



センサーの管理とセンサー主導のテスト

- [センサーとセンサー主導のテストについて \(1 ページ\)](#)
- [センサーのプロビジョニング \(2 ページ\)](#)
- [センサーを使用したネットワーク正常性のモニターとトラブルシューティング \(8 ページ\)](#)
- [センサーの管理とバックホールの設定 \(16 ページ\)](#)
- [SCEP プロファイルの管理 \(21 ページ\)](#)
- [センサー主導テスト \(22 ページ\)](#)

センサーとセンサー主導のテストについて

センサーはセンサー主導のテストを使用して、ワイヤレスネットワークの正常性を判断します。ワイヤレスネットワークには、AP 無線、WLAN の設定、ワイヤレス ネットワーク サービスが含まれます。

アシュアランス専用センサーをサポートしています。これはセンサー機能を実行するための専用ハードウェアです。

専用の Cisco Aironet 1800s アクティブセンサーは、PnP を使用してブートストラップされます。このセンサーは、アシュアランスサーバーの到達可能性の詳細を取得すると、アシュアランスサーバーと直接通信します。

サポート対象のセンサーとシスコ ワイヤレス コントローラのソフトウェアリリース

センサー機能に必要なシスコ ワイヤレス コントローラと Cisco Aironet 1800s アクティブセンサーイメージの最小ソフトウェアバージョンは、次のとおりです。

サポート対象のセンサーとワイヤレスコントローラ	最小ソフトウェア リリース
シスコ ワイヤレス コントローラ (35xx、55xx、85xx)	8.5.115.0

サポート対象のセンサーとワイヤレスコントローラ	最小ソフトウェア リリース
Cisco Catalyst 9800 ワイヤレスコントローラ	IOS-XE 16.12.1s 以降
Cisco Aironet 1800s アクティブ センサー	8.8.263.0

センサーのプロビジョニング

ワイヤレス Cisco Aironet 1800s アクティブ センサーのプロビジョニング

ステップ 1 イーサネットモジュールなしで Cisco Aironet AP 1800S センサーを使用している場合は、ワイヤレスコントローラの Cisco プロビジョニング SSID を有効にする必要があります。

(注) ソフトウェアリリース 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサーデバイスプロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。 [バックホールの設定の管理 \(18 ページ\)](#) を参照してください。

Cisco ワイヤレス コントローラについては、 [ワイヤレス コントローラのプロビジョニング SSID の有効化 \(3 ページ\)](#) を参照してください。

Cisco Catalyst ワイヤレス コントローラについては、 [Cisco Catalyst ワイヤレスコントローラのシスコプロビジョニング SSID の有効化 \(3 ページ\)](#) を参照してください。

ステップ 2 センサのバックホール設定を作成します。

『[バックホールの設定の管理 \(18 ページ\)](#)』を参照してください。

ステップ 3 Cisco Aironet 1800s アクティブ センサーをプロビジョニングします。

『[ワイヤレスまたはセンサー デバイスのプロビジョニング \(4 ページ\)](#)』を参照してください。

ステップ 4 (オプション) デバイスインベントリでセンサーデバイスが使用可能になった後、ソフトウェアイメージのアップグレードを選択できます。 [Cisco DNA Center ユーザガイド](#) の「ソフトウェア イメージのプロビジョニング」のトピック を参照してください。

ワイヤレスコントローラのプロビジョニング SSID の有効化

ステップ 1 Cisco ワイヤレスコントローラにログインします。

[ネットワークサマリー (Network Summary)] ページが表示されます。

ステップ 2 [Advanced] タブをクリックします。

[概要 (Summary)] ページが表示されます。

ステップ 3 上部のメニューバーで、[管理 (Management)] タブをクリックします。

ステップ 4 左側のナビゲーションウィンドウで、[クラウドサービス (Cloud Services)] > [センサ (Sensor)] を選択します。

[バックホール設定 (Backhaul Configuration)] ページが表示されます。

ステップ 5 [SSID] フィールドに「**TFTP**」と入力します。

ステップ 6 [Auth-type] ドロップダウンリストから [Open] を選択します。

ステップ 7 [Provisioning] ドロップダウンリストから [Enable] を選択します。

ステップ 8 [DHCP Interface] ドロップダウンリストが [management] に設定されていることを確認します。

ステップ 9 [Apply] をクリックします。

プロビジョニングを有効化すると、[CiscoSensorProvisioning] という非表示の WLAN が作成され、センサーは EAP-TLS クライアント証明書を使用して参加します。これにより、センサーは DHCP オプション 43 を使用するか、または DNS を介して Cisco DNA Center の IP アドレスを見つけることができます。

Cisco Catalyst ワイヤレスコントローラのスコーププロビジョニング SSID の有効化

ステップ 1 Cisco Catalyst ワイヤレスコントローラ GUI にログインします。

ステップ 2 左側のナビゲーションペインで、[Configuration] > [Cloud Services] の順に選択します。

[Cloud Services] ページが表示されます。

ステップ 3 [Network Assurance] タブで、次の手順を実行します。

- [Network Assurance Configuration] 領域で、[Service Status] トグルを [Enabled] に設定します。
- [Provisioning] エリアで、[Provisioning] トグルを [Enabled] に設定します。

ステップ 4 (オプション) [VLAN Interface] フィールドに VLAN インターフェイスの名前を入力します。

ステップ 5 [Apply] をクリックします。

プロビジョニングを有効化すると、[CiscoSensorProvisioning] という非表示の WLAN が作成されます。ウィンドウの右下隅に、次のエラーメッセージが表示されます。

Error in Configuring

CLI Line 2 Please associate the wlan and policy profile CiscoSensorProvisioning to the desired AP.

(注) このメッセージはエラーではありません。メッセージには、実行する必要があるアクションに関する情報が表示されます。

ステップ 6 [CiscoSensorProvisioning] ポリシープロファイルが作成されていることを確認します。

a) 左側のナビゲーションペインで、**[Configuration]** > **[Policy]** の順に選択します。

[Policy Profile] ページが表示されます。

b) [CiscoSensorProvisioning] ポリシーが [Policy Tag Name] カラムの下に表示されていることを確認します。

ステップ 7 WLAN および [CiscoSensorProvisioning] ポリシープロファイルを適切な AP に関連付けます。次の手順を実行します。

a) 左側のナビゲーションペインで、**[Configuration]** > **[Tags]** の順に選択します。

[Manage Tags] ページが表示されます。

b) [Policy] タブで [Add] をクリックします。

c) [Name] フィールドにポリシータグの一意の名前を入力します。

d) [Add] をクリックします。

e) [WLAN Profile] ドロップダウンリストから [CiscoSensorProvisioning] を選択します。

f) [Policy Profile] ドロップダウンリストから、[CiscoSensorProvisioning] を選択します。

g) ✓ をクリックします。

h) [Save & Apply to Device] をクリックしてポリシータグを保存します。

(注) AP のポリシータグを変更すると、AP に関連付けられているクライアントが切断され、再接続される可能性があります。

ワイヤレスまたはセンサー デバイスのプロビジョニング

この手順では、[プラグアンドプレイデバイス (Plug And Play Devices)] リストからデバイスを要求する方法について説明します。代わりに、[Claim] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『[Network Plug and Play Troubleshooting Guide for Cisco DNA Center](#)』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- ネットワーク階層内のサイトを定義します。[ネットワーク階層の設計](#)を参照してください。

- デバイスの CLI および SNMP ログイン情報を定義します。



(注) CLI、SNMPv2c、または SNMPv3 ログイン情報を使用してワイヤレスデバイスを要求できます。SNMPv2cを使用している場合は、読み取りと書き込みの両方のログイン情報を指定します。

- 必要に応じて、イメージを展開する場合は、プロビジョニングされる Cisco Catalyst 9800-CL デバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。



(注) Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ導入プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。プラグアンドプレイプロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- センサー デバイスをプロビジョニングするには、センサーが Cisco DNA Center エンタープライズ IP アドレス (private/enp9s0) を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Cisco DNA Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ (DHCP オプション 42) とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Cisco DNA Center の仮想 IP アドレスです。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します : **[Provision]** > **[Plug and Play]**。

ステップ 2 テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。


ステップ 4 デバイステーブルの上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

ステップ 5 (任意) **[Assign Site]** ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。

b) 次のいずれかを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、**[Assign]** をクリックし、**[Select a Site]** ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、**[Actions]** 列で、省略記号アイコン **...** の上にカーソルを置き、**[Apply Site to All]** を選択します。

- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions]列で、省略記号アイコン  の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

割り当てられたサイトに関連付けられているワイヤレス ネットワーク プロファイルにオンボーディング テンプレートがある場合、Cisco DNA Center はこのテンプレートを PnP オンボーディングに使用します。

(注) **[System] > [Settings] > [Device Settings] > [PnP AP Location]** ウィンドウでは、次のようになります。

- **[Configure AP Location]** チェックボックスがオンの場合、Cisco DNA Center は PnP オンボーディング中にこのサイトを AP ロケーションとして割り当てます。
- **[Configure AP Location]** チェックボックスがオフの場合、Cisco DNA Center は PnP オンボーディング中にこのサイトを AP ロケーションとして設定しません。**[Configure Access Points]** ワークフローを使用して AP の場所を設定できます。

詳細については、『[Cisco DNA Center Administrator Guide](#)』の「Configure AP Location for PnP Onboarding」を参照してください。

c) [Next] をクリックします。

ステップ 6 [Assign Configuration] ウィンドウで、次の手順を実行します。

- [Configuration] 列で、設定するデバイスの [Assign] をクリックします。
- デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次のステップに進みます。それ以外の場合は、次の設定のいずれかを変更または構成します。

- **[Device Name]** : 必要に応じてデバイスのホスト名を変更します。
- **[Image]** : このドロップダウンリストで、デバイスに適用するゴールデンソフトウェアイメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。
- **[Template]** : このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

(注) デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択してから先に進む必要があります。

- **Catalyst ワイヤレス LAN コントローラの設定** : ワイヤレス LAN コントローラの場合、次のフィールドに値を入力します。[Wireless Management IP]、[Subnet Mask]、[Gateway]、[IP Interface Name]、また任意で [VLAN ID]。

IPv6 アドレスを持つ Cisco DNA Center コントローラを使用している場合は、最初の 3 つのフィールドに IPv6 値を入力する必要があります。IPv4 アドレスを持つコントローラを使用している場合は、それらのフィールドに IPv4 値を入力する必要があります。

- AP デバイスの場合、[Radio Frequency Profile] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。
- Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
- ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサーデバイスプロファイル（バックホール）を選択します。
 - (注) リリース 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサー デバイス プロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。
- 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

- c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。
- [Clear Device Certificates] : このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
 - [Clear Images] : このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
 - [Clear Templates] : このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
 - [Clear License Levels] : このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン **...** の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。
- ワイヤレス コントローラ デバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。
- e) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] をクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。
- f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 7 [テンプレートのプロビジョニング (Provision Templates)] ウィンドウで、[デバイス (Devices)] エリアからテンプレートを選択し、ドメインフィールドにドメイン名を入力して、[次へ (Next)] をクリックします。

ステップ 8 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューを確認できます。

ステップ 9 設定プレビューが成功したかどうかを確認するには、各デバイスの [Device Configuration] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [Actions] リンクをクリックして、実行する必要があるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[割り当ての設定 (Assign Configuration)] 手順に戻って設定を変更したり、[設計 (Design)] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。デバイスを管理しているワイヤレスコントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 10 [Device Configuration] 列で、[Preview Configuration] をクリックして設定を確認します。

ステップ 11 [要求 (Claim)] をクリックします。

ステップ 12 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

(注) 選択したサイトに競合する操作がある場合、現在の設定を続行するには、既存、スケジュール済み、またはレビュー保留の操作が完了するまで待つか、この操作を破棄する必要があります。

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、『[Cisco DNA Center ユーザガイド](#)』の「Complete the Provisioning Process」[英語] を参照してください。

センサーを使用したネットワーク正常性のモニターとトラブルシューティング

すべてのワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング

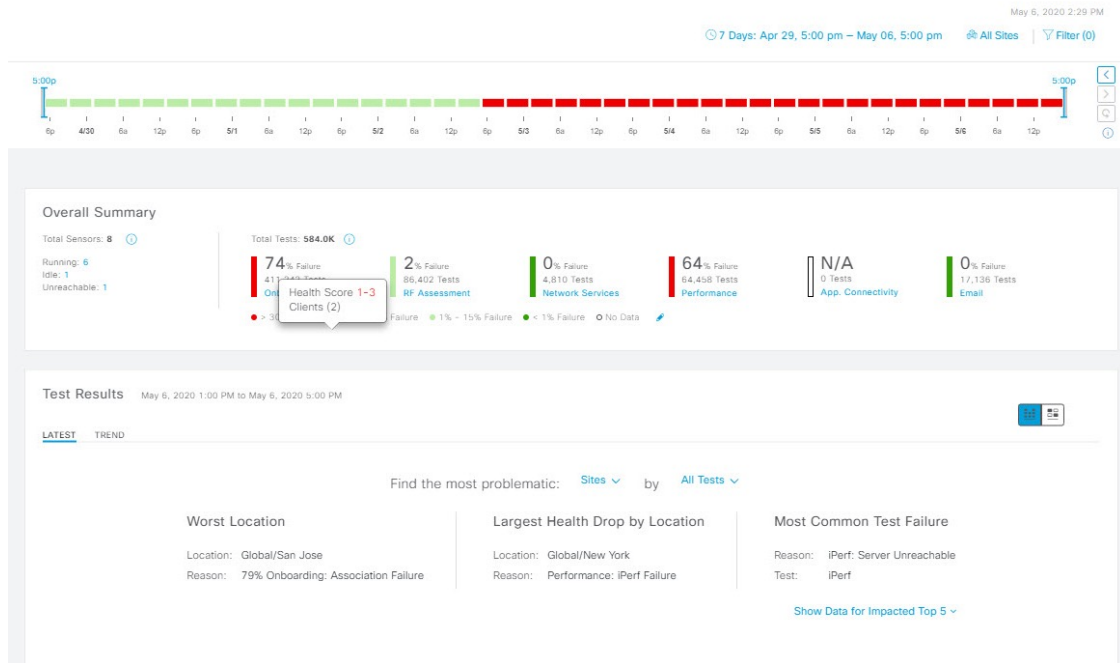
すべてのワイヤレスセンサーから受信したデータに基づくネットワーク正常性のグローバルビューを取得するには、次の手順を実行します。

始める前に


センサー主導テストが追加され、スケジュール済みであることを確認してください。[テンプレートを使用したセンサー主導テストの作成と実行 \(26 ページ\)](#) を参照してください。


ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します : **[Assurance] > [Dashboards] > [Wireless Sensors]** の順に選択します。

図 1: **[Wireless Sensors]** ダッシュボード




ステップ 2 次の機能には、**[Wireless Sensors]** ダッシュボードの上部メニューバーを使用します。

タイムラインエリア	
アイテム	説明
 時間範囲の設定	ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 <ol style="list-style-type: none"> ドロップダウンメニューで範囲の長さ ([3 Hours]、[24 Hours]、または[7 days]) を選択します。 [Start Date] と時刻、[End Date] と時刻を指定します。 [Apply] をクリックします。

タイムラインエリア	
アイテム	説明
 <p>階層ロケーションの設定</p>	<p>ダッシュボードに表示するデータをネットワークのロケーションから選択できます。ダッシュボードにセンサーデータを表示するには、ネットワーク内のサイト、ビルディング、またはフロアのチェックボックスをオンにします。</p> <p>(注) ダッシュボードにデータを表示しないように、すべてのロケーションを除外することはできません。すべてのロケーションのチェックボックスをオフにすると、すべてのロケーションのデータがダッシュボードに表示されます。</p>
[Filter] アイコン	<p>SSID および無線周波数帯域に基づいて、ダッシュボードに表示するデータを選択できます。</p> <p>フィルタを追加するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [Filter] をクリックします。 ドロップダウンメニューから [SSID] タブをクリックし、該当する SSID のチェックボックスをオンにします。 ドロップダウンメニューから、[Band] タブをクリックし、[2.4 GHz] または [5 GHz] のオプションボタンを選択します。 [Apply] をクリックします。 <p>選択したすべてのフィルタを削除するには、次の手順を実行します。</p> <ol style="list-style-type: none"> [Filter] アイコンをクリックします。 [Clear Filters] をクリックします。

ステップ 3 タイムラインを使用して、時間範囲内の特定の時刻に全体テストが失敗した割合を表示します。

時間範囲は、タイムラインの上にある  の設定で決まります。

タイムラインのブロックは、時間範囲内の特定の時間枠を表します。各ブロックの時間枠は、タイムラインに設定された時間範囲によって決まります。



- 時間範囲が [3 Hours] の場合、各ブロックは 15 分を表します。
- 時間範囲が [24 Hours] の場合、各ブロックは 30 分を表します。
- 時間範囲が [7 Days] の場合、各ブロックは 4 時間を表します。

ブロックは、テストが失敗した割合の重大度を示すために色分けされています。



ブロックの上にマウスポインタを合わせると、各テストカテゴリごとにテスト失敗率の内訳が表示されません。


ステップ 4 次の機能には、[Overall Summary] ダッシュレットを使用します。

[Overall Health Summary] ダッシュレット	
アイテム	説明
[Total Sensors] エリア	<p>ネットワーク内のすべてのセンサーとそのステータスの全体像が表示されます。センサーのステータスタイプは、次のとおりです。</p> <ul style="list-style-type: none"> • [Idle] : センサーはオンボードされており、スケジュールされたテストはありません。 • [Running] : センサーはオンボードされており、テストスイートまたはテストテンプレートに含まれています。 • [Unreachable] : センサーからハートビートが受信されませんでした。 <p>ステータスタイプの横にあるハイパーリンク番号をクリックすると、スライドインペインが開き。そのステータスのセンサーが表示されます。</p> <p>スライドインペインで[Name]カラムの下にあるセンサー名をクリックすると、そのセンサーの360度ビューが表示されます。「ワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング (14 ページ)」を参照してください。</p>

[Overall Health Summary] ダッシュレット	
アイテム	説明
全体テスト	<p>すべてのセンサーで実行されたテストの合計数と、次のテストカテゴリに基づくテスト結果の内訳が表示されます。</p> <p>[Onboarding] RF アセスメント ネットワーク サービス パフォーマンス App. 接続性 電子メール</p> <p>テストカテゴリをクリックすると、そのテスト結果に関する追加の詳細情報が表示されるスライドインペインを開くことができます。</p> <p>スライドインペインで、左側のテストタイプのタブをクリックすると、そのテストタイプのデータが記載されたスライドインペインが表示されます。スライドインペインには、次の情報が表示されます。</p> <ul style="list-style-type: none"> • テスト結果、将来のトレンド、およびテストで使用された AP のリストが表示されたチャート。 <p>(注) テストカテゴリが RF アセスメント の場合、チャートには、テスト結果ではなく、KPI データレートと SNR が表示されます。</p> <ul style="list-style-type: none"> • データタイプのカテゴリ： 上位のエラー理由（該当する場合）、上位の AP、上位のロケーション、上位の帯域、および 上位の SSID（該当する場合）。 • テストを実行したセンサーの詳細データが格納されたテーブル。 <p>データタイプカテゴリからデータセグメントをクリックすると、テーブルに表示するデータをフィルタリングできます。</p>
 しきい値の編集	<p>テスト失敗率の重大度を示す色分けされた範囲のしきい値は、カスタマイズできます。</p> <p>● > 30% Failure ● 15% - 30% Failure ● 1% - 15% Failure ● < 1% Failure</p> <p>しきい値をカスタマイズするには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. 編集アイコン（）をクリックします。 2. [Edit Threshold] メニューで、色分けされた各範囲のフィールドにパーセンテージ値を入力します。 3. [Apply] をクリックします。

ステップ 5 [Test Results] ダッシュレットを使用して、センサーテストが最も失敗したネットワーク内のロケーションを表示します。

[Test Results] ダッシュレット	
アイテム	説明
[Latest] タブと [Trend] タブ	<p>これらのタブでは、ダッシュレットに表示するデータの範囲を定義します。</p> <ul style="list-style-type: none"> • [Latest] : ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。 • [Trend] : 過去 24 時間のデータが表示されます。
 [Heatmap View] と [Card View] トグル	<p>このトグルボタンで、ダッシュレットのビューを [Heatmap View] と [Card View] で切り替えることができます。</p> <p>デフォルトでは、[Heatmap View] が表示されます。</p>
 [Heatmap View]	<p>次の統計カテゴリの上位 5 ランキングがダッシュレットの上部に表示されます。</p> <ul style="list-style-type: none"> • [Worst Location, Buildings, Floors] または [Sensors] : テスト失敗率が最も高かったサイト、ビルディング、フロア、またはセンサー。 • [Largest Health Drop by Location, Buildings, Floors] または [Sensors] : 正常性の低下が最も急激なサイト、ビルディング、フロア、センサー。 • [Most Common Test Failure] : テスト失敗率が最も高かったテストタイプ。 <p>各統計情報カテゴリの上位スポットのみが表示されます。[Show Data for Impact Top 5] をクリックすると、完全なランキングが表示されます。</p> <p>ランキングの下には、センサーテストエラーの結果がヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。</p> <ul style="list-style-type: none"> • ランキングやヒートマップに表示するデータをソートするには、[Find the most problematic] エリアのドロップダウンリストを使用します。最初のドロップダウンリストでは、ロケーションまたはセンサー別にデータをソートできます。2番目のドロップリストでは、テストタイプ別にデータをソートできます。 • 特定のロケーションまたはセンサーのヒートマップをフィルタリングするには、検索フィールドを使用します。 • ブロックの上にカーソルを合わせると、テスト失敗の正確なパーセンテージ値が表示されます。 • 色分けされたブロックをクリックすると、スライドインペインが開き、交差する部分のテスト結果に関する詳細が表示されます。

[Test Results] ダッシュレット	
アイテム	説明
 [Card View]	<p>カード形式でデータが表示され、高レベルのモニタリングと比較が可能です。</p> <p>データをソートするには、[Find the most problematic] エリアのドロップダウンリストを使用します。</p>

ワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング

特定のワイヤレスセンサーの360度ビューを表示するには、次の手順を実行します。センサーのテスト結果、パフォーマンスの傾向、およびネイバー AP を表示できます。また、センサーのイベントログの表示や、ダウンロードもできます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance] > [Dashboards] > [Wireless Sensors]** の順に選択します。

[Sensor Dashboard] が表示されます。

ステップ 2 [Sensors Dashboard] から、次のいずれかを実行します。

- [Overall Summary] ダッシュレットで、[Running]、[Idle]、[Unreachable] エリアのいずれかでハイパーリンク番号をクリックします。

次に、[Sensor Status] スライドインペインで、センサーのハイパーリンク名をクリックします。


- [Overall Summary] ダッシュレットで、ハイパーリンクされたテストカテゴリをクリックします。

スライドインペインで、テーブルからセンサーのハイパーリンク名をクリックします。

- [Test Results] ダッシュレットで、ヒートマップから色分けされたボックスをクリックします。

スライドインペインで、テーブルからセンサーのハイパーリンク名をクリックします。

センサーの 360 度ビューが表示されます。

ステップ 3 右上隅にある  [Time Range] の設定をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

- a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。
- b) 開始日付と時刻、終了日付と時刻を指定します。
- c) [Apply] をクリックします。

ステップ 4 センサーの基本情報（センサーのシリアル番号、現在の状態、稼働時間、バックホールタイプ、IP アドレスなど）を表示するには、タイムラインの上にあるヘッダーを使用します。また、センサーのイベントログの表示やダウンロードも可能です。


イベントログの表示やダウンロードには、次の手順を実行します。

- a) ヘッダーの最後にある [View Logs] をクリックします。
[Event Logs] スライドインペインが現れ、イベントログが表示されます。
- b) イベントログの保存先となるサポートバンドルファイルを生成するには、[Event Logs] スライドインペインで、[Request Support Bundle] をクリックします。

注目 サポートバンドル要求がダウンロードできるようになるまでに、約 3 ～ 5 分かかります。

- c) [Download Support Bundle] をクリックして、サポートバンドルのダウンロードプロンプトを開きます。

ステップ 5 タイムラインを使用して、指定した時間範囲内の特定の時刻に全体テストが失敗した割合を表示します。タイムラインには、次の機能があります。

- タイムラインの上にある [Time Range]  で時間範囲を設定します。
- タイムラインのブロックによって示される特定の時間枠で、全体テストが失敗した割合を表示します。ブロックの上にマウスカーソルを合わせると、各テストカテゴリごとにテスト失敗率の内訳が表示されます。

ステップ 6 折りたたみ可能なカテゴリを使用して、テスト結果、パフォーマンス傾向、およびネイバー AP に関する情報を表示します。

テスト結果カテゴリ
<p>センサーテスト失敗の結果は、テスト対象の AP ごとにヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。</p> <ul style="list-style-type: none"> • テストタイプ別にデータをソートするには、[Test Type] ドロップダウンリストを使用します。 • 特定の AP のヒートマップをフィルタ処理するには、検索フィールドを使用します。 • ブロックの上にカーソルを合わせると、テスト失敗の正確なパーセンテージ値が表示されます。 • [Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。 <ul style="list-style-type: none"> • [Latest] : ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。 • [Trend] : 過去 24 時間のデータが表示されます。

センサーパフォーマンスのトレンドカテゴリ

テストタイプに基づいて、センサーのパフォーマンスデータを折れ線グラフまたはチャートで表示します。時間ベースのテストタイプの場合、比較ビューを使用すると、現行センサー、最高パフォーマンスのセンサー、および最悪パフォーマンスのセンサーのパフォーマンスを表示できます。

- 特定のテストタイプのデータを表示するには、[Test Type] ドロップダウンリストを使用します。
- 時間ベースのテストタイプの場合は、[+ Add Custom Location] をクリックすると、メニューを使用して、特定のロケーションのセンサーパフォーマンスデータを追加できます。サイト、ビルディング、またはフロアのセンサーパフォーマンスを選択できます。

ネイバー AP カテゴリ

センサーのネイバー AP とその RSSI が、リストビューとマップビューで表示されます。

周波数帯域に基づいて AP をフィルタ処理するには、[Band] エリアのオプションボタンを使用します。

(注) センサーは、30 分ごとにネイバー AP をスキャンします。

センサーの管理とバックホールの設定

ネットワーク内のセンサーの管理

ネットワーク内のオンボード済みセンサーを表示するには、次の手順を実行します。SSH とステータス LED を有効にして、これらのセンサーの名前を変更できます。

始める前に

センサーがサイトに割り当てられていることを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Assurance] > [Settings] > [Sensors] の順に選択します。

[Sensor List] ウィンドウが表示されます。

図 2: [Sensor List] ウィンドウ

Sensor	Status	SSH	LED	Location	SCEP Profile	Last Seen	Backhaul Type
wired4540	Running	On	On	.../New York/ny-bld-1/ny-floor-1	MS	May 6, 2020 2:48 pm	Wired
AP70F3.5A88.4DB0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	ISE51	May 6, 2020 2:48 pm	Wireless
AP70F3.5A80.6300	Running	Off	On	.../New York/ny-bld-1/ny-floor-1	MS	May 6, 2020 2:48 pm	Wireless
AP70F3.5A80.2088	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	ISE52	May 6, 2020 2:48 pm	Wired
AP70F3.5A7E.3BC0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	MS	May 6, 2020 2:48 pm	Wireless
AP70F3.5A7E.26C0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	MS	May 6, 2020 2:48 pm	Wired
60CBwireless	Idle	On	On	...ngalore/big-bld-1/big-floor-1	None	May 6, 2020 2:48 pm	Wireless
5FE0wireless	Idle	On	On	...ngalore/big-bld-1/big-floor-1	ISE52	May 6, 2020 2:48 pm	Wireless

ステップ 2 左側のペインで、表示するネットワーク階層を指定します。

ステップ 3 基準に適合するセンサーを表示するには、テーブルの上にあるカテゴリをクリックします。カテゴリは次のとおりです。

- [Total] : 選択したネットワーク階層内のすべてのセンサー。
- [Running] : 現在テストを実行しているセンサーが表示されます。
- [Idle] : テストが割り当てられていないセンサーが表示されます。
- [Unreachable] : オンボードされているが、Cisco DNA Center に応答していないセンサーが表示されません。

ステップ 4 テーブルに表示するデータをカスタマイズできます。

- ☰ をクリックします。
- メニューからテーブルに表示するデータのチェックボックスをオンにします。
- [Apply] をクリックします。

ステップ 5 センサーの SSH 設定を構成するには、次の手順を実行します。

- センサーのチェックボックスをオンにします。
- [Actions] ドロップダウンリストにカーソルを合わせて、[Edit SSH] を選択します。
[Edit SSH] スライドインペインが表示されます。
- [EDIT SSH] スライドインペインで、[SSH] トグルをクリックして SSH を有効にします。
- [Username] および [Password] フィールドに、使用する SSH ログイン情報を入力します。
- [Save] をクリックします。

ステップ 6 センサーのステータス LED を変更するには、次の手順を実行します。

- センサーのチェックボックスをオンにします。

- b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit LED] を選択します。
[Edit SSH] スライドインペインが表示されます。
- c) [Edit LED] スライドインペインで、[LED] トグルをクリックして、ステータス LED を有効または無効にします。

ステップ7 [Save] をクリックします。

ステップ8 センサーの名前を変更するには、次の手順を実行します。

- a) センサーのチェックボックスをオンにします。
- b) [Actions] ドロップダウンリストから、[Edit Sensor Name (s)] を選択します。
[Edit Sensor Name (s)] スライドインペインが表示されます。
- c) [Edit Sensor Name (s)] スライドインペインで、[Name] フィールドに名前を入力します。
- d) [Save] をクリックします。

ステップ9 SCEP プロファイルを使用してセンサーを登録するには、次の手順を実行します。

- a) センサーのチェックボックスをオンにします。
- b) [Actions] ドロップダウンリストから、[Enroll using SCEP] を選択します。
[Enroll using SCEP] スライドインペインが表示されます。
- c) [Select SCEP Profile] ドロップダウンリストから SCEP プロファイルを選択します。
詳細については、「[SCEP プロファイルの管理](#)」を参照してください。
- d) [Username] と [Password] を選択し、必要な詳細情報を入力します。ユーザー名として [Custom] オプションを選択する場合は、[No Password] を選択します。
- e) [Save] をクリックします。
- f) ステータスを確認するには、[Sensor List] ウィンドウの [SCEP Profile] 列を確認します。緑のチェックマーク (✓) は成功、赤の X アイコンは失敗を示します。✓ または X アイコンにカーソルを合わせると、詳しい情報が表示されます。

バックホールの設定の管理

ワイヤレスセンサのバックホール設定を表示、作成、管理するには、次の手順を実行します。ワイヤレスセンサーには、Cisco DNA Center と通信するためのバックホール SSID が必要です。

永続的なワイヤレスバックホール接続の詳細については、[センサデバイスでの永続的なワイヤレスバックホール接続 \(20 ページ\)](#) を参照してください。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：[Assurance]>[Settings]>[Sensors] の順に選択します。

[Sensor List] ウィンドウが表示されます。

ステップ2 [Settings] タブにカーソルを合わせ、[Backhaul Settings] を選択します。

ステップ3 バックホール SSID を追加および管理するには、次の手順を実行します。

a) [Add Backhaul] をクリックします。

[Create Sensor Backhaul SSID Assignment] ウィンドウが表示され、[Wired Backhaul] と [Wireless Backhaul] の2つの領域が表示されます。

b) [Settings name] フィールドでバックホール SSID の名前を入力します。

c) [Wired Backhaul] 領域で、次を設定します。

- [Level of Security] : 選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
 - [802.1x EAP] : Extensible Authentication Protocol (EAP) を有線 LAN で渡すために使用される規格。
 - [Open] : セキュリティまたは認証は使用されません。
- [EAP Method] : [802.1x EAP] を選択した場合は、ドロップダウンリストからユーザ認証に次のいずれかの EAP 方式を選択する必要があります。
 - [EAP-FAST] : 指定されたフィールドにユーザ名とパスワードを入力します。
 - [PEAP-MSCHAPv2] : 指定されたフィールドにユーザ名とパスワードを入力します。
 - [EAP-TLS] : [Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。
[Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。
 - [PEAP-TLS] : [Enroll Using Certificate Bundle] または [Enroll using SCEP] を選択します。
[Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name (SSID)] 領域で、ワイヤレスネットワーク (SSID) を選択し、次を設定します。

- [Level of Security] : 選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。
 - [WPA2 Enterprise] : 拡張可能認証プロトコル (EAP) (802.1x) を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワークユーザを認証および承認します。
 - [WPA2-Personal] : パスフレーズまたは事前共有キー (PSK) を使用して、良好なセキュリティを実現します。ワイヤレスネットワークにアクセスするパスキーがあれば誰でも使用できます。
[WPA2 Personal] を選択した場合は、[Passphrase] テキストボックスにパスフレーズを入力します。

- [PSK Format] : 使用可能な事前共有キーの形式は次のとおりです。
 - [ASCII] : ASCII PSK パスフレーズをサポートします。
 - [HEX] : 64 文字の HEX キー PSK パスワードをサポートします。
- [Open] : セキュリティまたは認証は使用されません。

e) [Save] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

- a) バックホール設定のチェックボックスをオンにします。
- b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

- a) バックホール設定のチェックボックスをオンにします。
- b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

センサデバイスでの永続的なワイヤレスバックホール接続

Cisco DNA Center はセンサーデバイスでの永続的なワイヤレスバックホール接続をサポートしており、ワイヤレステストのアクティビティに関係なく、ワイヤレス接続は「常時オン」になっています。

- ワイヤレスセンサ専用のバックホール接続では、バックホールとワイヤレス用に次の2つの MAC アドレスが使用されます。
 - ベース無線 + 0x10 (バックホール SSID)
 - ベース無線 + 0x11 (テスト SSID)

有線センサーではベース無線 + 0x10 (テスト SSID) MAC アドレスがテスト用に使用されます。

- センサーではデュアル同時無線動作が使用されます。1 つはバックホール接続用、もう 1 つはワイヤレステスト用です。
- スキャンを実行している間、および別の帯域をテストするためにインターフェイスを切り換えている間は、バックホール接続が中断します。
- バックホール接続の中断の頻度は、テスト設定に応じて異なります。
- バックホールとテスト SSID の帯域が同じである場合、バックホール接続は永続になりません。

SCEP プロファイルの管理

この手順では、ワイヤレスセンサーの登録に使用する Simple Certificate Enrollment Protocol (SCEP) プロファイルを表示、作成、管理する方法を示します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Assurance] > [Settings] > [Sensors] の順に選択します。

ステップ 2 [Setting] > [SCEP Profiles] の順にクリックします。

ステップ 3 SCEP プロファイルを追加および管理するには、次の手順を実行します。

a) [Add SCEP Profiles] をクリックします。

[Create SCEP Profile] ウィンドウが表示されます。

b) [Create SCEP Profile] ウィンドウで、次の詳細を入力します。

- [SCEP Profile Name] : SCEP プロファイルの名前を入力します。
- [URL Base] : 有効なサーバーを入力します。

(注) **ISE** の場合は、次のように入力します。

`http://ISE_IP_or_FQDN_Name:9090/auth/caservice/pkiclient.exe`

Microsoft CA の場合は、次のように入力します。

`http://Microsoft_SCEP_IP_or_FQDN_Name/CertSrv/mscep/mscep.dll`

- [Common Name] : 有効な名前を入力します。
- [State]
- [Country Code]
- [Locality]
- [Organization]
- [Organization Unit]
- [Email]
- [Sever certificate fingerprint]

c) [Save] をクリックします。

ステップ 4 既存の SCEP プロファイルを編集するには、次の手順を実行します。

- a) SCEP プロファイルの横にあるチェックボックスをオンにします。
- b) [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 SCEP プロファイルを削除するには、次の手順を実行します。

- a) SCEP プロファイルの横にあるチェックボックスをオンにします。

- b) [Actions] ドロップダウン リストから、[Delete] を選択します。

センサー主導テスト

センサー主導テストの作成方法 アシュアランス

アシュアランスでセンサー主導テストを作成する方法は2通りあります。次の方法の中から1つを選択してください。

メソッド	説明
レガシー	レガシー方式（テストスイートとも呼ばれる）を使用してセンサー主導テストを作成できます。 レガシーの方法を使用したセンサー主導テストの作成と実行（22 ページ） を参照してください。
テンプレート	テンプレートを使用してセンサー主導テストを作成できます。 このメソッドにより、再利用可能なセンサー主導テストのテンプレートを作成し、ネットワーク内の複数のロケーションに迅速に展開できます。 テンプレートを使用したセンサー主導テストの作成と実行（26 ページ） を参照してください。

レガシーの方法を使用したセンサー主導テストの作成と実行

レガシー方式（テストスイートとも呼ばれる）を使用してセンサー主導テストを作成および実行するには、次の手順を実行します。



警告 レガシーテスト方式は、近い将来に廃止される予定です。

始める前に

Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[Inventory] で表示されるようにしてください。[ワイヤレス Cisco Aironet 1800s アクティブ センサーのプロビジョニング（2 ページ）](#) を参照してください。

- ステップ 1** 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]>[Settings]>[Sensors]** の順に選択します。

ステップ 2 [Legacy Tests] タブをクリックします。

[Legacy Tests] ウィンドウが表示されます。

ステップ 3 新しいセンサーテストを追加するには、右上隅にある [+ Add Test] をクリックします。

[Add Test] ウィンドウが表示されます。

ステップ 4 テストをスケジュールするには、次の設定を行います。

設定	説明
[Test Name] フィールド	<p>テストスイート名を入力します。</p> <p>(注) 文字、数字、アンダースコア、ハイフン、ピリオドのみ使用できます。</p>
[Location] ドロップダウン リスト	<p>次の手順を実行します。</p> <ol style="list-style-type: none"> ドロップダウンリストからセンサーのロケーションを選択します。 テストに追加する無線センサーの SSID のチェックボックスをオンにします。 必要に応じて、ログイン情報を設定します。 <p>Web 認証対応 SSID に適用</p> <p>レイヤ 3 セキュリティでは、SSID で Web 認証が有効になっている場合、次の機能を使用できます。</p> <ul style="list-style-type: none"> ユーザー認証による Web 認証の場合は、必要なログイン情報を入力します。 パススルー方式による Web 認証の場合は、メールアドレスの入力を選択できます。 <p>(注)</p> <ul style="list-style-type: none"> センサーのテストでは、内部認証のみがサポートされています。 Web 認証は、シスコ ワイヤレス コントローラおよびソフトウェア リリース 8.7 を搭載した Cisco Aironet 1800s アクティブセンサーでサポートされます。 <p>WPA2 Enterprise 対応 SSID に適用</p> <p>サポートされるメソッドは、EAP-FAST、PEAP MSCHAPv2、および EAP-TLS です。</p> <p>EAP-TLS を選択した場合は、証明書とそのパスワードが必要です。証明書をアップロードするには、[Certificate] ドロップダウンメニューをクリックしてから、[Add New Certificate Bundle] をクリックします。</p>

設定	説明
[Interval] ドロップダウンメニュー	<p>センサーテストのスケジュールを指定します。次のオプションがあります。</p> <ul style="list-style-type: none"> • [Daily] : センサーテストは継続的に反復実行されます。デフォルトの間隔は 1 時間です。 • [Once] : センサーテストは、指定された日時に 1 回実行されます。

ステップ 5 [Next] をクリックして、[Select Tests] ステップに進みます。

ステップ 6 [Select Tests] ステップでは、次の設定を行います。

- a) 実行対象の [Network Tests] のチェックボックスをオンにして、テストに必要な情報を入力します。

ネットワークのテスト	
[Test Type]	説明
オンボーディングのテスト	<p>クライアントのオンボーディングテスト（通常、関連付け、AAA、および DHCP を含む）を実行します。</p> <p>(注)</p> <ul style="list-style-type: none"> • このオプションはデフォルトで選択されていて、選択解除できません。 • オンボーディングのテストは、Cisco Aironet 1800s アクティブセンサーのソフトウェアリリース 8.8.260.0 以降でサポートされています。
DNS のテスト	ドメイン名の IP アドレスを解決します。
ホストの到達可能性テスト	Internet Control Message Protocol (ICMP) エコー要求を使用して到達可能性を確認します。
RADIUS のテスト	センサーが Dot1x サプリカントとして機能し、ワイヤレスで認証します。Dot1x サプリカントは、Protected Extensible Authentication Protocol (PEAP) と Password Authentication Protocol (PAP) や Microsoft バージョンのチャレンジハンドシェイク認証プロトコル (MS-CHAP) などのプロトコルをサポートしています。

- b) 実行対象の [Performance Tests] のチェックボックスをオンにして、テストに必要な情報を入力します。

パフォーマンステスト	
[Test Type]	説明
速度テスト	ネットワーク診断テスト (NDT) サーバーがある場合は、所定のフィールドに NDT サーバーの IP アドレスを入力します。NDT サーバーがプロキシサーバー経由で到達可能である場合は、所定のフィールドにプロキシサーバーの IP アドレスを入力します。

パフォーマンステスト	
[Test Type]	説明
IPSLA テスト	<p>センサーから AP への UDP ジッター、UDP エコー、パケット損失、および遅延の測定を実行します。</p> <p>IPSLA テストを実行するには、ドロップダウンリストから各 SSID の [Service Level] オプションを選択します。[Platinum] (音声)、[Gold] (ビデオ)、[Silver] (ベストエフォート)、および [Bronze] (バックグラウンド) のオプションがあります。</p>

(注) 速度テストと IPSLA テストは、シスコワイヤレスコントローラおよびソフトウェアリリース 8.8 以降の Cisco Aironet 1800s アクティブセンサーでサポートされます。

c) 実行対象の [Application Tests] のチェックボックスをオンにして、テストに必要な情報を入力します。

電子メールのテスト	
[Test Type]	説明
電子メールのテスト	<p>主要な構成は以下のとおりです。</p> <ul style="list-style-type: none"> • [POP3] : Post Office Protocol3。POP3 サーバーの TCP ポート (110) に接続します。 • [IMAP] : Internet Message Access Protocol。IMAP サーバーの TCP ポート (143) に接続します。 • [Outlook Web Server] : Outlook Web サーバー (OWS) にログインします。
Web のテスト	指定された URL へのアクセスと応答データの確認をテストします。
ファイル転送のテスト	<p>ファイルのアップロードおよびダウンロード動作をテストします。</p> <p>(注) センサーテストの最大ファイルサイズは 5 MB です。</p>

ステップ 7 [Next] をクリックして、[Select Sensors] ステップに進みます。

ステップ 8 [Select Tests] ステップでは、次の設定を行います。

- すべての AP について RSSI しきい値を設定するには、次の操作を実行します。
 1. [Threshold] をクリックして、[RSSI Threshold] スライダを目的の値までドラッグします。
 2. [Number of Target APs] ドロップダウンリストから、センサーでテストする AP 番号を選択します。
 3. [Apply] をクリックします。
- 特定の AP を選択してテストするには、次の手順を実行します。
 1. テストに使用するセンサーのチェックボックスをオンにします。

2. [Target AP #] 列の [V] をクリックして、すべてのセンサーのネイバー AP を表示します。
3. [Target AP] 列で、テストする AP のチェックボックスをオンにします。
(注)
 - 最大 5 つの AP を選択できます。
 - センサーのネイバー AP は 30 分ごとに更新されます。

ステップ 9 [Next] をクリックして、センサーテストを作成します。

新しいテストが追加され、[Test Suites] ウィンドウに表示されます。

テンプレートを使用したセンサー主導テストの作成と実行

テンプレートを使用してセンサー主導テストを作成および実行するには、次の手順を実行します。テンプレートを使用したセンサー主導テストのワークフローは、次の 2 つの部分から構成されます。

1. **テストテンプレートの作成**：テスト対象の SSID、使用するテストタイプ、AP カバレッジなどのテスト構成を設定します。
2. **テストテンプレートの展開**：テストテンプレートの作成後、テスト対象のロケーションを選択し、テストスケジュールを設定します。テストテンプレートを展開すると、実行の準備が整います。

センサー主導テストを複数のロケーションや複数のスケジュールで実行する必要があるユースケースの場合、テンプレートを使用すると便利です。テンプレートを使用すると、コピーを作成して、テストロケーションやスケジュールの各インスタンスに対して展開できます。これにより、各インスタンスに対して同じテストを繰り返し作成する必要がなくなります。

始める前に

- Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[Inventory] で表示されるようにしてください。 [ワイヤレス Cisco Aironet 1800s アクティブ センサーのプロビジョニング \(2 ページ\)](#) を参照してください。
- センサーテストテンプレートを再起動すると、そのテンプレート上のすべてのセンサーで同時にテストの実行が開始されるため、結果のグラフに周期的なパターンが現れることに注意してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Assurance] > [Settings] > [Sensors] の順に選択します。

ステップ 2 [Test Templates] タブをクリックします。

[Test Templates ウィンドウが表示されます。

図 3: [Test Templates] ウィンドウ

Test Name	SSID with Test Types	AP Coverage	Location	Schedule
sjcdot1x	5520-LOCAL-WLAN-1: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous
EAPTLS	ISEEAPTLS: Onboarding, RF Assessment, App.Connectivity, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous
3rd party test	8540-hidden: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous
NYC	SensorSSID: Onboarding, RF Assessment, Net.Service, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/New York/ny-bld-1/ny-floor-1	Periodic
EAPTLS8540	EAPTLS8540: Onboarding, RF Assessment	5GHz: 1, -70dBm	Deploy Test	N/A

ステップ 3 新しいセンサーテストテンプレートを作成するには、[+ Add Sensor Test] をクリックします。センサーテストテンプレートを作成するためのウィザードが表示されます。

ステップ 4 [Set up Sensor Test] ステップでは、次の設定を行います。

- [Test Template Name] : テストの名前を入力します。
(注) 文字、数字、アンダースコア、ハイフン、ピリオドのみ使用できます。
- [Ssid Selection] : センサーテストを行う SSID のチェックボックスをオンにします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Enter SSID Credentials] ステップでは、選択した SSID のログイン情報を入力します。

- セキュリティがオープンな SSID の場合は、次を選択します。
 - [Open] : パススルー方式の Web 認証を使用した SSID の場合は、電子メールアドレスを入力します。
 - [ISE Guest Portal] : ISE ゲストポータルのラベルを選択します。
 - [Clearpass Guest Portal] : Clearpass ゲストポータルのラベルを選択し、[Apply] をクリックします。
- **WPA2 パーソナルセキュリティ**を使用した SSID の場合は、パスワードを入力します。
- **WPA2 エンタープライズセキュリティ**を使用した SSID の場合は、EAP メソッド、ユーザー名、およびパスワードを入力します。

ステップ 7 [Add Proxy Settings] チェックボックスをオンにして、プロキシ設定を有効にします。

ステップ 8 次のプロキシ設定を指定します。

- [Proxy Server]
- [Proxy Port]
- [Proxy UserName]
- [Proxy Password]

ステップ 9 [Next] をクリックします。

ステップ 10 [Define Sensor Test Category Details] ステップでは、対象にするテストタイプのチェックボックスをオンにします。

a) テストカテゴリが**オンボーディング**の場合、テストタイプは[Association]、[Authentication]、[DHCP]です。

(注) これらのテストタイプはすべてデフォルトで選択されており、テストテンプレートから除外できません。

b) テストカテゴリが**RF アセスメント**の場合、テストタイプは[Data Rate]、[SNR]です。

(注) これらのテストタイプはすべてデフォルトで選択されており、テストテンプレートから除外できません。

c) テストカテゴリが**ネットワークサービステスト**の場合は、次のテストタイプから選択します。

- [DNS] : ドメイン名の IP アドレスを解決します。
- [RADIUS] : センサーが Dot1x サブリカントとして機能し、ワイヤレスで認証します。

d) テストカテゴリが**パフォーマンステスト**の場合は、次のテストタイプから選択します。

- [Internet (NDT)] : ネットワーク診断ツール (NDT) を使用して速度テストを実行します。

ネットワーク診断テスト (NDT) サーバーがある場合は、所定のフィールドに NDT サーバーの IP アドレスを入力します。NDT サーバーがプロキシサーバー経由で到達可能である場合は、所定のフィールドにプロキシサーバーの IP アドレスを入力します。

- [iPerf3] : iPerf3 テストは、ネットワークパフォーマンスの測定に使用されるツールです。この機能を使用すると、一定量のトラフィックでネットワークの速度テストを実行して、トラフィックが通過できるかどうかをテストできます。

iPerf3 テストを実行するには、[iPerf3] チェックボックスをオンにしてから、表示されるフィールドに iPerf3 サーバーの IP アドレス、UDP 帯域幅、およびポートの詳細を入力します。

iPerf3 の制限事項

- iPerf3 サーバーは最大 5 つまで追加できます。
- 各 iPerf3 サーバーについて、テンプレートごとに最大 5 つのポートを使用するように設定できます。iPerf3 テストを実行するポートはセンサーでランダムに選択されます。

- 特定の iPerf3 サーバーにおいて、2つのセンサーを同じポートに同時に接続することはできません。
- 「iPerf : サーバーがビジー状態 (iPerf: Server Busy) 」 エラーメッセージは、iPerf3 テストを実行しているセンサーの数に対応する十分な iPerf3 インスタンスがないことを示します。
この問題を解決するには、次のいずれかを実行します。
 - iPerf3 サーバーインスタンスを追加します。これを行うには、既存のサーバーで iPerf3 テストをサポートするポートを拡張します。
 - iPerf3 テストを実行するように設定されているセンサーの数を減らします。これを行うには、iPerf3 テスト用に別個のテンプレートを作成します。

- [IP SLA] : センサーから AP への UDP ジッター、UDP エコー、パケット損失、および遅延の測定を実行します。

IPSLA テストを実行するには、ドロップダウンリストから各 SSID の [Service Level] オプションを選択します。[Platinum] (音声)、[Gold] (ビデオ)、[Silver] (ベストエフォート)、および [Bronze] (バックグラウンド) のオプションがあります。

- e) テストカテゴリが**アプリケーションテスト**の場合、次のテストタイプから選択します。

- [Host Reachability] : (ICMP) エコー要求を使用した到達可能性をテストします。
- [Web] : 指定した URL へのアクセスと応答データの検証をテストします。
- [FTP] : ファイルのアップロードおよびダウンロード動作をテストします。

(注) センサーテストの最大ファイルサイズは 5 MB です。

- f) テストカテゴリが**電子メール**の場合、次のテストタイプから選択します。

- [POP3] : Post Office Protocol3。POP3 サーバーの TCP ポート (110) に接続します。
- [IMAP] : Internet Message Access Protocol。IMAP サーバーの TCP ポート (143) に接続します。
- [Outlook Web Access] : Outlook Web サーバーにログインし、アクセスを検証します。

ステップ 11 [Next] をクリックします。

ステップ 12 **AP カバレッジの選択**ステップでは、次を実行します。

- a) [2.4GHz] と [5GHz] チェックボックスでテストする周波数帯域を選択します。
- b) 選択した帯域の [Number of Target APs] ドロップダウンリストで、センサーでテストする AP 番号を選択します。

(注) 最大 5 つの AP を選択できます。

- c) 選択した帯域の [RSSI Range] スライダーで、該当する RSSI までをドラッグします。

ステップ 13 [Next] をクリックします。

- ステップ 14** [Summary] ステップでは、テンプレートの設定を確認します。
[SSIDs] や [AP Coverage] ステップで、[Edit] をクリックすると、設定をやり直すことができます。
- ステップ 15** [Create Test] をクリックしてテンプレートを作成します。
テストテンプレートが作成されると、確認のためのダイアログボックスが表示されます。
- ステップ 16** [Done! **Sensor Test Created**] 確認ウィンドウで [Deploy Test to Locations] をクリックして、テストテンプレートを実行するロケーションとスケジュールを設定します。
- 重要** テストを展開せずに [Test Templates] ウィンドウに戻る場合は、[Location] 列から [Deploy Test] をクリックしてテスト展開の次の手順に進んでください。
- ステップ 17** [Select Location] ステップでは、左側の階層メニューを使用して、テストテンプレートを展開するサイト、ビルディング、ロケーションのチェックボックスをオンにします。
- ステップ 18** [Next] をクリックします。
- ステップ 19** [Set Schedule] ステップでは、テスト頻度オプションを次から 1 つ選択します。
- [Periodic] : 指定した間隔でテストを実行します。 [Interval] ドロップダウンリストから、間隔を選択します。
 - [Scheduled] : 指定した期間中、指定した曜日にテストを実行します。
 1. [S]、[M]、[T]、[W]、[T]、[F]、[S] の各ボタンをクリックして、テストを実行する曜日を選択します。
 2. 選択した曜日に対して、[From] タイムピッカーからテスト期間の開始時刻と終了時刻を指定します。
 3. [Select Value] ドロップダウンメニューで、該当するテスト期間を選択します。
 4. 選択した曜日に別のテスト期間を追加するには、[+ Add] をクリックして、テスト期間を設定するための新しい行を追加します。
 5. テスト期間を削除するには、ごみ箱アイコンをクリックします。
 - [Continuous] : テストは無期限に実行され、完了後に繰り返されます。
- ステップ 20** [Next] をクリックします。
- ステップ 21** [Summary] ステップで、展開の詳細を確認します。
[Location] や [Schedule] ステップで、[Edit] をクリックすると、設定をやり直すことができます。
- ステップ 22** [Deploy Test] をクリックします。
[Test Template] ウィンドウにテストテンプレートが表示されます。
- ステップ 23** テストテンプレートでテストを実行するには、[Run Now] をクリックします。
-

センサー主導テストの管理

センサー主導テストのテンプレートを管理するには、次の手順に従います。センサー主導テストのテンプレートの複製や削除だけでなく、実行中のテンプレートの展開を解除することもできます。

始める前に

センサー主導テストのテンプレートを作成します。[テンプレートを使用したセンサー主導テストの作成と実行 \(26 ページ\)](#) を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Assurance]**>**[Settings]**>**[Sensors]** の順に選択します。

ステップ 2 **[Test Templates]** タブをクリックします。

[Test Templates] ウィンドウが表示されます。

図 4: **[Test Templates]** ウィンドウ

Test Name	SSID with Test Types	AP Coverage	Location	Schedule
<input type="checkbox"/> sjcdot1x	5520-LOCAL-WLAN-1: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous
<input type="checkbox"/> EAPTLS	ISEEAPTLS: Onboarding, RF Assessment, App Connectivity, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous
<input type="checkbox"/> 3rd party test	8540-hidden: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous
<input type="checkbox"/> NYC	SensorSSID: Onboarding, RF Assessment, Net Service, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/New York/ny-bid-1/ny-floor-1	Periodic
<input type="checkbox"/> EAPTLS8540	EAPTLS8540: Onboarding, RF Assessment	5GHz: 1, -70dBm	Deploy Test	N/A

ステップ 3 テストテンプレートを複製するには、次の手順を実行します。

- 複製するテストテンプレートのチェックボックスをオンにします。
- [Actions]** > **[Duplicate]** の順に選択します。
- [Input the new Test Name]** ダイアログボックスで、テストテンプレートの複製名を入力します。
- [Save]** をクリックします。

[Test Templates] ウィンドウに複製されたテストテンプレートが表示されます。テストを展開するには、**[Location]** ステップから **[Deploy Test]** をクリックします。

ステップ 4 テストテンプレートを削除するには、次の手順を実行します。

- 複製するテストテンプレートのチェックボックスをオンにします。
- [Actions]** > **[Delete]** の順に選択します。

- c) [Warning] ダイアログボックスで、[Yes] をクリックします。
テストテンプレートが削除されます。

ステップ 5 テストテンプレートの展開を解除するには、次の手順を実行します。

- a) 展開を解除する実行中のテストテンプレートのチェックボックスをオンにします。
- b) [Actions] > [Undeploy] の順に選択します。
- c) [Warning] ダイアログボックスで、[Yes] をクリックします。
テストテンプレートの実行が停止されます。

警告 テストテンプレートの展開を解除すると、ロケーションとスケジュールの設定が削除されます。

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。