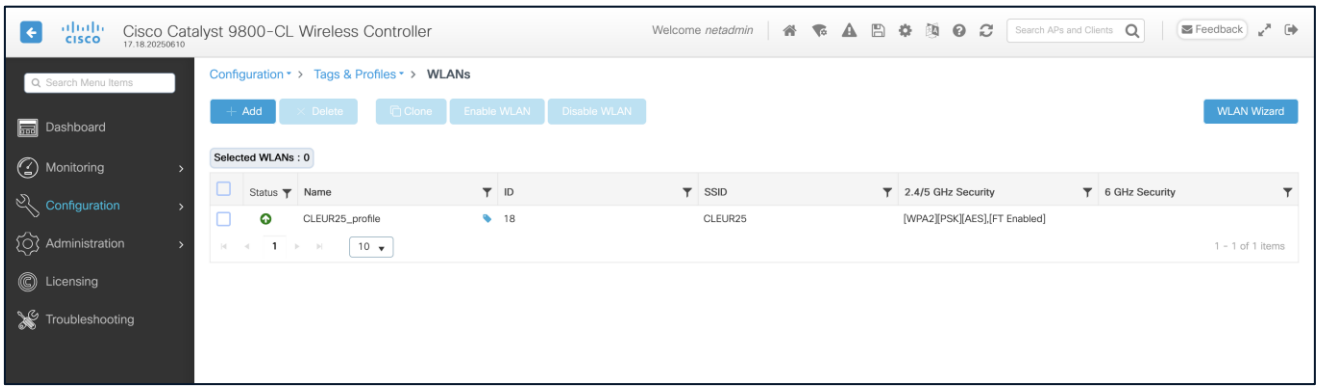

図 6.　　WLAN

[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [タグ（Tags）] > [ポリシー（Policy）] タブ > テーブルで [ポリシータグ（Policy Tag）] をクリックします。

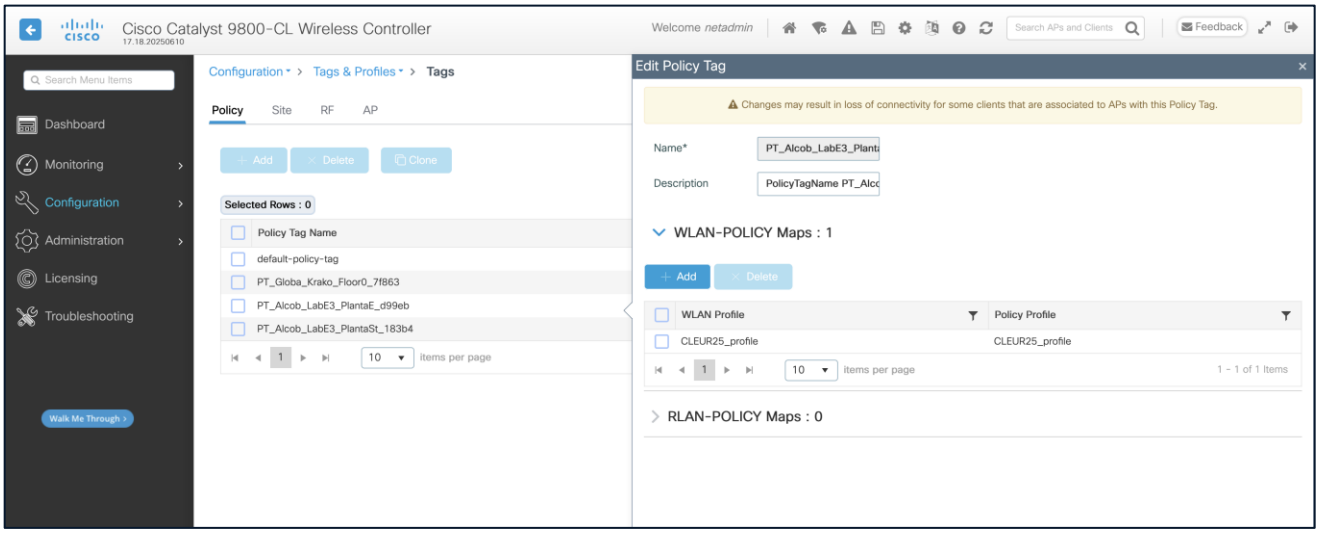

図 7.　　ポリシータグの例

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
wlan CLEUR25_profile 18 CLEUR25
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 security ft
 security wpa psk set-key ascii 0 Cisco123!
 no security wpa akm dot1x
 security wpa akm psk
 security pmf optional
 no shutdown

wireless profile policy CLEUR25_profile
```

```
 autoqos mode fastlane
 description CLEUR25_profile
 dhcp-tlv-caching
 exclusionlist timeout 180
 http-tlv-caching
 ipv4 flow monitor avc_ipv4_assurance input
 ipv4 flow monitor avc_ipv4_assurance_dns input
 ipv4 flow monitor avc_ipv4_assurance_rtp input
 ipv4 flow monitor avc_ipv4_assurance output
 ipv4 flow monitor avc_ipv4_assurance_dns output
 ipv4 flow monitor avc_ipv4_assurance_rtp output
 ipv6 flow monitor avc_ipv6_assurance input
 ipv6 flow monitor avc_ipv6_assurance_dns input
 ipv6 flow monitor avc_ipv6_assurance_rtp input
 ipv6 flow monitor avc_ipv6_assurance output
 ipv6 flow monitor avc_ipv6_assurance_dns output
 ipv6 flow monitor avc_ipv6_assurance_rtp output
 vlan VLAN15
 no shutdown

wireless tag policy PT_Alcob_LabE3_PlantaE_d99eb
 description "PolicyTagName PT_Alcob_LabE3_PlantaE_d99eb"
 wlan CLEUR25_profile policy CLEUR25_profile
```

設定を確認するには、次のコマンドを実行することを推奨します。次に、出力例を示します。

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
show wireless tag policy detailed <policy-tag-name>

CW9800#show wireless tag policy detailed polic_tag_1

Policy Tag Name : polic_tag_1
Description     : PolicyTagName polic_tag_1

Number of WLAN-POLICY maps: 2
WLAN Profile Name                Policy Name
------------------------------------------------------------------------
CLEUR25_profile                  CLEUR25_profile
CLEUR25_1X_profile               CLEUR25_1X_profile
```

サイトタグ：AP プロファイル設定

テスト用 AP（CW9172H）で使用される AP プロファイルで、アプリケーション ホスティングを有効にする必要があります。ただし、「要件」に記載されているライセンス要件が変更されることはありません。

WebUI：[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [AP 参加（AP Join）] > テーブルで [AP 参加プロファイル（AP Join Profile）] をクリックし、AP プロファイル内で [一般（General）] タブを選択し、[アプリホスト（Apphost）] を有効にします。

また、AP 参加プロファイルで NTP を設定することも推奨されます。

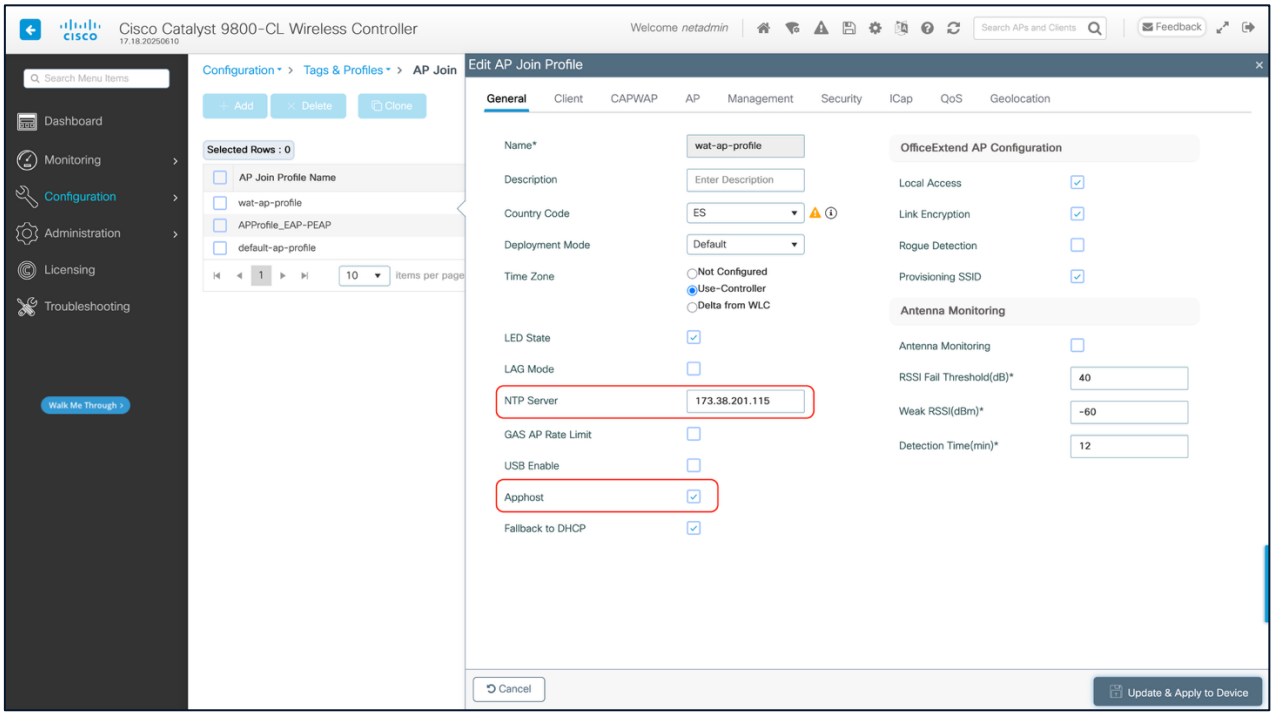

図 8.　　アプリケーション ホスティングの有効化

既存の AP 参加プロファイルとその対応するサイトタグを使用できます。または、それぞれに特定のものを作成できます。以下の例を参照してください。

WebUI：[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [タグ（Tags）]で、[サイト（Site）] タブを選択します。

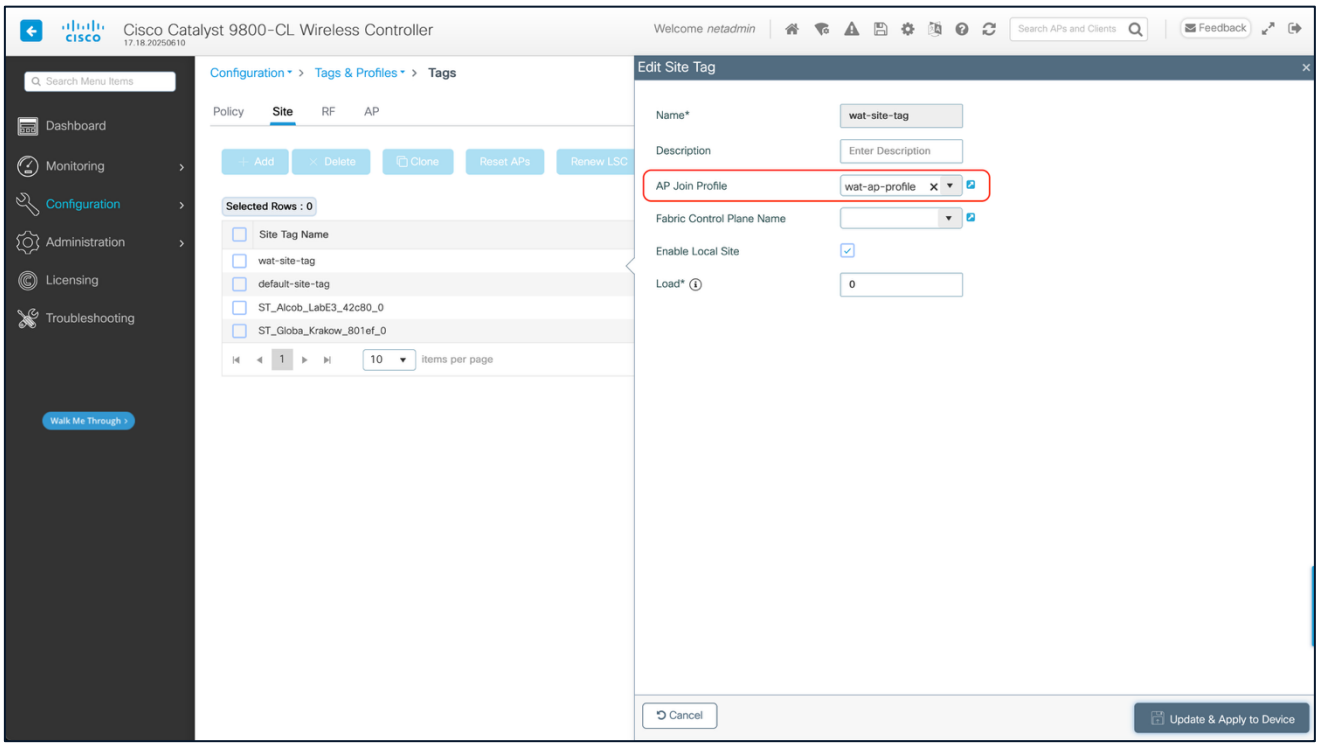

図 9.　　サイト タグ

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
ap profile <ap-profile-name>
 apphost
 ntp ip <ntp-ip-address>

wireless tag site <site-tag-name>
 ap-profile <ap-profile-name>
```

（オプション）プロキシ設定

テスト AP の有線管理 VLAN にプロキシが必要ない場合は、このセクションをスキップできます。

ThousandEyes エージェントをダウンロードし、ThousandEyes プラットフォームとのその後の通信を行うには、インターネットにアクセスできる必要があります。AP 管理 VLAN が直接インターネットにアクセスできず、アクセスするために HTTP プロキシが必要な場合は、AP 参加プロファイルでプロキシを設定します。

注：　現在、基本認証を使用する HTTP プロキシはサポートされていません。

WebUI：[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [AP 参加（AP Join）] > テーブルで [AP 参加プロファイル（AP Join Profile）] をクリックし、AP プロファイル内で [管理（Management）] タブ、[デバイス（Device）] タブの順に選択して、[HTTP プロキシ設定（HTTP Proxy Configuration）] セクションで必要な詳細を入力します。

クライアント プロキシ サーバーは次の形式である必要があります。

```
http://< URL or IP >
https://< URL or IP >
```

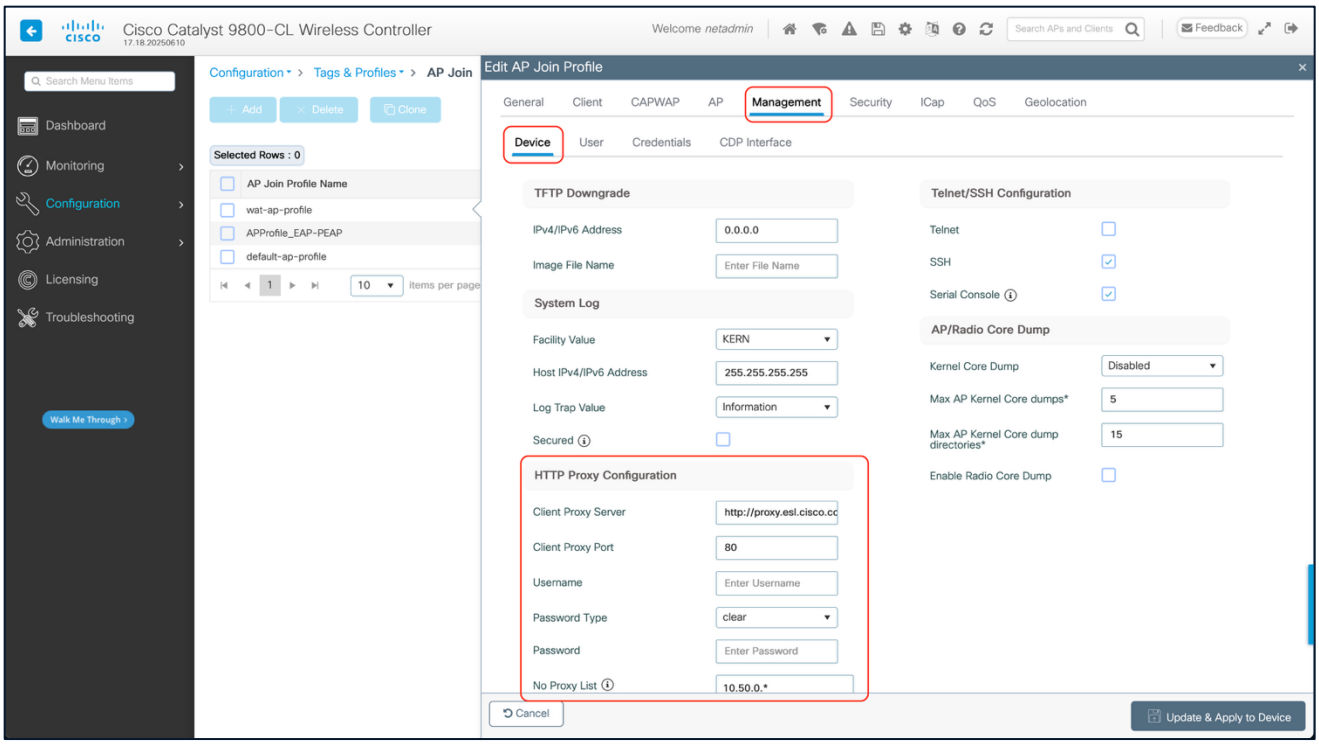

図 10.　　プロキシ設定

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
ap profile <ap-profile-name>
 apphost
 ip http client proxy <hostname>
```

注：　ホスト名は次の形式である必要があります。

```
http://< URL or IP >
https://< URL or IP >
```

設定を確認するには、次のコマンドを実行することを推奨します。次に、出力例を示します。

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
show ap profile name <ap-profile-name> detailed


CW9800#show ap profile name wat-ap-profile detailed
```

```
AP Profile Name                 : wat-ap-profile
[…]
NTP server                      : 173.38.201.115
[…]
Proxy :
  Hostname                      : http://proxy.esl.cisco.com
  Port                          : 80
  NO_PROXY list                 : 10.50.0.*
  Username                      : Not Configured
```

AP タグの割り当て

これは、既存の Cisco Wireless 9800 シリーズ コントローラで有効なものと同じ手順です。このセクションはリマインダのみを目的としています。手順に変更はありません。

サイトタグを割り当てる方法には、いくつかの方法があります。

- **静的**：AP を選択し、特定のタグを割り当てます。設定は、AP のイーサネット MAC アドレスに基づいてコントローラに保存されます。AP がその特定のコントローラに参加すると、常に指定されたタグが割り当てられます。
- **ロケーション**：これは C9800 の内部設定であり（AP ごとに設定可能な AP の場所ではありません）、主に基本セットアップフローで使用されます。ロケーションでは、3 つのタグ（ポリシー、サイト、および RF）グループを作成し、そこに AP を割り当てることができます。
- **フィルタ処理**：正規表現を使用して、コントローラに参加する AP にタグを割り当てることができます。現時点では、AP 名に基づいてフィルタを設定できるため、この方法は設定済みの AP には使用できません。
- **AP**：AP 自体が、プラグアンドプレイ（PnP）を介して学習した、またはコントローラからプッシュされたタグ情報を伝送します。

わかりやすくするために、正規表現フィルタ処理またはタグの一括割り当てを使用します。

正規表現フィルタ処理

AP 名に基づいて正規表現ルールを作成し、タグを割り当てます。

WebUI：[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [タグ（Tags）] > [AP] > [フィルタ処理（Filter）]

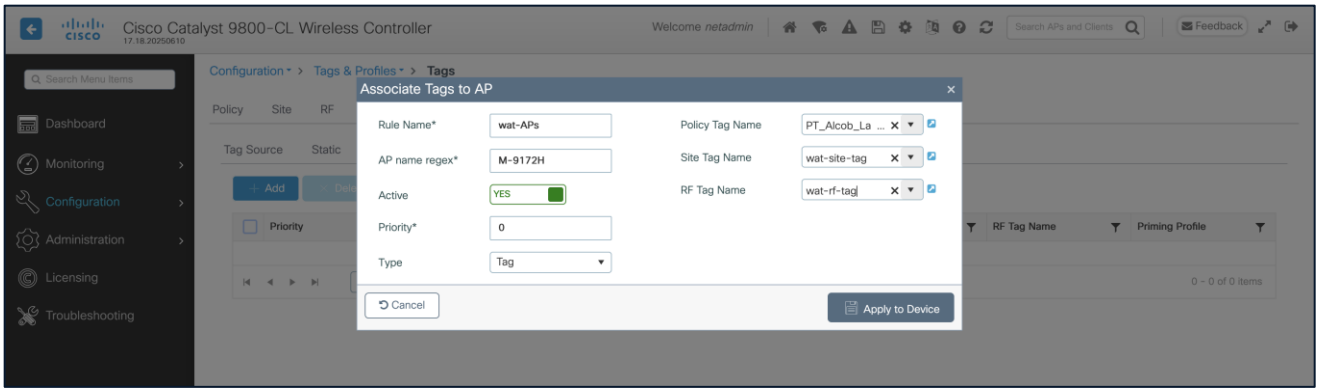

図 11.　　正規表現フィルタの例

CLI を使用して ROMmon ファイルを転送した場合の upgrade コマンドの例：

```
ap filter name wat-APs
 ap name-regex M-9172H
 tag policy PT_Alcob_LabE3_PlantaE_d99eb
 tag rf wat-rf-tag
 tag site wat-site-tag
```

タグの一括割り当て

このメソッドを使用して、複数の AP に同じタグを簡単に割り当てることができます。

WebUI：[設定（Configuration）] > [ワイヤレスセットアップ（Wireless Setup）] > [詳細（Advanced）]

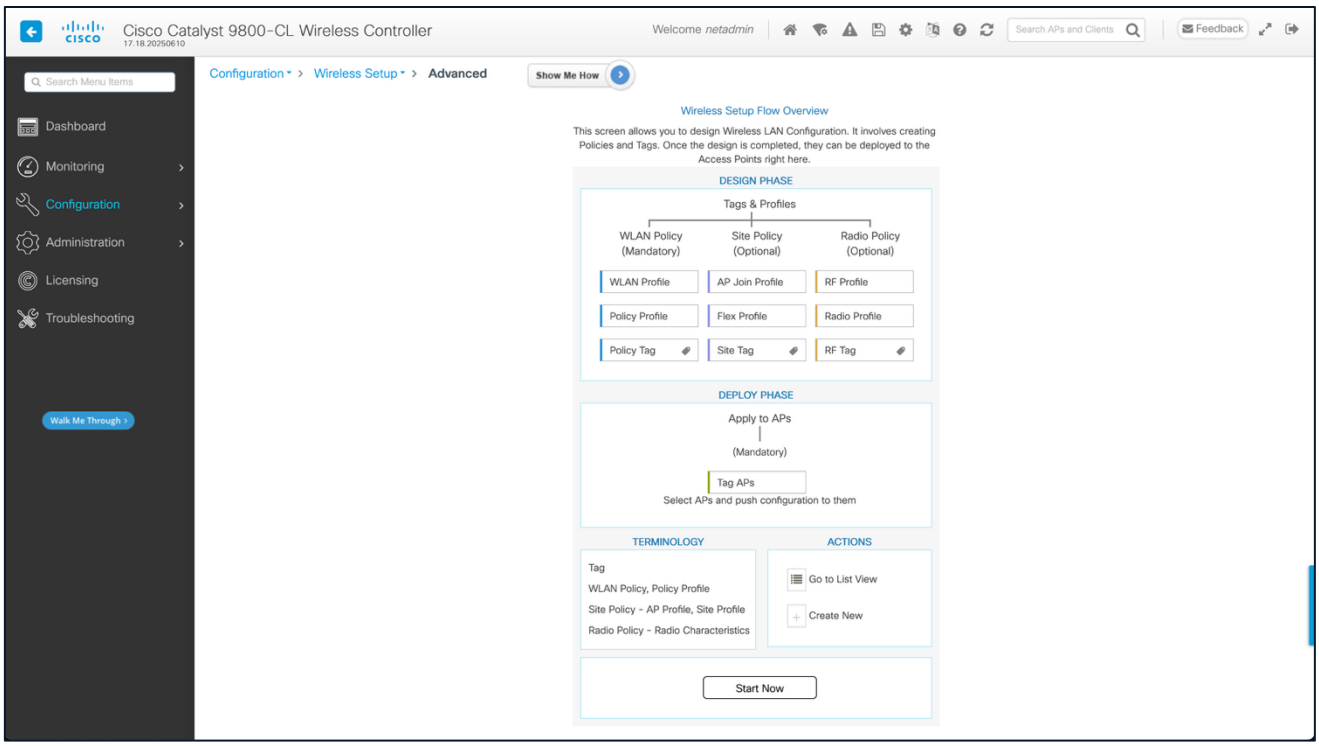

図 12.　　タグの一括割り当てへのアクセス

下部にある [今すぐ開始（Start Now）] をクリックしてから、[適用（Apply）] セクションに移動し、アイコンをクリックして AP リストを表示します。

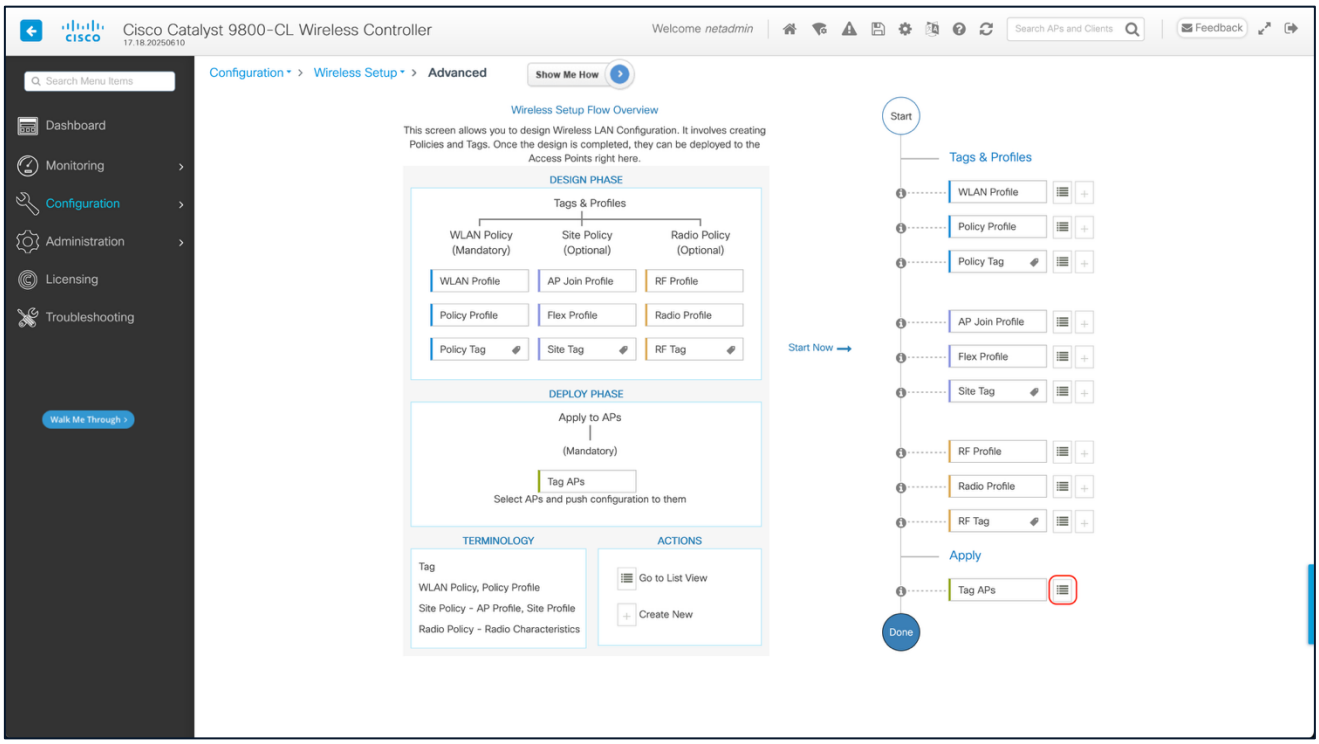

図 13.　　タグの一括割り当て：タグを適用

タグ付けする AP を選択します。

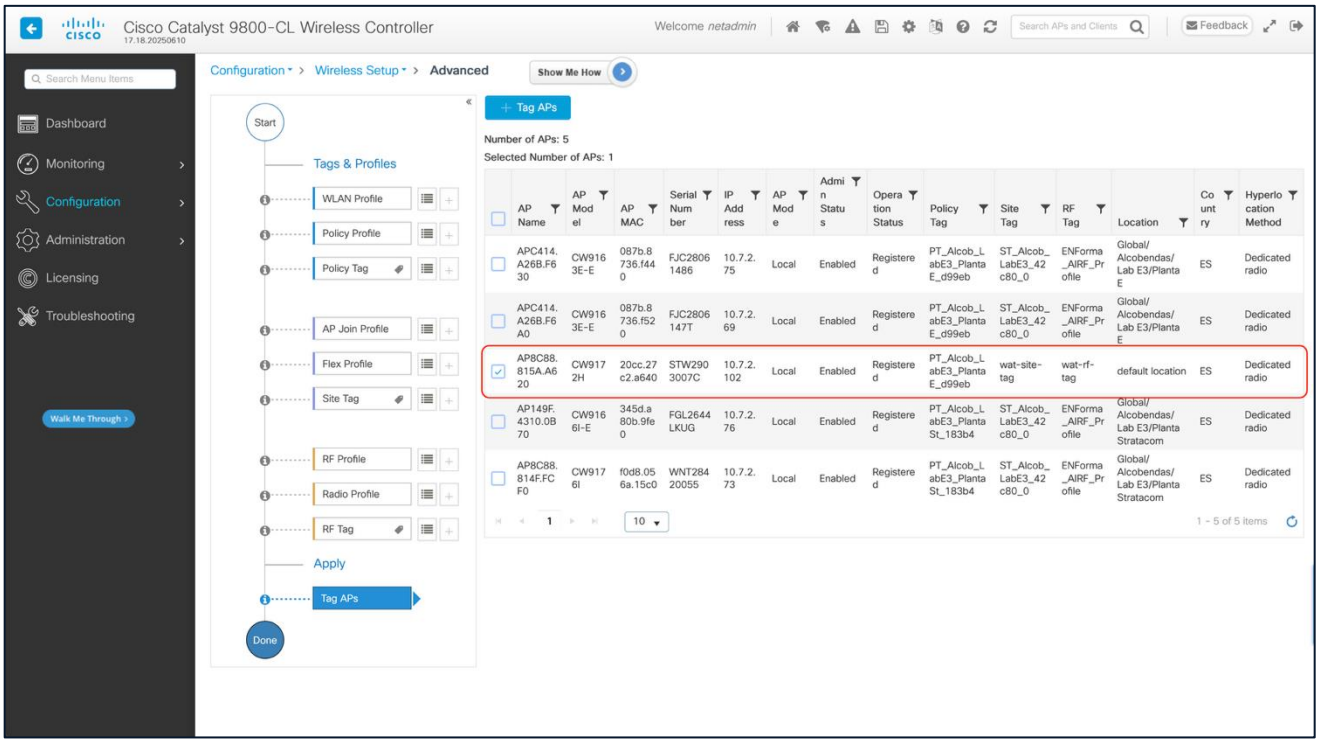

図 14.　　タグの一括割り当て：AP を選択

使用するタグを選択します。

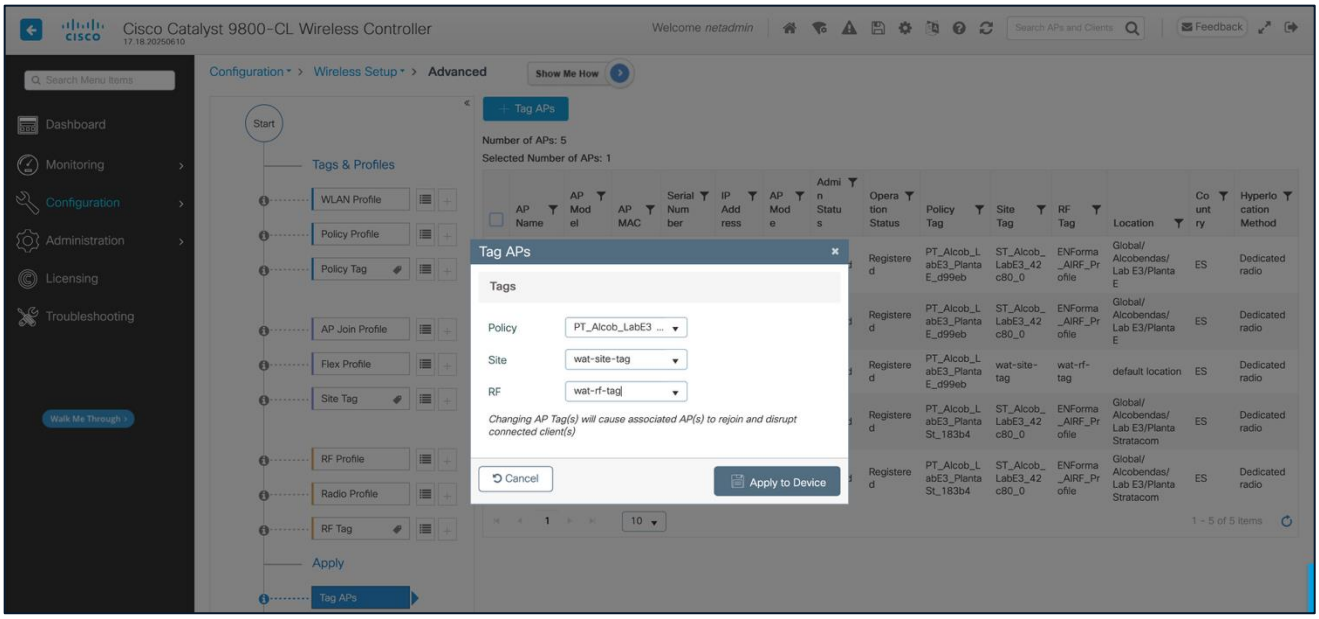

図 15.　　タグの一括割り当て：タグを選択

ThousandEyes でのテストの設定

SSID の設定

エージェント登録を検証しています。

WLC の設定が完了すると、シスコ ワイヤレス アクセス ポイントで実行されているエンドポイント エージェントが ThousandEyes ポータルに表示されます。WLC にインストールした後、エンドポイントエージェントが ThousandEyes プラットフォームに登録されるまでに約 5 ～ 10 分かかることに注意してください。

ThousandEyes プラットフォームで、[Endpoint Experience] に移動してから、[エージェント設定（Agent Settings）] をクリックします。[エージェント設定（Agent Settings）] で、[フィルタの追加（Add Filter）] をクリックします。次に、[プラットフォーム（Platform）] フィルタで [シスコワイヤレス（Cisco Wireless）] を選択します。これにより、ワイヤレスアクセスポイントにインストールされているエンドポイント エージェントのみが表示されます。

SSID の設定

エンドポイントエージェントがアクセスポイントにインストールされ、ThousandEyes プラットフォームに正常に登録されていることを確認したら、次のステップは SSID の設定です。エンドポイントエージェントはこれらの SSID を使用して、目的の SSID をブロードキャストしているさまざまな AP に接続し、それらの AP 間を循環します。SSID を設定するには、[SSID 設定（SSID Configurations）] に移動し、[SSID 設定の作成（Create SSID Configuration）] をクリックします。

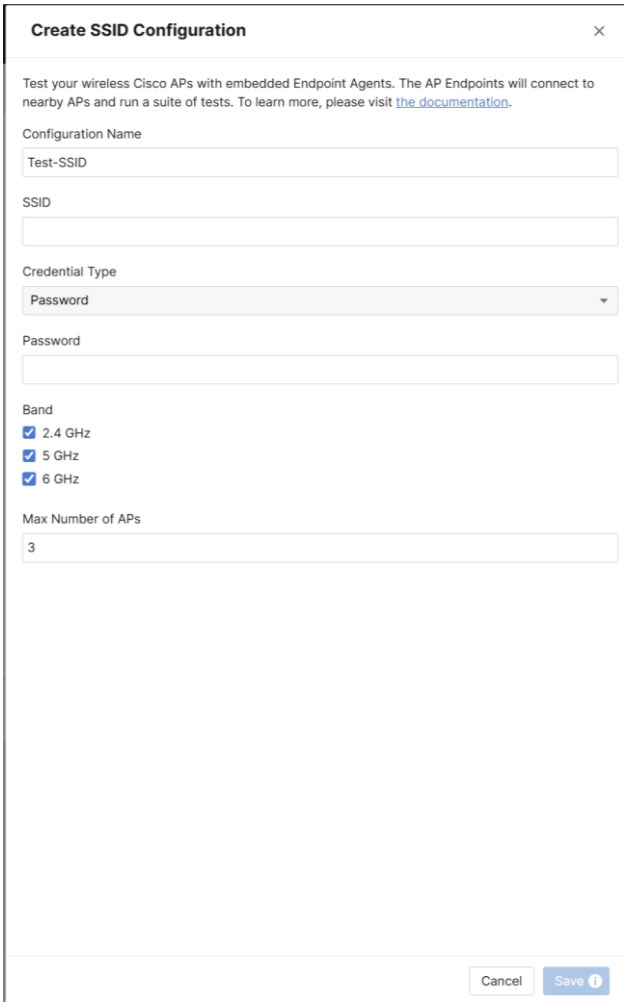

図 16.　　SSID の設定

注：　アクティブなテスト AP ごとに最大 3 つの SSID を設定できます。

[SSID 設定（SSID Configuration）] セクションには、次のフィールドが含まれます。

- **[設定名（Configuration Name）]**：設定の任意の名前。
- **SSID**：アクティブ テスト アクセスポイントがオンボードされたときに ThousandEyes にインポートされる、使用可能な SSID のリスト。このドロップダウンメニューでは、この設定の優先 SSID を選択できます。また、これらの提案に限らず、任意の SSID を手動で設定することもできます。
- **[クレデンシャルタイプ（Credential Type）]**：認証設定を指定します。認証オプションについては以下で説明します。
- **[バンド（Band）]**：テスト用のワイヤレス帯域を指定します。
- **[最大 AP 数（Max Number of APs）]**：アクティブ テスト アクセスポイントが 1 回にテストする BSSID の最大数を指定します。

Credential Type

アクティブ テスト アクセスポイントが SSID に接続して認証するには、認証が必要です。[SSID 設定（SSID Configuration）] セクションの [クレデンシャルタイプ（Credential Type）] フィールドで、使用する認証のタイプを指定できます。次のオプションを使用できます。

- パスワード
- ユーザー名/パスワード
- 証明書
- オープン

パスワード

[パスワード（Password）] を選択した場合は、この SSID に使用する PSK（事前共有キー）を入力する必要があります。

ユーザー名/パスワード

[ユーザー名/パスワード（Username/Password）] を選択した場合は、サポートされている EAP メソッド（PEAP、LEAP、または EAP-FAST）のいずれかを選択し、対応するユーザー名とパスワードを指定する必要があります。

証明書

[証明書（Certificate）] を選択した場合は、[LSC]（ローカルで有効な証明書）オプションまたは [手動（Manual）] オプションのいずれかを選択する必要があります。

LSC は、アクセスポイント（AP）でプロビジョニングされたデジタル証明書を管理および制御できる機能です。LSC を使用すると、証明書が独自の認証局（CA）から直接発行されるため、監視とセキュリティが強化されます。LSC は、一般的に、**有線 802.1X 認証を保護する**ために使用されます。LSC とその設定方法の詳細については、次のガイドを参照してください。https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9100-access-points/221127-configure-locally-significant-certificat.html

使用可能な証明書のオプションは次のとおりです。

- [LSC] が選択されている場合、次の 3 つの設定オプションを使用できます。
  - **[EAP 外部アイデンティティ（EAP Outer Identity）]**：オプションのフィールドです。指定しない場合、デフォルトで「anonymous」になります。
  - **[サーバー証明書の確認（Verify Server Certificate）]**：デフォルトで有効になっています（推奨）。有効にすると、エージェントは RADIUS サーバー証明書を検証します。無効にすると、エージェントは RADIUS 証明書を検証しません。
  - **[信頼できるサーバーCA 証明書（Trusted Server CA Certificate）]**：オプションのフィールドです。異なる認証局（CA）がインフラストラクチャ証明書（AP 証明書や WLC 証明書など）と RADIUS サーバー証明書を発行する環境では、クライアントは、安全に認証するために、RADIUS 証明書を発行した CA を信頼する必要があります。したがって、複数の CA が使用されている場合は、この設定に RADIUS サーバー証明書に署名する CA を入力する必要があります。同じ CA が AP/WLC 証明書と RADIUS サーバー証明書の両方に署名しており、すでにクライアントデバイスによって信頼されている場合、このフィールドを指定する必要はありません。
- [手動（Manual）] が選択されている場合、次の 5 つの設定オプションを使用できます。
  - **[クライアントバンドル（PKCS #12）（Client Bundle (PKCS #12)）]：** クライアントバンドルは、クライアント証明書チェーンと秘密キーを含む単一の PKCS#12 ファイル（.p12 または .pfx）ファイルです。

- **[秘密キーのパスワード（Private Key Password）]**：オプションのフィールドです。クライアントバンドル内の秘密キーをロック解除するために使用されるパスワード。PKCS#12 ファイルにパスワードがない場合は空のままにします。
- **[EAP 外部アイデンティティ（EAP Outer Identity）]**：オプションのフィールドです。指定しない場合、デフォルトで「anonymous」になります。
- **[サーバー証明書の確認（Verify Server Certificate）]**：デフォルトで有効になっています。有効にすると、エージェントは RADIUS サーバー証明書を検証します。無効にすると、エージェントは RADIUS 証明書を検証しません。
- **[信頼できるサーバーCA 証明書（Trusted Server CA Certificate）]**：オプションのフィールドです。異なる認証局（CA）がインフラストラクチャ証明書（AP 証明書や WLC 証明書など）と RADIUS サーバー証明書を発行する環境では、クライアントは、安全に認証するために、RADIUS 証明書を発行した CA を信頼する必要があります。したがって、複数の CA が使用されている場合は、この設定に RADIUS サーバー証明書に署名する CA を入力する必要があります。同じ CA が AP/WLC 証明書と RADIUS サーバー証明書の両方に署名しており、すでにクライアントデバイスによって信頼されている場合、このフィールドを指定する必要はありません。

オープン（認証なし）
このオプションを選択すると、認証は必要ありません。

ワイヤレスアクティブテストの設定

WLC からインポートされた SSID を ThousandEyes プラットフォームで設定したら、ワイヤレステストの設定に進むことができます。このセクションでは、ワイヤレスアクティブテスト設定を作成し、以前に設定した SSID をアクティブ テスト アクセスポイントに関連付けます。

[Endpoint Experience] に移動し、[テスト設定（Test Settings）] をクリックして、[ワイヤレスアクティブテスト（Wireless Active Testing）] を選択し、[新しいワイヤレステストの作成（Create New Wireless Test）] をクリックします。

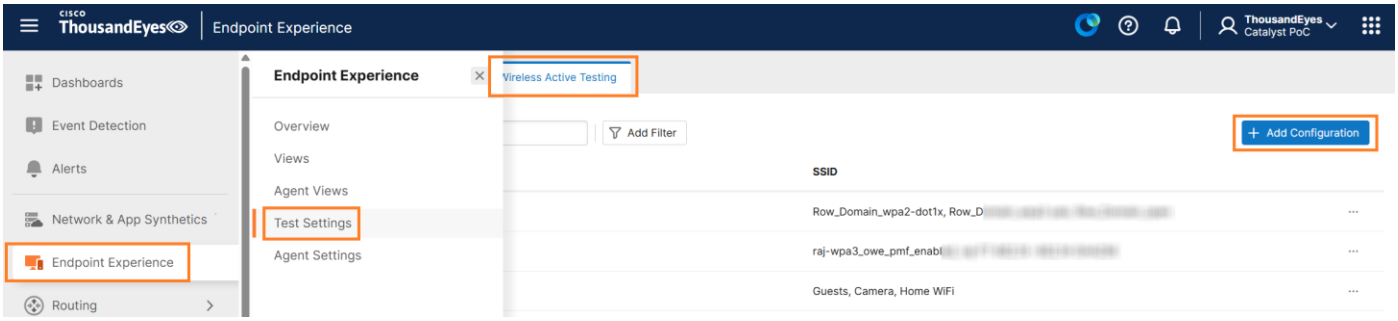

図 17.　　ワイヤレスアクティブテスト設定 - 1

次の図に示すように、ワイヤレスアクティブテストのセクションは 3 つのパートで構成されています。

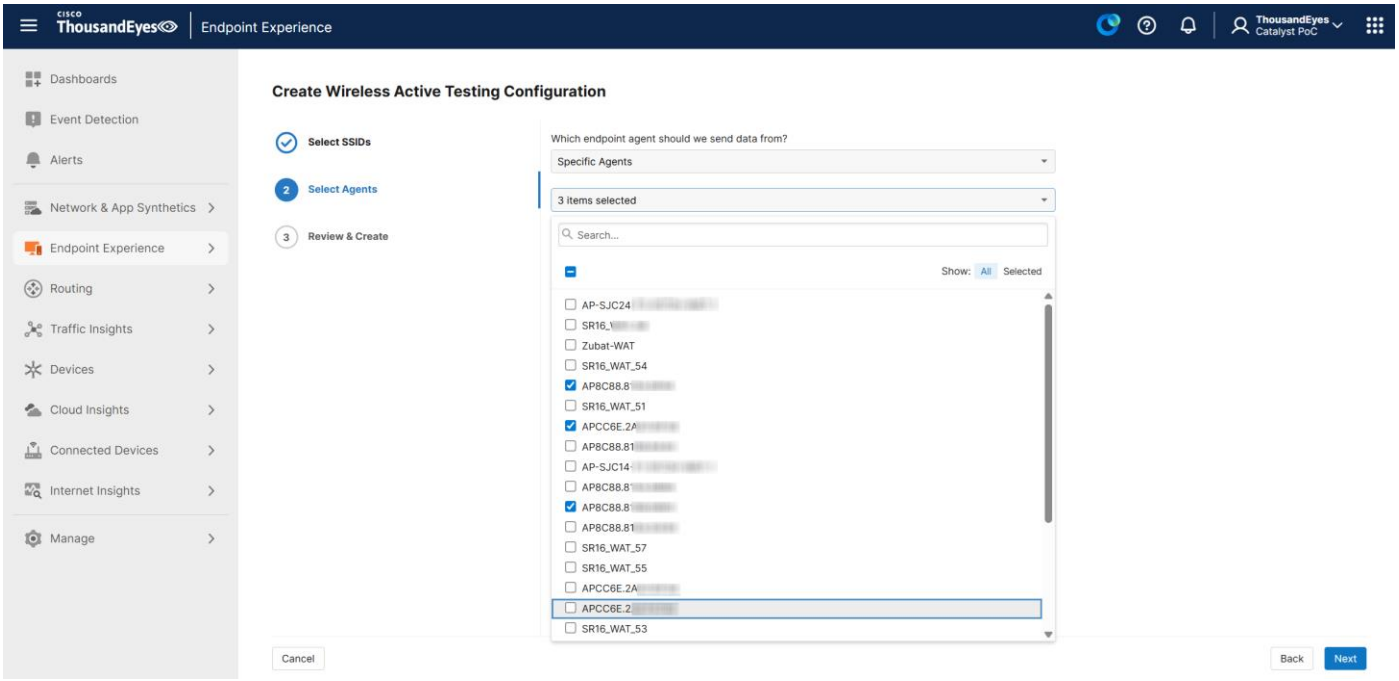

図 18.　　ワイヤレスアクティブテスト設定 - 2

4. **[SSID を選択（Select SSIDs）]**：ワイヤレスセンサー設定の名前を入力し、ワイヤレスアクティブ テスト用に最大 3 つの SSID を選択します。

1. **[エージェントを選択（Select Agents）]**：テスト用にこれらの SSID に関連付けるエンドポイントエージェントを選択します。前に選択した SSID をテストに使用するエンドポイントエージェントを選択する際、次の 3 つのオプションがあります。

   - **[すべてのエージェント（All Agents）]**：アクセスポイントで実行されているすべてのエンドポイントエージェント
   - **[特定のエージェント（Specific Agents）]**：選択したエンドポイントエージェントのみ
   - **[エージェントラベル（Agent Labels）]**：特定のラベルに関連付けられているエンドポイントエージェントのみ。

注：　エージェントラベルは、エージェントをグループ化または管理するためのタグとして機能する論理構造です。サンプルについては、次のセクションを参照してください。

2. **[確認と作成（Review & Create）]**：最後の部分では、設定を確認し、すべて問題がなければ、[作成（Create）] をクリックします。設定が完了すると、アクティブ テスト アクセスポイントが設定された SSID への接続を開始し、ワイヤレスメトリックの収集を開始します。

注：　設定完了後、ThousandEyes プラットフォームでデータが使用可能になるまでに最大 20 分かかる場合があります。ただし、通常はそれよりも短時間で終わります。

エンドポイント エージェント ラベルの設定

エージェントラベルは、エージェントをグループ化または管理するためのタグとして機能する論理構造です。エージェントの使用方法はいくつかあり、たとえば、AP で実行されているすべてのエージェントに 1 つのラベルを作成

することができます。その場合、プラットフォームフィルタを使用して、アクセスポイント：シスコワイヤレスで実行されているすべてのエージェントを選択できます。

注： SSID ベースのラベルは、ワイヤレスアクティブテスト設定内では使用できないことに注意してください。

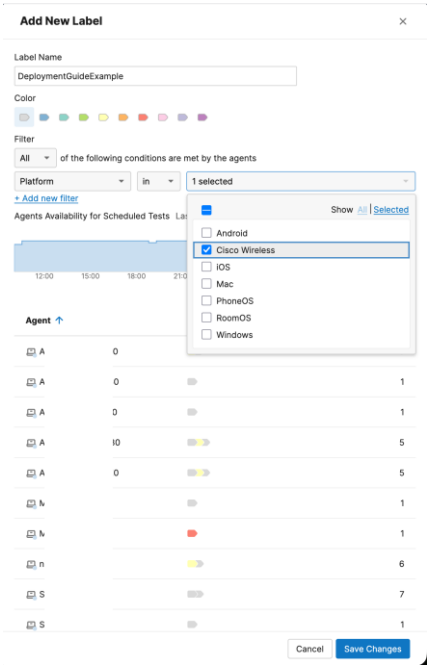

図 19. シスコ ワイヤレス エージェント ラベル フィルタ

ラベルの詳細については、次のドキュメントを参照してください。https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/configuring/configure-endpoint-agent-labels

詳細については、https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/configuring/configure-endpoint-agent-labels を参照してください。

模擬テストの設定

ThousandEyes エンドポイントエージェントを使用したワイヤレス アクティブ テストでは、ワイヤレスモニタリングに加えて、重要なビジネスアプリケーションの模擬テストを設定できます。設定プロセスは、他のエンドポイントエージェントの場合と同じです。詳細な手順とベストプラクティスについては、「Monitoring an Application using Synthetic Tests」を参照してください。

ThousandEyes でのワイヤレス アクティブ テスト データの活用

ThousandEyes プラットフォームでのワイヤレス アクティブ テスト データの解釈と利用

このセクションでは、ThousandEyes プラットフォーム内のワイヤレス アクティブ テストのデータに焦点を当てています。これらのテストから生成されたテストデータを解釈し、効果的に使用する方法について説明します。

エンドポイントエージェントのデータの表示に関するより広範なガイダンスについては、次のドキュメントを参照してください。https://docs.thousandeyes.com/product-documentation/end-user-monitoring/viewing-data#local-networks-view

ダッシュボード

ダッシュボードを使用すると、大量のテストデータのモニターと可視化が簡単に行えます。これにより、問題を迅速に特定して解決できます。

テスト結果を効率的に追跡し、外部支援の必要性を減らすために、シスコではダッシュボードテンプレートを提供しています。これらのテンプレートにより一貫性を促進し、複数のアカウント組織を管理するためのベストプラクティスをサポートします。

詳細については、次の記事を参照してください。

- **ダッシュボードテンプレートの使用**：https://docs.thousandeyes.com/product-documentation/dashboards/dashboard-templates
- **ダッシュボードのカスタマイズ**：https://docs.thousandeyes.com/product-documentation/dashboards/customizing-your-dashboard
- **ダッシュボードのドリルダウンによるトラブルシューティング**：https://docs.thousandeyes.com/product-documentation/dashboards/troubleshooting-with-drill-down

単一エージェントビュー

ThousandEyes プラットフォームで、[Endpoint Experience] > [エージェントビュー（Agent Views）] の順に選択します。

[検索（Search）] セクションを使用して、調査する特定のエンドポイントエージェントを入力して選択します。

エージェントビュー画面は複数のセクションに分割されています。

[メトリック（Metrics）] セクションで、[接続（Connection）] を選択し、右側にある [メトリック（Metrics）] ドロップダウンメニューから [RSSI] を選択します。

中央のグラフには、選択したタイムフレーム中にテストされた SSID が、対応する RSSI 値とともに表示されます。

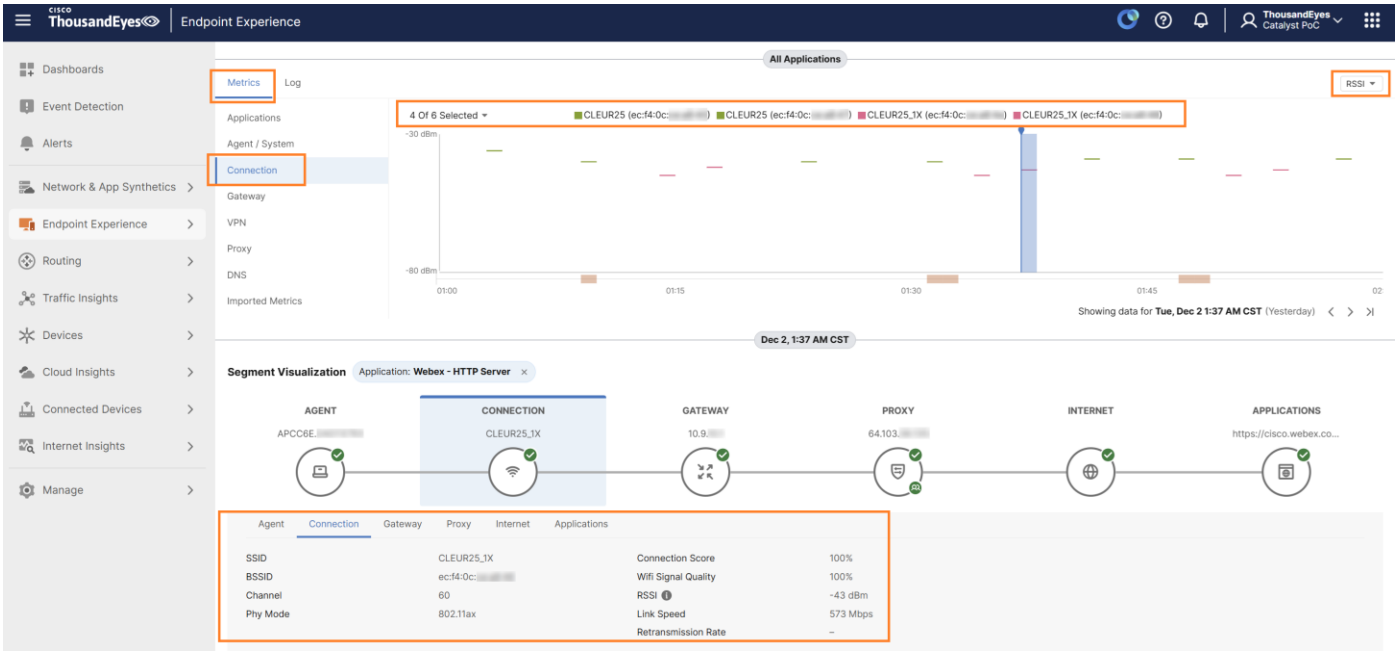

図 20.　　単一エージェントビュー

[セグメントの可視化（Segment Visualization）] セクションの [接続（Connection）] タブでは、SSID、BSSID、チャンネル、Phy モード、接続スコア、Wi-Fi 信号品質、RSSI、リンク速度などのワイヤレス関連データを表示できます。

[メトリック（Metrics）] の横にある [ログ（Log）] タブをクリックすると、選択したタイムフレーム中に報告されたログを表示できます。これらのログには、イベントの詳細なエントリが記録されます。

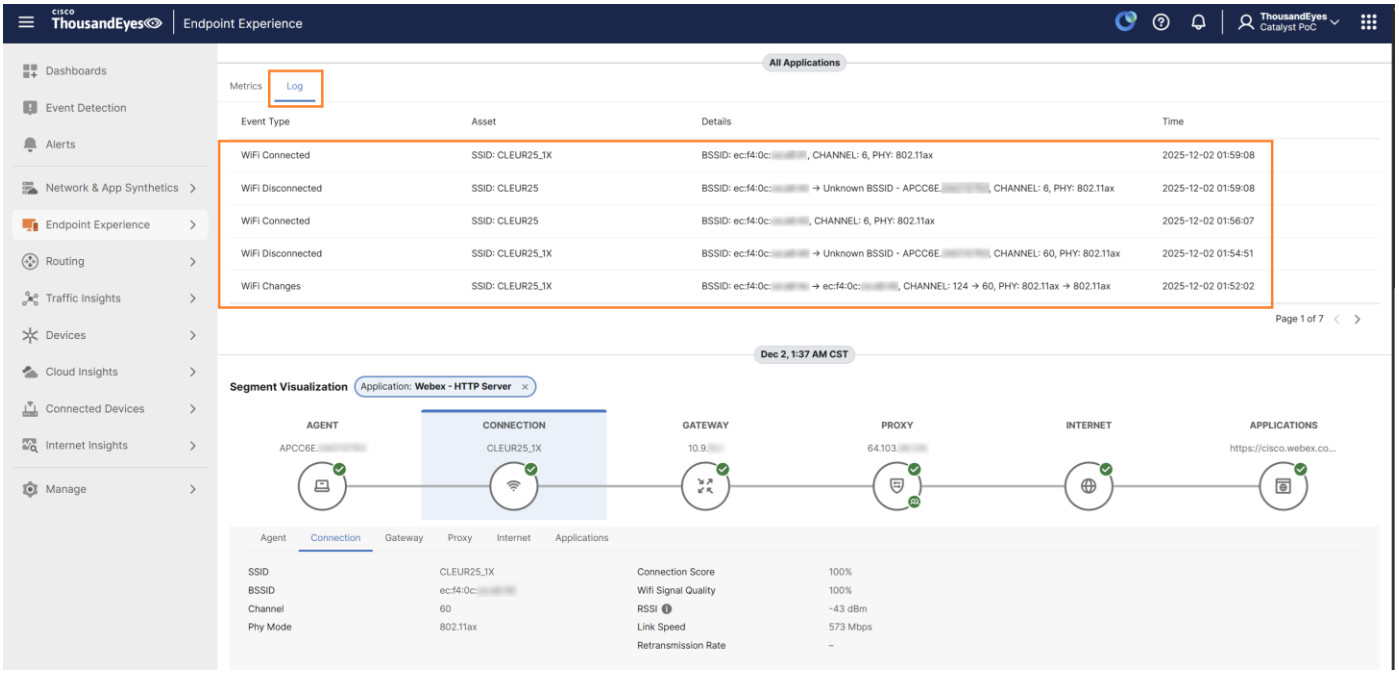

図 21.　　単一エージェントビューでのログ

ローカルネットワークビュー

ローカルネットワークビューでは、個々のエージェントに焦点を当てる単一エージェントビューとは異なり、複数のエンドポイントエージェント間で集約されたワイヤレスデータを表示できます。このビューにアクセスするには、[Endpoint Experience] > [ビュー（Views）] に移動してから、[ローカルネットワークとワイヤレス（Local Networks and Wireless）] を選択します。

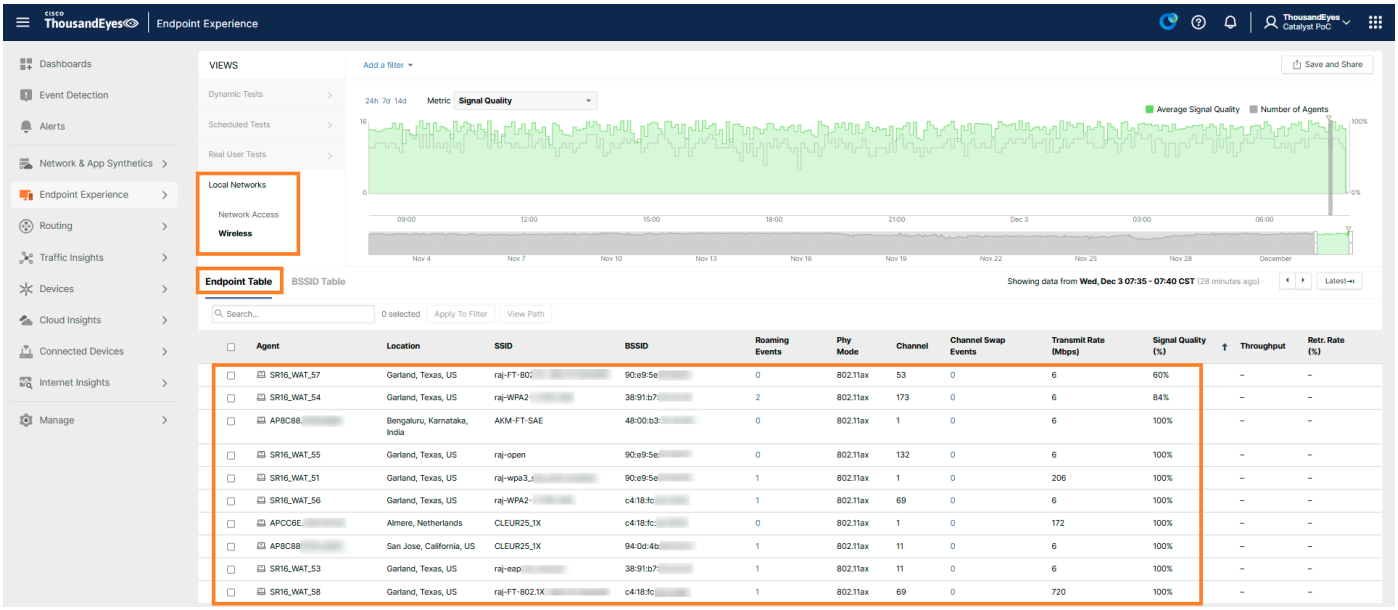

図 22.　　ローカルネットワーク：エンドポイントテーブル

このビューの [エンドポイントテーブル（Endpoint Table ）] には、選択したタイムフレーム中にアクティブだったすべてのエンドポイントエージェントが、関連するワイヤレスメトリックとともに表示されます。

BSSID テーブルは、同じビューを BSSID の観点から提供します。

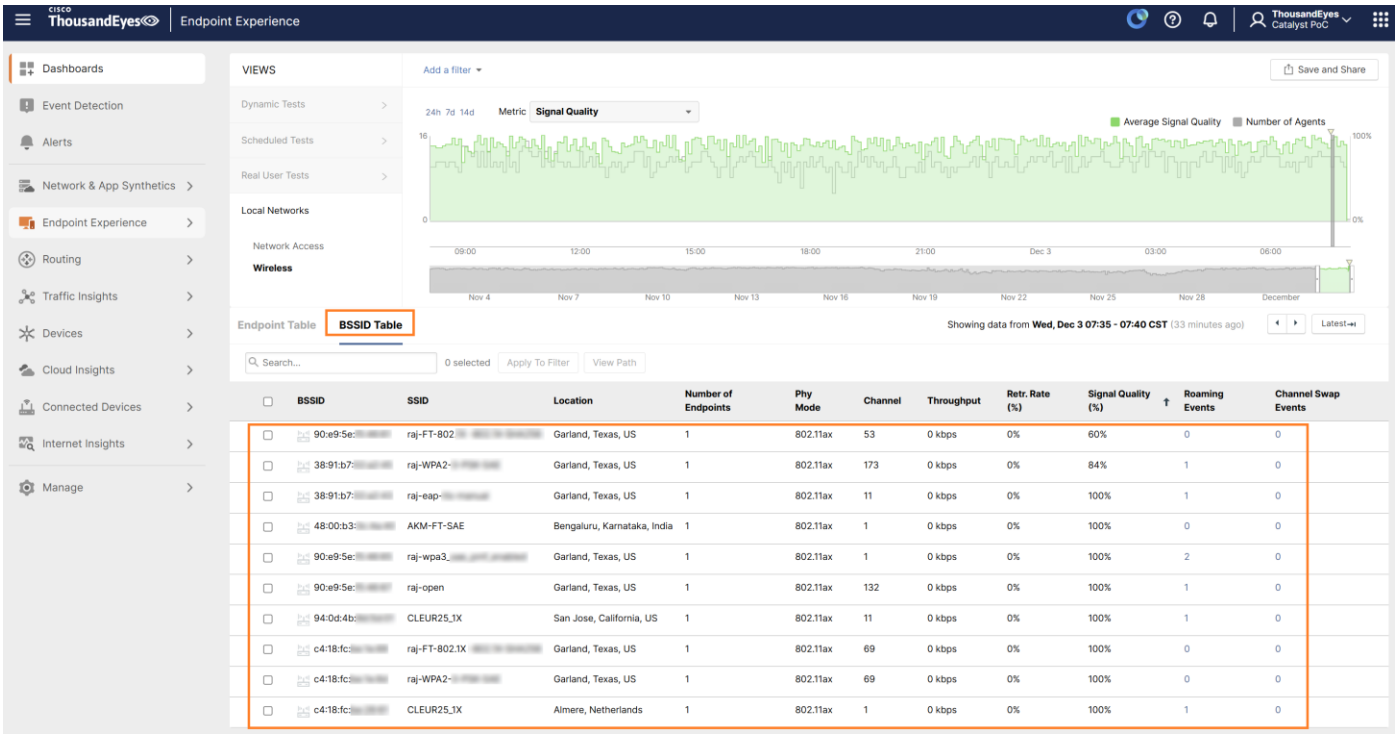

図 23.　　ローカルネットワーク：**BSSID** テーブル

付録

異なる SSID で異なるアプリケーションをテストする方法

シナリオによっては、SSID A と SSID B で異なる対象をテストする必要がある場合が考えられます。たとえば、SSID A は社内 SSID で、SSID B はゲスト SSID の場合などです。

手順は次のとおりです。

1. SSID A の **SSID** 設定を作成します（「SSID の設定」ステップを参照）。
2. SSID B の **SSID** 設定を作成します。
3. **エージェントラベル**「L1」を作成します。これは必須ではありませんが、「エンドポイント エージェント ラベルの設定」で説明されているように、大規模な管理の場合は推奨されます。
4. SSID A と SSID B の両方を選択して**ワイヤレスセンサー設定**を作成します。その後、エージェントラベル L1 に割り当てます（ラベルを使用しない場合は、エージェントに直接割り当てます）。
5. **エージェントラベル**「SSID_A_tests」を作成し、「SSID A」の「SSID」フィルタを使用して設定します。

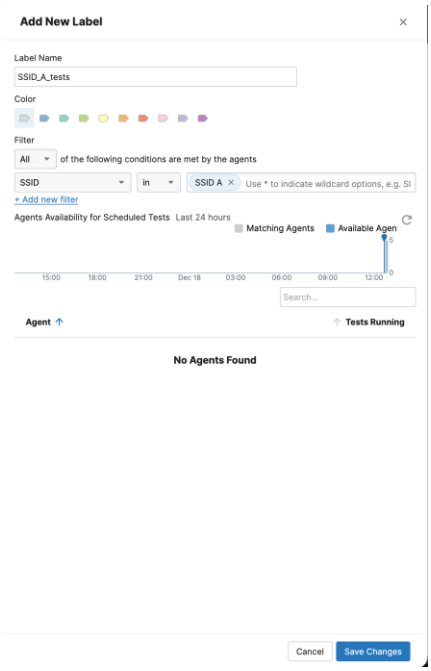

図 24.　　エージェントラベル SSID A フィルタ

6. **エージェントラベル**「SSID_B_tests」を作成し、「SSID B」の「SSID」フィルタを使用して設定します。
7. SSID A でテストする**スケジュール済みテスト**を、ラベル「SSID_A_tests」に割り当てます。
8. SSID B でテストする**スケジュール済みテスト**を、ラベル「SSID_B_tests」に割り当てます。

テストサイクルで SSID が変更されるたびに、エージェントは接続中の SSID を確認し、適切なテストを実行します。

トラブルシューティング

AP で次のコマンドを実行すると、アクティブテストについての詳細情報を取得できます。

```
show wat configuration
show wat agent status
show wat manager stats
show wat manager history
show wat logs
show wat test configuration
show wat test summary
show wat detail
```

便利な参考資料

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア設定ガイド、Cisco IOS XE 17.18.x：ワイヤレスアクティブテスト：https://www.cisco.com/content/en/us/td/docs/wireless/controller/9800/17-18/config-guide/b_wl_17_18_cg/m_thousandeyes-integration-enhancements.html

ThousandEyes ワイヤレスアクティブテスト設定ガイド：https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents/wireless-active-testing

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。