Cisco DNA アシュアランス リリース 2.2.3 ユーザーガイド

初版：2021 年 8 月 4 日

最終更新：2023 年 7 月 14 日

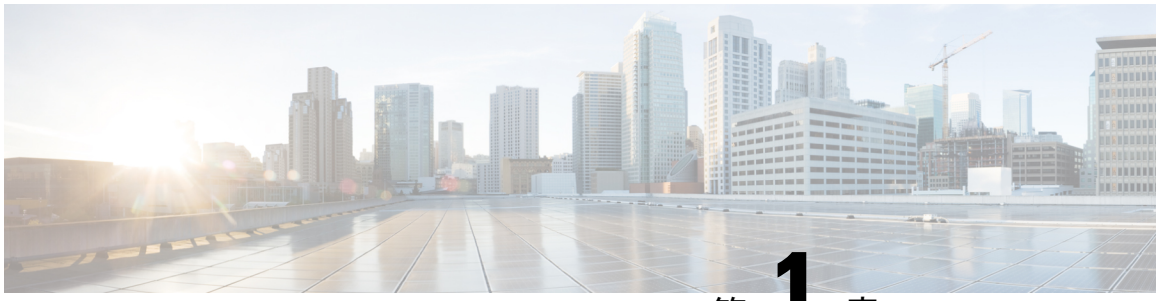
シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2023 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

新機能および変更された機能に関する情報

Cisco DNA Assurance リリース 2.2.3 の最新情報

次の表は、Cisco DNA アシュアランス リリース 2.2.3.6、2.2.3.4、2.2.3.3、および 2.2.3 の新機能と変更された機能をまとめたものです。

表 *1 : Cisco DNA* アシュアランス リリース *2.2.3.6* の新機能および機能変更

機能	説明
Cisco SD-Access：LISP と Pub/Sub セッション	[SD-Access Health] で、ファブリックサイトにおける [LISP] と [Pub/Sub] のセッションの監視がサポートされます。これらの KPI は、ファブリックサイト、SD-Access トランジット、トランジット コントロール プレーン、およびデバイスの正常性の計算に含まれています。 ファブリックサイトの正常性の監視 （201 ページ）、トランジットおよびピアネットワークの正常性の監視 （205 ページ）、およびデバイスの健全性のモニターとトラブルシューティング （102 ページ）を参照してください。

表 *2 : Cisco DNA* アシュアランス リリース *2.2.3.4* の新機能および機能変更

機能	説明
Power over Ethernet（PoE）AP 電力モード供給ダッシュレット	完全に電力が供給されている AP と部分的に電力が供給されている AP の分布を表示できます。この情報を表示するには、メニューアイコン（☰）をクリックして、 をクリックして **[Assurance]** > **[PoE]** を選択します。[PoE] ダッシュボードが開きます。 ネットワーク内の PoE 対応デバイスの監視 （304 ページ）を参照してください。

機能	説明
仮想ネットワーク 360 ウィンドウ	仮想ネットワークの詳細を表示できます。この情報を表示するには、メニューアイコン（≡）をクリックして、をクリックして**[Assurance]**>**[Health]**>**[SD-Access]**を選択します。 仮想ネットワークの正常性の監視 （210 ページ）および仮想ネットワークの正常性スコア （214 ページ）を参照してください。
クライアントダッシュボードのワイヤレスクライアントのトレンドビューの機能強化	クライアントの正常性サマリーでは、ワイヤレスクライアントのトレンドビューが強化されています。放射状棒チャートは、オンボーディングに失敗したクライアントの分布と、オンボーディング失敗の理由を示します。 すべてのクライアント デバイスの健全性のモニターとトラブルシューティング （137 ページ）を参照してください。
Webex クライアント 360	Webex クライアント 360 では、クライアント ミーティング テーブルが次の列で拡張され、各ミーティングの全体的な状態を示します。 • アプリケーション：Webex Control Hub によって報告された正常性スコアと KPI が表示されます。 • ネットワーク：管理対象ネットワークデバイスからエクスポートされたNetFlow 経由で Cisco DNA Center によって報告された正常性スコアと KPI が表示されます。 「クライアントデバイスの健全性のモニターとトラブルシューティング （152 ページ）」を参照してください
Cisco AI Network Analytics — クライアントエクスペリエンスに基づく無線インサイト	Cisco AI Network Analytics は、機械学習アルゴリズムを使用して、潜在的にクライアント エクスペリエンスが低いワイヤレス AP を特定します。AP は長期間にわたって継続的に分析され、最適ではないクライアント エクスペリエンスを提供していると疑われる AP は、根本的な原因と提案される改善点によってグループ化されます。 ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する （320 ページ）を参照してください。

表 *3 : Cisco DNA* アシュアランス リリース *2.2.3.3* の新機能および機能変更

機能	説明
アシュアランス のサイト階層サポート	**[Assurance]** > **[Health]** と **[Assurance]** > **[Issues]** のダッシュボードが拡張され、[Overall]、[Network]、[Clients] などの正常性タブと、[Open]、[Resolved]、[Ignored] などの問題タブのサイト階層フィルタとサイトテーブルが表示されるようになりました。 企業の全体的な健全性のモニターとトラブルシューティング（131 ページ）、ネットワークの健全性のモニターとトラブルシューティング（93 ページ）、すべてのクライアントデバイスの健全性のモニターとトラブルシューティング（137 ページ）、未解決の問題を表示（217 ページ）、解決済みの問題の表示（234 ページ）、および無視された問題の表示（236 ページ）を参照してください。

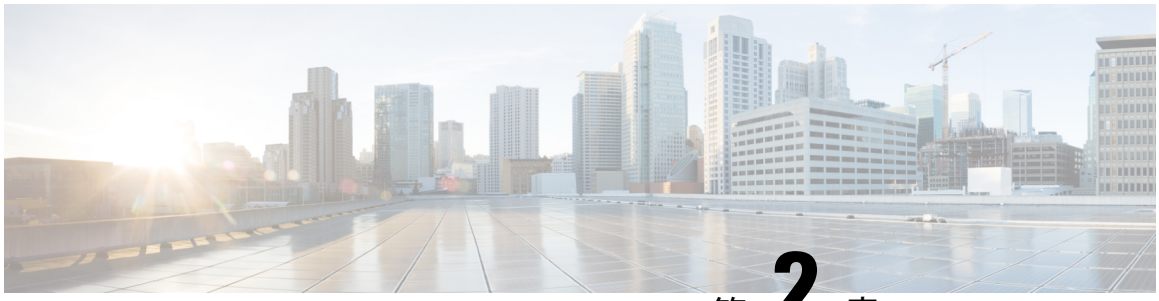
次の表は、Cisco DNA アシュアランス 2.2.3 の新機能と変更された機能をまとめたものです。

表 *4 : Cisco DNA* アシュアランス リリース *2.2.3* の新機能および機能変更

機能	説明
AP 360 のネイバービューと不正ビュー	AP 360 では、[RF] タブの下に [Neighbors and Rogues] セクションが表示されます。このセクションには、[Band]（2 GHz および 5 GHz）、[Type]（すべて、ネイバー、および不正）、[RSSI Range]（0 ～ -100 dBm）などのフィルタが含まれます。選択したフィルタに応じて、AP デバイスと Wi-Fi アナライザのグラフが更新されます。 デバイスの健全性のモニターとトラブルシューティング（102 ページ）を参照してください。
AP 360 KPI	[Device Details] エリアには、次の AP 詳細属性が含まれています。 • 一般情報：電源ステータス • ネットワーク情報：接続されたスイッチ [Connectivity] タブには、次の属性が含まれています。 • イーサネット インターフェイス KPI の接続済みスイッチバナーが追加されました。 • 無線固有 KPI の現在のチャネルと拡張チャネルが追加されました。 [RF] タブで、無線固有 KPI の Clean Air ステータスと Tx Power が追加されました。 無線固有 KPI の Tx Power およびチャネル情報チャートが新たに追加されました。 デバイスの健全性のモニターとトラブルシューティング（102 ページ）を参照してください。

機能	説明
アプリケーションアシュアランスとテレメトリの IPv6 サポート	次のデバイスからの IPv6 トラフィックを監視し、監視データを**アシュアランス**ダッシュボードに表示します。 • Cisco IOS-XE ソフトウェアバージョン 17.2.1 以降を実行している Cisco Catalyst 9300 シリーズおよび Catalyst 9400 シリーズ スイッチ。 • Cisco IOS-XE ソフトウェアバージョン 17.3 以降を実行しているルータ。 • Cisco IOS-XE ソフトウェアバージョン 17.3 以降を実行している Cisco DNA トラフィック テレメトリ アプライアンス。
アプリケーションの正常性ダッシュボードに追加された専用 SSID フィルタ	SSID フィルタオプションが**[Assurance]** > **[Health]** > **[Application]**ダッシュボードに追加されました。SSID フィルタオプションでは、SSID を選択できます。選択した内容に応じて、**アプリケーションの正常性**ダッシュボードの情報が更新されます。
Auto Refresh	Cisco DNA Center アシュアランスの正常性ウィンドウは、自動更新設定をサポートします。この設定オプションを使用すると、全体的な正常性、ネットワーク、クライアント、アプリケーション、デバイス 360、クライアント 360、Wi-Fi 6 などのアシュアランスウィンドウの自動更新機能を有効にすることができます。
SD-Access ランディングウィンドウとファブリックビュー	このリリースでは、[SD-Access] タブが**[Assurance]** > **[Health]**ダッシュボードに追加されています。ファブリック固有の正常性の情報は、ネットワークの正常性ウィンドウとは別のウィンドウに表示されます。SD-Access ファブリックネットワーク全体の正常性を表示し、ドリルダウンして、サイト固有およびデバイス固有のファブリックの正常性情報に関する詳細を表示できます。 SD-Access ファブリックの正常性の監視とトラブルシュート （198 ページ）およびファブリックサイトの正常性の監視 （201 ページ）を参照してください。
PoE の拡張機能	[Assurance] > [Dashboards] > [PoE] ダッシュボードでは、新しい [PoE AP Power Mode Distribution] ダッシュレットに、完全に電力が供給されている AP と部分的に電力が供給されている AP の分布が表示されます。 さらに、AP の Power over Ethernet（PoE）要素がデバイスとクライアントの詳細ウィンドウに表示されるようになりました。 ネットワーク内の PoE 対応デバイスの監視 （304 ページ）、デバイスの健全性のモニターとトラブルシューティング （102 ページ）、およびクライアントデバイスの健全性のモニターとトラブルシューティング （152 ページ）を参照してください。
クライアント 360 のオンボーディング時間	クライアント 360 では、タイムラインスライダに、関連付け、認証、DHCP 時間などのクライアント オンボーディングの詳細が表示されます。 クライアントデバイスの健全性のモニターとトラブルシューティング （152 ページ）を参照してください。

機能	説明
パストレースの拡張機能	パストレースは、ネットワークパケットをキャプチャするために [Live Traffic] 機能が拡張されています。 「パス トレースの実行 （375 ページ）」を参照してください
Webex クライアント 360 の機能強化	クライアント 360 では、Webex 360 を使用して、クライアントの Webex ミーティングを表示および監視します。 クライアントデバイスの健全性のモニターとトラブルシューティング （152 ページ）を参照してください。
クライアント オンボーディングのサーバー遅延	[Client Onboarding Times] ダッシュレットでは、最新のクライアント オンボーディング チャートの詳細ビューに、認証および DHCP オンボーディングのサーバーおよび遅延時間が表示されます。 すべてのクライアント デバイスの健全性のモニターとトラブルシューティング （137 ページ）を参照してください。
ネットワークヒートマップの機能強化	[Network Heatmaps] ウィンドウは、CSV ファイルへのヒートマップデータの**エクスポート**をサポートしています。 ネットワークヒートマップ内アクセスポイントの比較 （328 ページ）を参照してください。
[Network Services] ダッシュレット	[Overall Health] ダッシュボードの新しい [Network Services] ダッシュレットには、企業全体のワイヤレスコントローラによって報告されたすべての [AAA] および [DHCP] サーバーの成功および失敗したトランザクションの合計が表示されます。 企業の全体的な健全性のモニターとトラブルシューティング （131 ページ）を参照してください。
ネットワーク サービス	このリリースでは、[Network Services] タブが**[Assurance]** > **[Health]**ダッシュボードに追加されています。[Network Services] タブでは、ワイヤレスコントローラによって報告された [AAA] および [DHCP] サーバーのすべてのトランザクションと遅延を表示および監視できます。 AAA ネットワークサービスの監視 （187ページ）、およびDHCP ネットワークサービスの監視 （190 ページ）を参照してください。



第 2 章

Cisco DNA アシュアランス の概要

About Cisco DNA アシュアランス

アシュアランス増え続けるビジネスニーズに対応するために、優れた一貫性のあるサービスレベルを保証する包括的なソリューションを提供します。リアクティブなネットワーク監視とトラブルシューティングに対応するだけではなく、ネットワーク実行のプロアクティブかつ予測的側面にも対応し、クライアント、アプリケーション、およびサービスの最適なパフォーマンスを確保します。

アシュアランス には、次のような利点があります。

- ネットワーク、クライアント、およびアプリケーション関連の問題へ実用的な情報を提供します。これらの問題は、複数の情報の基本的および高度な相関関係から成り立っているため、ホワイトノイズと誤検出は除外されます。
- システムガイド付きとガイドなしの両方のトラブルシューティングを提供します。アシュアランス は多くの問題に対してシステムガイド付きアプローチを提供します。このアプローチでは、複数の重要業績評価指標（KPI）が関連付けられ、テストおよびセンサーからの結果を使用して問題の根本原因を特定してから、可能なアクションを提示して問題を解決します。データの監視ではなく、問題点を浮き彫りにすることに重点が置かれています。アシュアランス では、非常に頻繁にレベル 3 サポートエンジニアの作業が実行されます。
- ネットワークとネットワークデバイス、クライアント、アプリケーション、およびサービスに関する詳細な正常性スコアを提供します。アクセス（オンボーディング）と接続の両方のクライアント エクスペリエンスが保証されます。

アシュアランス のアーキテクチャ

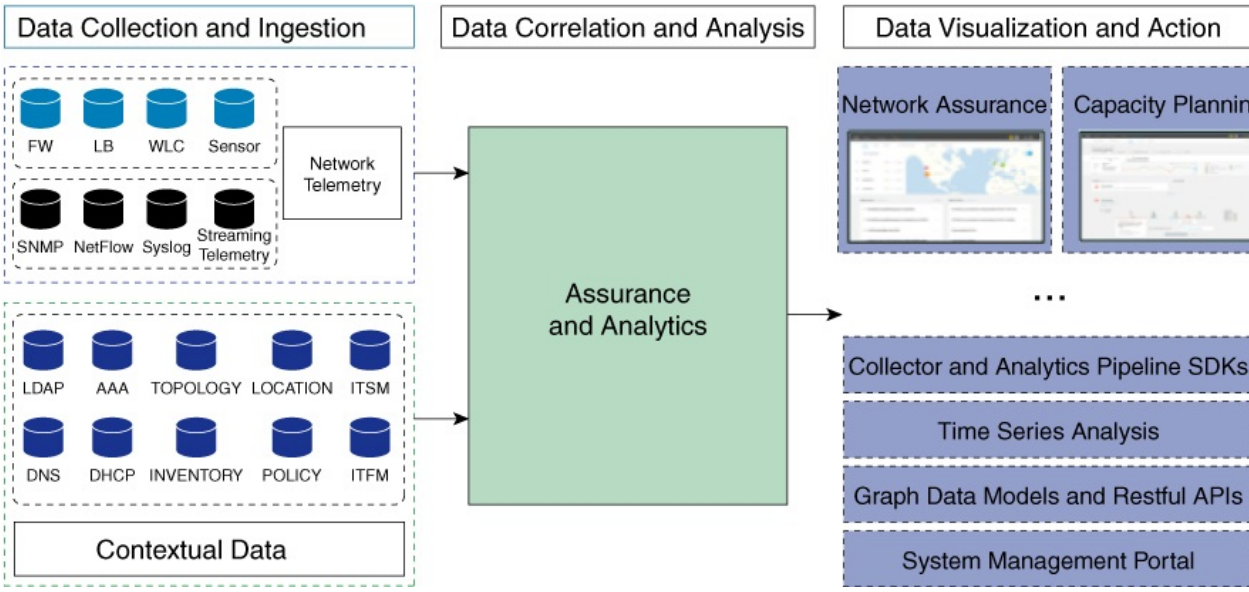
企業は多数のネットワークデータを扱っています。IT組織にとっては、ネットワークデータの量、多様性、速度、および精度への対応が重要です。アシュアランスは、ネットワークデータの問題（ある場合）を処理するために設計されています。

アシュアランス 多目的でリアルタイムのネットワークデータの収集および分析エンジンであり、これによりネットワークデータのビジネスにおける可能性を大幅に向上させることができます。

アシュアランス 収集層と分析層を簡略化および抽象化し、Web インターフェイスとともに豊富な API を提供しています。アシュアランスは、1 セットのネットワークデータを使用して幅広い使用例に対応します。これらの利点により、ネットワークデータの収集および分析に伴う動作およびネットワーク管理のオーバーヘッドが合理化され、企業はそれぞれの企業目標に効果的に注力できます。

柔軟なアーキテクチャを備えた アシュアランス は、広範な Cisco DNA 戦略をサポートしながら、モニターリングとトラブルシューティング、コスト管理、ポリシー検出など、一般的な多くの使用例に対応します。

次の図とその後の情報で、アシュアランス アーキテクチャについて説明します。



- **データ収集と取り込み**：アシュアランスはストリーミングテクノロジーを活用して、さまざまなネットワークテレメトリとコンテキストデータをリアルタイムで収集します。
- **データ相関関係と分析**：データが取り込まれると、アシュアランスはデータを関連付けて分析します。

- **データの可視化とアクション**：データはデータベースに保存され、API を介してアシュアランスやその他のアプリケーション（キャパシティプランニングなど）に公開されます。アシュアランス は、以下を提供するオープンシステムです。
  - コレクタと分析パイプライン SDK
  - 時系列分析
  - グラフデータモデルと RESTful API
  - システム管理ポータル

IPv6 アドレスのサポート

Cisco DNA Center では IPv6 アドレスがサポートされています。単一の IPv6 アドレスは多くのテキスト形式で表現できますが、Cisco DNA Center では標準形式の IPv6 アドレスのみサポートされています。標準形式は、次に示されているように、正規化圧縮形式とも呼ばれます。

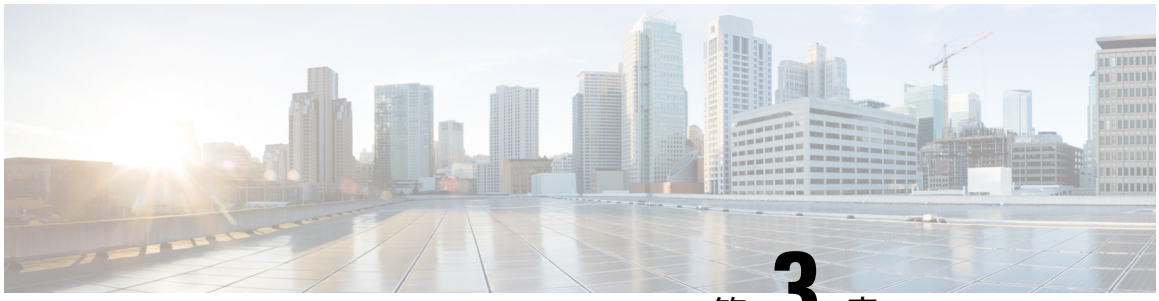
```
2001:db8::1:0:0:1
```

始める アシュアランス

アシュアランス の使用を開始するには、まず、サーバーがネットワーク外と通信できるように Cisco DNA Center を設定する必要があります。

Cisco DNA Center の設定後、現在の環境で アシュアランス の使用を開始する方法を決定します。

- 既存のインフラストラクチャ：既存のインフラストラクチャ（ブラウンフィールド導入）があれば、ディスカバリを実行して開始します。ディスカバリを実行すると、すべてのデバイスが **[Inventory]** ウィンドウに表示されます。詳細については、基本的な設定のワークフロー （17 ページ）を参照してください。
- 新規または存在しないインフラストラクチャ：既存のインフラストラクチャがなく、ゼロから開始（新規導入）する場合は、ネットワーク階層を設計します。ネットワーク階層の設計については、Cisco DNA Center ユーザガイドを参照してください。



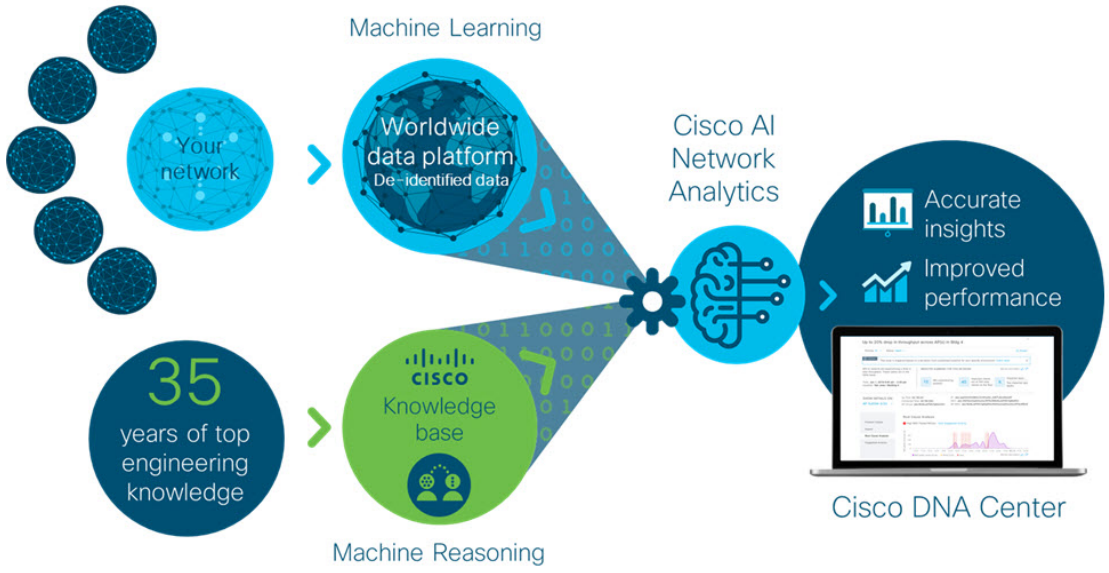
第 3 章

Cisco AI Network Analytics の概要

About Cisco AI Network Analytics

Cisco AI Network Analytics は、Cisco DNA Center に搭載されているアプリケーションです。機械学習と機械推論の能力を活用して、ネットワークの導入に特化した正確なインサイトを提供し、問題の迅速な解決を可能にします。次の図とその後の情報で、Cisco AI Network Analytics アーキテクチャについて説明します。

図 *1 : Cisco AI Network Analytics* アーキテクチャ



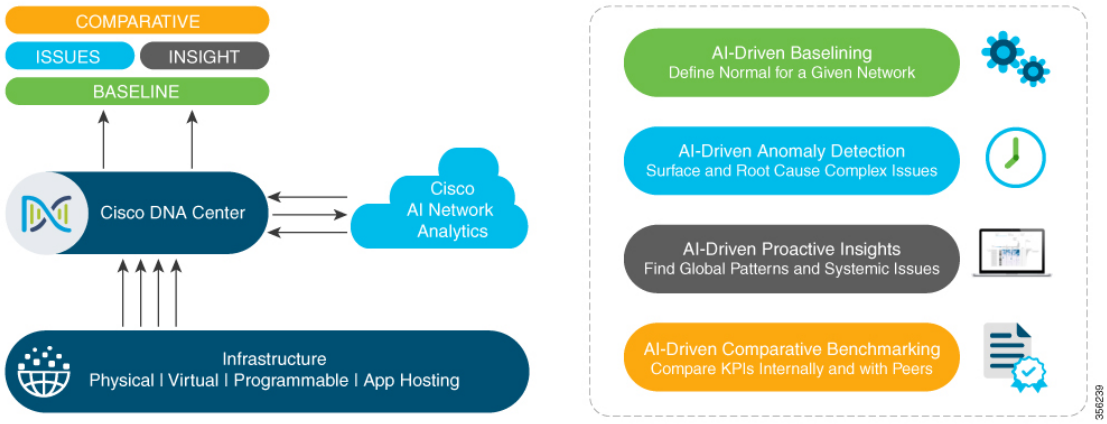
Cisco AI Network Analytics 構成は次のとおりです。

- 特定のネットワーク環境に応じた機械学習モデルの構築と分析を実現するグローバルなクラウドベースのデータプラットフォーム。
- 人間の専門知識を自動化し、ナレッジベースリポジトリ内のワークフローをキャプチャする機械推論エンジン。

機械学習

Cisco AI Network Analytics は高度な機械学習（ML）技術、および非特定化ネットワークイベントデータを含む高度なクラウド学習プラットフォームを活用して、ネットワーク内の重大な問題を特定し、豊富な情報を提供します。これにより、Cisco AI Network Analytics では問題の迅速なトラブルシューティングと根本原因の特定、トレンドとインサイトの特定による相対的な視点の獲得が実現します。Cisco AI Network Analytics は、Cisco DNA アシュアランス と完全に統合された Cisco DNA Center のシンプルかつ直感的で強力なユーザーインターフェイスを駆使して、こうした価値を提供します。

図 *2 : Cisco AI Network Analytics* 機能



Cisco AI Network Analytics は、次のとおりです。

- **クラウドベースのインフラストラクチャ**：ネットワークイベント情報が Cisco DNA Center で非識別化され、セキュアな暗号化チャネルを介して Cisco AI Network Analytics クラウドベースのインフラストラクチャに送信されます。Cisco AI Network Analytics クラウドは、このような非識別化されたネットワークイベント データに対して機械学習モデルを実行し、問題点と包括的なインサイトを Cisco DNA Center に返します。
- **インテリジェントな問題の検出と分析**には、次の機能が含まれます。
  - **AI 駆動型の基準値設定**：基準値設定は、ネットワークダイナミクスの分析に使用される手法です。特定のネットワークの「通常」（基準）の動作を定義するための動作パターンを抽出します。次に、実際のネットワークパフォーマンスがその基準と比較されます。

    Cisco AI Network Analytics 最先端の機械学習技術を活用して、特定のネットワークとサイトの現在の条件に合わせて基準を定義します。Cisco AI Network Analytics は、こ

の情報に基づいて特定の時点における各ネットワークとサイトの正常な動作を定義し、最も重要な問題を特定できます。

- **AI 駆動型の異常検出**：異常を検知して、根本原因を特定し、トラブルシューティングを容易にします。

  Cisco AI Network Analytics 次のタイプの AI 駆動型の問題を検出できます。

  - **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な DHCP 時間、過剰な DHCP 障害回数、過剰な AAA 時間、過剰な AAA 障害回数、過剰な関連付け時間、過剰な関連付け障害回数。
  - **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーションアプリケーションのスループット、およびソーシャルアプリケーションのスループット。

- **トレンドとインサイト**には、次の機能があります。
  - **AI 駆動型のプロアクティブインサイト**：グローバルパターン（トレンド）と乖離度を調べて、システム生成のインサイトを提供します。
- **比較ベンチマーク**には、次の機能があります。
  - **AI 駆動型 AP 比較**：ヒートマップ内の特定の月について、ネットワーク内のすべての AP を比較してトレンドを把握し、洞察を得ます。
  - **AI 駆動型のピア比較**：選択した主要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。
  - **AI 駆動型のサイト比較**：選択した KPI について、ネットワーク内の別のサイトと比較して、サイト（ビルディング）のパフォーマンスを判断します。

機械推論

機械推論エンジン（MRE）は、ネットワーク自動化エンジンであり、人工知能（AI）を使用して複雑なネットワーク運用ワークフローを自動化します。完全に自動化された推論エンジンに人間の知識と専門知識をカプセル化し、複雑な根本原因の分析、問題や脆弱性の検出、および手動または自動による是正処置の実行を支援します。MRE は、シスコのネットワーキング エキスパートによって構築された、クラウドホスト型のナレッジベースを実装しています。

Cisco AI ネットワーク分析の利点

Cisco AI Network Analytics には、次のような利点があります。

- **可視性の向上**：各ネットワークは一意であり、ネットワーク環境は常に変化しています。Cisco AI Network Analytics は、ローカルネットワークから継続的に関連データを収集し、そのデータを集約非特定化データセットと関連付けた後、高度な機械学習モデルを活用し

て、特定のネットワークとサイトに関連する基準を作成します。これらの基準は、ネットワーク環境の変化に応じて、デバイス数、ユーザー数、およびアプリケーション数が増加するのに伴い、学習し適応します。

- **インサイトの向上**：Cisco AI Network Analytics では、機械学習を使用して、ネットワークからの膨大な量のデータを個別のネットワーク基準値に関連付け、ネットワークに重大な影響をもたらす問題を明らかにします。これにより、問題の関連性が絞り込まれます。Cisco AI Network Analytics は、ネットワーク動作の傾向とパターンを検出し、具体的な問題が派生する前に問題を特定できるようにします。
- **ガイド付きアクション**：Cisco AI Network Analytics は、機械学習アルゴリズムと自動化されたワークフローを使用して論理的なトラブルシューティング手順を実行し、エンジニアが問題を実行して解決できるようにします。これにより、IT部門は、問題と脆弱性を検出し、根本原因を分析し、迅速に是正措置を施すことができます。

Cisco AI Network Analytics のライセンスと導入

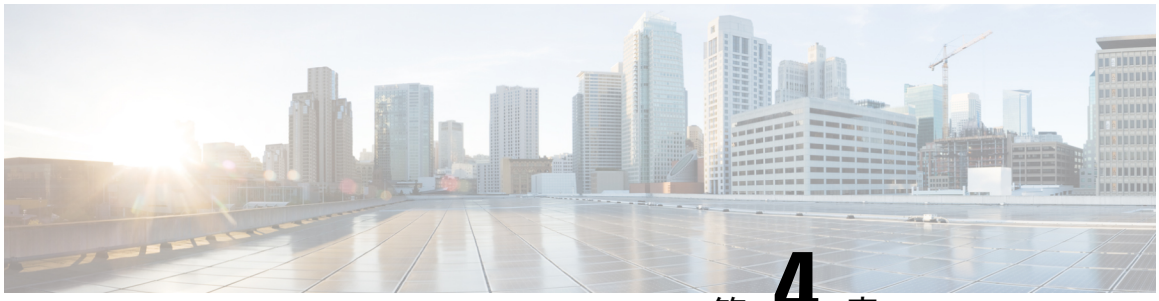
Cisco AI Network Analytics は、Cisco DNA Center の **Cisco DNA Advantage** ソフトウェアライセンスの一部です。これは追加のコンポーネントとして提供され、アシュアランスのユーザーインターフェイスとシームレスに統合されます。このソリューションにより、最先端の機械学習により生成されたインサイトと問題が提供され、機械学習エンジンで発生した問題の分析、トラブルシューティング、および対応に必要な可視化ツールもいっしょに提供されます。

Cisco AI Network Analytics を展開するには、（アプライアンス フォーム ファクタで稼働している）Cisco DNA Center の実行インスタンスと、Cisco AI Network Analytics クラウドへの HTTPS 接続が必要です。HTTPS 接続は、プロキシサーバーを介してもサポートされます。HTTPS 接続にプロキシサーバーを使用する場合、設定は Cisco DNA Center グローバル設定から継承されます。ネットワークイベントデータは、クラウドに送信される前に非特定化されます。結果とインサイトは Cisco AI Network Analytics クラウドサービスによって返され、復号された後、アシュアランス ユーザーインターフェイスに直接表示されます。詳細については、「Cisco AI Network Analytics Privacy Data Sheet」を参照してください。

Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされている Cisco AI Network Analytics の機能

Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされている Cisco AI Network Analytics の機能、およびソフトウェアの最小バージョンを次の表に示します。

Cisco DNA Center リリース	サポートされる機能	Cisco IOS-XE の最小ソフトウェアバージョン
2.2.3	• **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な関連付け時間、過剰な関連付け障害回数、過剰な認証時間、過剰な認証障害回数、過剰な DHCP 時間、過剰な DHCP 障害回数。 （注） スループットの問題はサポートされていません。 • **トレンドと考察**	16.12.1s



第 4 章

アシュアランス を使用するための Cisco DNA Center の設定

アシュアランス アプリケーションの使用を開始する前に、アシュアランス を設定する必要があります。ここでは、アシュアランスを設定するために実行する必要がある基本タスクについて説明します。この章は、Cisco Digital Network Architecture Center ユーザー ガイド と併用してください。

制限事項と制約事項

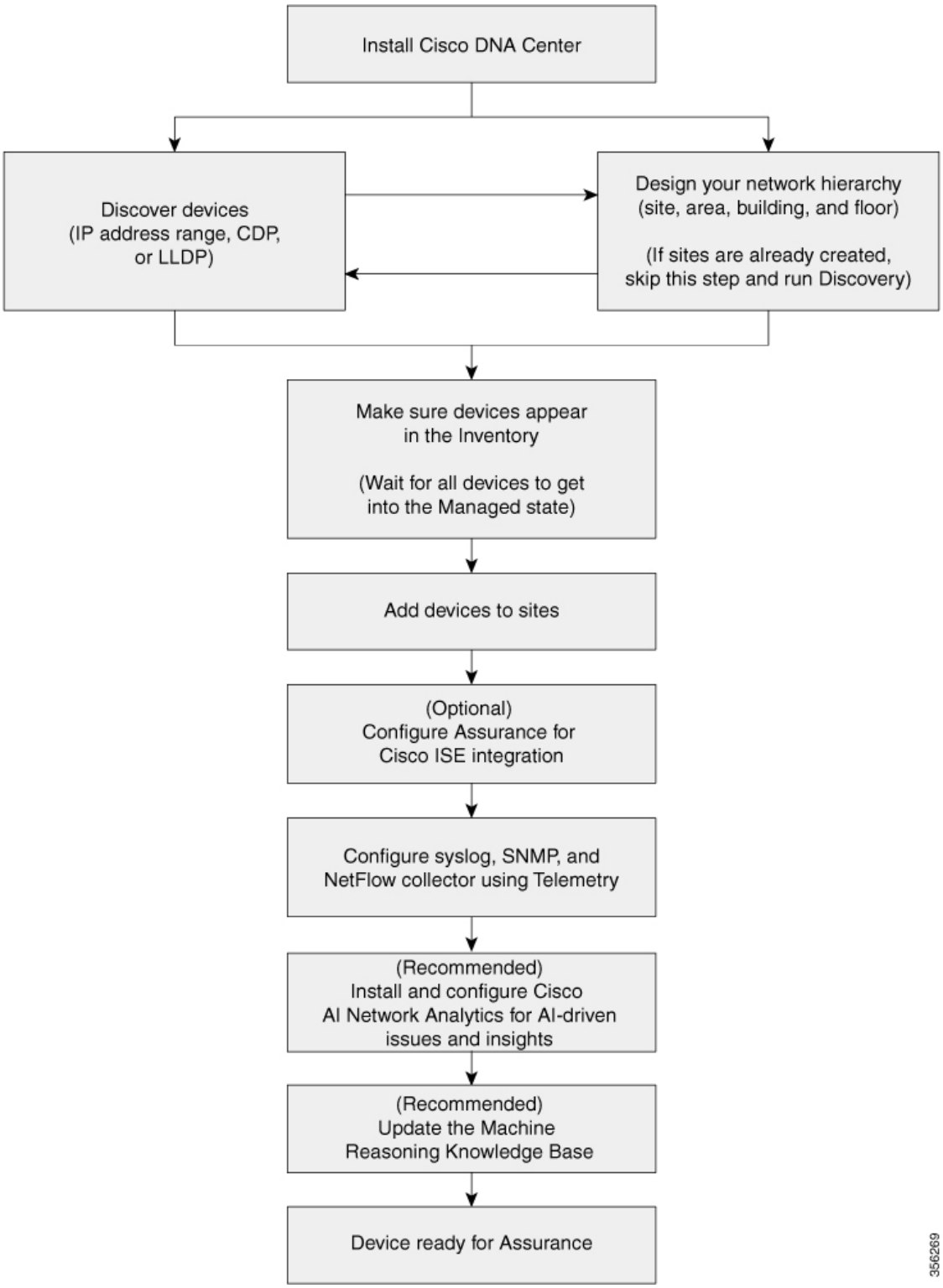
アシュアランスでは、管理対象デバイスへの NAT 接続はサポートされていません。

基本的な設定のワークフロー

アシュアランス アプリケーションの使用を開始する前に、アシュアランスを使用するために Cisco DNA Center を設定する必要があります。

基本的なワークフローを理解するために、次の図と次の手順を参照してください。

図 *3 :* アシュアランスを使用するための *Cisco DNA Center* の設定の基本的なワークフロー



始める前に

制限事項と制約事項 （17 ページ）を参照してください。

ステップ 1 Cisco DNA Center をインストールします。

Cisco DNA Center 設置ガイドを参照してください。

ステップ 2 任意の順序で次の操作を行います。

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、アクセス ポイント）を検出します。

  IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。

  （注） Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

- ネットワーク階層を設計します。エリア、サイト、ビルディング、フロアなど、デバイスの場所を設定します。

  ネットワーク階層のサイトの作成 （46 ページ）、建物の追加 （47 ページ）、およびビルディングへのフロアの追加 （47 ページ）を参照してください。

  （注） サイトがすでに作成されている場合は、このステップをスキップし、Discovery を実行できます。

ステップ 3 デバイス インベントリにデバイスが表示されることを確認します。

インベントリに関する情報の表示 （69 ページ）を参照してください。

（注） すべてのデバイスが管理状態になるのを待つ必要があります。

ステップ 4 サイトへのデバイスの追加

デバイスをサイトに追加する （78 ページ）を参照してください。

ステップ 5 AP を追加する場合は、フロア マップに割り当てて配置することをお勧めします。

「AP の追加、配置、および削除 （54 ページ）」を参照してください。

ステップ 6 ネットワークでのユーザー認証に Cisco Identity Services Engine を使用している場合、アシュアランス を設定して Cisco ISE を統合できます。統合することで、アシュアランスのユーザー名やオペレーティング システムなど、有線クライアントの詳細な情報を参照できます。

Cisco DNA Center 向けの Cisco ISE の設定について （78 ページ）を参照してください。

ステップ 7 テレメトリを使用して、Syslog、SNMP トラップ、および NetFlow コレクタ サーバーを設定します。

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （83 ページ）を参照してください。

ステップ 8 （推奨）AI 駆動型の問題を確認し、ネットワークインサイトを取得するには、Cisco AI Network Analytics データ収集を設定します。

Cisco AI Network Analytics データ収集の設定 （84 ページ）を参照してください。

ステップ 9 （推奨）最新の機械推論ワークフローにアクセスするには、機械推論ナレッジベースを更新します。

機械推論ナレッジベースの更新 （87 ページ）を参照してください。

ステップ 10 アシュアランス アプリケーションの使用を開始します。

デバイスの検出

ディスカバリ機能は、ネットワーク内のデバイスをスキャンし、検出されたデバイスの一覧をインベントリに送信します。

ディスカバリについて

ディスカバリ機能は、ネットワーク内のデバイスをスキャンし、検出されたデバイスの一覧をインベントリに送信します。

また、ディスカバリ機能は、デバイスの可制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（これらの設定がデバイスにまだ存在しない場合）。

デバイスは次の 3 つの方法で検出できます。

- Cisco Discovery Protocol（CDP）を使用し、シード IP アドレスを指定します。
- IP アドレスの範囲を指定します（最大 4096 デバイスの範囲がサポートされます）。
- Link Layer Discovery Protocol（LLDP）を使用し、シード IP アドレスを指定します。

ディスカバリ基準を設定する際は、ネットワーク検出時間を短縮するために役立つ設定があることに注意してください。

- [CDP Level] と [LLDP Level]：CDP または LLDP をディスカバリ方式として使用する場合は、CDP レベルまたは LLDP レベルを設定して、スキャンするシードデバイスからのホップ数を指定できます。デフォルトのレベル 16 では、大規模なネットワークの場合に時間がかかる可能性があります。そのため、検出する必要があるデバイスが少ない場合は、このレベルをより低い値に設定できます。
- [Subnet Filters]： IP アドレスの範囲を使用する場合は、特定の IP サブネット内のデバイスをディスカバリで無視するように指定できます。
- [Preferred Management IP]：CDP、LLDP、または IP アドレスの範囲のいずれを使用する場合でも、Cisco DNA Center がデバイスの任意の IP アドレスを追加するか、デバイスのループバックアドレスのみを追加するかを指定できます。

（注） Cisco SD-Access ファブリックおよび Cisco DNA アシュアランスについては、デバイスのループバックアドレスを指定することをお勧めします。

どの方式を使用する場合でも、Cisco DNA Center からデバイスにアクセスできる必要があり、デバイスを検出するための特定のクレデンシャルとプロトコルを Cisco DNA Center で設定する必要があります。これらのログイン情報は、**[Design]** > **[Network Settings]** > **[Device Credentials]** ウィンドウで（または [Discovery] ウィンドウでジョブごとに）設定して保存することができます。

（注） デバイスが Hot Standby Router Protocol（HSRP）や Virtual Router Redundancy Protocol（VRRP）などのファーストホップ解決プロトコルを使用する場合、そのデバイスは、そのフローティング IP アドレスによって検出され、インベントリに追加される可能性があります。その後、HSRP または VRRP に障害が発生すると、その IP アドレスが別のデバイスに割り当てなおされる場合があります。この場合、Cisco DNA Center が分析のために取得するデータによって問題が発生する可能性があります。

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- Cisco DNA Center によって検出されるデバイスの情報については、「サポート対象デバイスのリスト」を参照してください。
- Cisco DNA Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間（RTT）であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。
- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
  - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
  - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、設定のガイドラインと制限事項のディスカバリ （22 ページ）を参照してください。

優先管理 IP アドレス

Cisco DNA Center でデバイスが検出されると、デバイスの IP アドレスの 1 つが優先管理 IP アドレスとして使用されます。IP アドレスは、デバイスの組み込み管理インターフェイス、または別の物理インターフェイス、または Loopback0 のような論理インターフェイスの IP アドレスにすることができます。デバイスのループバック IP アドレスを優先管理 IP アドレスとして使用するために Cisco DNA Center を設定できます（その IP アドレスが Cisco DNA Center から到達可能である場合）。

優先管理 IP アドレスとして [Use Loopback IP] を選択した場合、Cisco DNA Center では次のように優先管理 IP アドレスが指定されます。

- デバイスに 1 つのループバック インターフェイスがある場合、Cisco DNA Center は、そのループバック インターフェイスの IP アドレスを使用します。
- デバイスに複数のループバック インターフェイスがある場合、Cisco DNA Center は、最上位の IP アドレスを持つループバック インターフェイスを使用します。
- ループバック インターフェイスがない場合、Cisco DNA Center は、最上位の IP アドレスを持つイーサネット インターフェイスを使用します（サブインターフェイスの IP アドレスは考慮されません）。
- イーサネット インターフェイスがない場合、Cisco DNA Center は、最上位の IP アドレスを持つシリアル インターフェイスを使用します

デバイスが検出された後に、**[Inventory]** ウィンドウから管理 IP アドレスを更新できます。

設定のガイドラインと制限事項のディスカバリ

Cisco DNA Center による Cisco Catalyst 3000 シリーズ スイッチおよび Catalyst 6000 シリーズ スイッチの検出に関する注意事項と制約事項は、次のとおりです。

- CLI ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定してください。これは、ディスカバリ機能のために Cisco DNA Center で設定する CLI ユーザ名およびパスワードと同じです。Cisco DNA Center にはデバイスへの最高レベルのアクセス権が必要です。
- 着信接続と発信接続の両方に関して、個々のインターフェイスで許可されるトランスポート プロトコルを明示的に指定してください。この設定には、**transport input** と **transport output** コマンドを使用してください。これらのコマンドについては、各デバイス タイプ用のコマンド リファレンス ドキュメントを参照してください。
- デバイスのコンソールポートと VTY 回線のデフォルトのログイン方式を変更しないでください。デバイスがすでに AAA（TACACS）ログインで設定されている場合は、Cisco DNA Center で定義されている CLI ログイン情報が、TACACS サーバで定義されている TACACS ログイン情報と同じであることを確認してください。

- Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

CDP を使用したネットワークの検出

Cisco Discovery Protocol（CDP）IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、IP アドレス範囲を使用したネットワークの検出 （30 ページ）およびLLDP を使用したネットワークの検出 （36 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベスト エフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで CDP を有効にします。
- ディスカバリの前提条件 （21 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 まだ表示されていない場合は [IP アドレス/範囲（IP Address/Range）] エリアを展開し、次のフィールドを設定します。

a) [ディスカバリ タイプ（Discovery Type）] で、[CDP] をクリックします。
b) [IP アドレス（IP Address）] フィールドでシード IP アドレスを入力し、Cisco DNA Centerでディスカバリ スキャンを開始します。

c) （任意）[サブネット フィルタ（Subnet Filter）] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネット マスクは、0 ～ 32 の値です。

d) [+] をクリックします。

手順 c および d を繰り返して、ディスカバリ ジョブから複数のサブネットを除外します。

e) （任意）[CDP レベル（CDP Level）] フィールドに、スキャンするシード デバイスからのホップ数を入力します。

有効値は 1 ～ 16 です。デフォルト値は 16 です。たとえば、CDP レベル 3 は、CDP がシード デバイスから最大 3 つのホップまでスキャンすることを意味します。

f) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （22 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

（注） ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスがCisco DNA Centerから到達可能であることを確認します。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。独自のログイン情報を設定する場合は、[Save] をクリックして現在のジョブに対してのみ保存することもできれば、[Save as global settings] チェックボックスをクリックし、次に [Save] をクリックして、現在または将来のジョブに対して保存することもできます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。
b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。
c) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 *5 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。

フィールド	説明
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *6 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *7 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。

フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *8 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意） [HTTP（S）] をクリックして、次のフィールドを設定します。

表 *9 : HTTPS* クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。

フィールド	説明
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

h) （任意）NETCONF が有効化されているネットワークデバイスが存在する場合、[NETCONF] をクリックして、[ポート（Port）] フィールドにポート数を入力します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830（デフォルトのポート番号）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合）

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

ステップ 6 デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。

有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始する前にキャンセルするには、[Cancel] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

[Discovery Details] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）] ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

IP アドレス範囲を使用したネットワークの検出

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （23 ページ）およびLLDP を使用したネットワークの検出 （36 ページ）を参照してください。

始める前に

ディスカバリの前提条件 （21 ページ）で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 まだ表示されていない場合は [IP アドレス/範囲（IP Address/Ranges）] エリアを展開し、次のフィールドを設定します。

a) [Discovery Type] で、[IP Address/Range] をクリックします。

b) [From] フィールドと [To] フィールドに、スキャンする Cisco DNA Center 最初の IP アドレスと最後の IP アドレス（IP アドレス範囲）を入力し、+ をクリックします。

検出スキャンに対して、単一の IP アドレス範囲または複数の IP アドレスを入力できます。

（注） Cisco ワイヤレス コントローラは、サービス ポート IP アドレスではなく、管理 IP アドレスを使用して検出する必要があります。それ以外の場合は、関連するワイヤレス コントローラ 360 および AP 360 のページでは、データが表示されません。

c) （任意） ステップ b を繰り返して、追加の IP アドレス範囲を入力します。

d) （任意） 検出スキャンから除外する IP アドレス/範囲またはサブネットを [Subnet Filter] フィールドに入力します。個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで *x.x.x.x* は IP アドレスを示し、*y* はサブネットマスクを示します。サブネット マスクは、0 ～ 32 の値です。

e) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） [ループバック IP を使用（Use Loopback IP）] の使用を選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Centerは優先管理 IP アドレス （22 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

ステップ 5 [クレデンシャル（Credentials）] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。独自のクレデンシャルを設定する場合、[保存（Save）] をクリックして現在のジョブにのみ保存できます。または、[グローバル設定として保存（Save as global settings）] チェックボックスをクリックし、次に [保存（Save）] をクリックして、現在または将来のジョブに保存できます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。

b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。

c) CLI クレデンシャルを設定するには、次のフィールドを設定します。

表 *10 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *11 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *12 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *13 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意） [HTTP（S）] をクリックして、次のフィールドを設定します。

表 *14 : HTTPS* クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

h) （任意）NETCONF が有効化されているネットワークデバイスが存在する場合、[NETCONF] をクリックして、[ポート（Port）] フィールドにポート数を入力します。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にし、ポートを次のいずれかに設定する必要があります。

- 830（デフォルトのポート番号）
- デバイスで使用可能なその他のポート
- Cisco DNA Center で設定されたカスタムポート（デバイスの可制御性が有効な場合）

NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。[Advanced] エリアで [Telnet] を選択すると、NETCONF は無効になります。

ステップ 6 （任意）デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルをクリックします。緑のチェックマークはプロトコルが選択されていることを示します。

有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

[Discovery Details] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）] ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol（LLDP）、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、CDP を使用したネットワークの検出 （23 ページ）およびIP アドレス範囲を使用したネットワークの検出 （30 ページ）を参照してください。

（注）

- ディスカバリ機能では、正しい SNMP 読み取り専用（RO）コミュニティ ストリングが必要です。SNMP RO コミュニティ ストリングが指定されていない場合、ベスト エフォートとして、ディスカバリ機能はデフォルトの SNMP RO コミュニティ ストリングを公的に使用します。
- CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで LLDP を有効にします。
- ディスカバリの前提条件 （21 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [Add Discovery] をクリックします。
[新規検出（New Discovery）] ウィンドウが表示されます。

ステップ 3 [ディスカバリ名（Discovery Name）] フィールドに、名前を入力します。

ステップ 4 [IP Address/Range] 領域を展開し、次のフィールドを設定します。

a) [ディスカバリ タイプ（Discovery Type）] で、[LLDP] をクリックします。

b) [IP アドレス（IP Address）] フィールドでシード IP アドレスを入力し、Cisco DNA Centerでディスカバリ スキャンを開始します。

c) （任意）[サブネット フィルタ（Subnet Filter）] フィールドで、ディスカバリ スキャンから除外する IP アドレスまたはサブネットを入力します。

個別の IP アドレス（*x.x.x.x*）または Classless Inter-Domain Routing（CIDR）アドレス（*x.x.x.x/y*）としてアドレスを入力できます。ここで*x.x.x.x* は IP アドレスを示し、*y* はサブネット マスクを示します。サブネット マスクは、0 ～ 32 の値です。

d) [+] をクリックします。

手順 c および d を繰り返して、ディスカバリ ジョブから複数のサブネットを除外します。

e) （任意）[LLDP レベル（LLDP Level）] フィールドで、スキャンするシード デバイスからのホップ数を入力します。

有効値は 1 ～ 16 です。デフォルト値は 16 です。たとえば、LLDP レベル 3 は、LLDP がシード デバイスから最大 3 つのホップをスキャンすることを意味します。

f) [Preferred Management IP] で、次のいずれかのオプションを選択します。

- [None]：デバイスはすべての IP アドレスを使用できます。
- [Use Loopback IP]：デバイスのループバックインターフェイスの IP アドレスを指定します。

（注） このオプションを選択し、デバイスにループバック インターフェイスがない場合、Cisco DNA Center は優先管理 IP アドレス （22 ページ）で説明されているロジックを使用して、管理 IP アドレスを選択します。

（注） ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスがCisco DNA Centerから到達可能であることを確認します。

ステップ 5 [Credentials] エリアを展開し、ディスカバリ ジョブで使用するクレデンシャルを設定します。

すでに作成されているグローバル クレデンシャルのいずれかを選択するか、独自のディスカバリ クレデンシャルを設定します。クレデンシャルを設定する場合は、[Save as global settings] チェックボックスをオンにして、将来のジョブのためにそれらを保存できます。

a) 使用するグローバル クレデンシャルが選択されていることを確認します。そのクレデンシャルを使用しない場合は、選択解除します。

b) 別のクレデンシャルを追加するには、[Add Credentials] をクリックします。
c) CLI クレデンシャルの場合は、次のフィールドを設定します。

表 *15 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスのCLIにログインするために使用する名前。
Password	ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Enable Password	CLI で高い権限レベルに移るために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 セキュリティ上の理由から、有効なパスワードを再入力します。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 *16 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。 （注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

e) （任意） [SNMP v3] をクリックして、次のフィールドを設定します。

表 *17 : SNMPv3* のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [noAuthNoPriv]：認証または暗号化を提供しません。 • [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。 • [AuthPriv]：認証と暗号化の両方を提供します。
Auth Type	使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5]：HMAC-MD5 に基づく認証。
Auth Password	SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の CBC モード AES。 • [None]：プライバシー設定はありません。

フィールド	説明
Privacy Password	AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。 （注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

f) （任意） [SNMP PROPERTIES] をクリックして、次のフィールドを設定します。

表 *18 : SNMP* のプロパティ

フィールド	説明
Retries	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
Timeout	再試行間隔を表す秒数。

g) （任意） [HTTP（S）] をクリックして、次のフィールドを設定します。

表 *19 : HTTPS* クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。

フィールド	説明
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

ステップ 6 （任意） デバイスとの接続に使用されるプロトコルを設定するには、[詳細（Advanced）] エリアを展開し、次のタスクを実行します。

a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。有効なプロトコルは、[SSH]（デフォルト）および [Telnet] です。

b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

ステップ 7 [Discover] をクリックして、すぐに検出を実行するか、または後で実行するために検出をスケジュールするかを選択します。

- 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。
- 後で検出をスケジュールするには、[Later] ラジオボタンをクリックして更新の日時を定義し、[Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出タスクを表示します。検出を開始する前に検出タスクを編集するには、[Edit] をクリックします。スケジュールされた検出ジョブを開始前にキャンセルする場合は、[Cancel] をクリックします。

[Discoveries] ウィンドウにスキャンの結果が表示されます。

[Discovery Details] ペインに、ステータス（アクティブまたは非アクティブ）および検出設定が表示されます。[デバイスのディスカバリ（Discovery Devices）]ペインに、検出されたデバイスのホスト名、IP アドレス、ステータスが表示されます。

ディスカバリ ジョブの管理

ディスカバリ ジョブの停止および開始

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 アクティブなディスカバリ ジョブを停止するには、次の手順を実行します。

a) **[Discoveries]** ペインで、関連するジョブを選択します。

b) [Stop] をクリックします。

ステップ 4 非アクティブなディスカバリ ジョブを再起動するには、次の手順を実行します。

a) **[Discoveries]** ペインで、関連するジョブを選択します。

b) [Re-discover] をクリックして、選択したジョブを再起動します。

ディスカバリ ジョブの複製

ディスカバリジョブを複製し、そのジョブ用に定義されているすべての情報を保持できます。

始める前に

少なくとも 1 つのディスカバリ ジョブを実行する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。

ステップ 4 [Copy & Edit] をクリックします。

Cisco DNA Center では、「*Copy of Discovery_Job*」という名前でディスカバリジョブのコピーが作成されます。

ステップ 5 （任意） 検出ジョブの名前を変更します。

ステップ 6 新しいディスカバリ ジョブのパラメータを定義または更新します。

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[ディスカバリ（Discovery）]**ペインで、削除する検出ジョブを選択します。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

使用された設定やクレデンシャルなどの、ディスカバリ ジョブに関する情報を表示できます。実行された各ディスカバリジョブに関する履歴情報（検出されたデバイスや検出に失敗したデバイスに関する情報など）も表示できます。

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Tools]** > **[Discovery]**。
[Discovery] ウィンドウがダッシュレットとともに表示されます。

ステップ 2 [View All Discoveries] をクリックします。

ステップ 3 **[Discovery]** ペインで、検出ジョブを選択します。もしくは、**[Search]** 機能を使用して、デバイス IP アドレスまたは名前によって、ディスカバリ ジョブを検索できます。

ステップ 4 詳細については、次の領域のひとつの隣にある下矢印をクリックします。

- [Discovery Details]：ディスカバリジョブを実行するために使用されたパラメータが表示されます。パラメータには、CDP または LLDP レベル、IP アドレス範囲、およびプロトコルの順序などの属性が含まれます。
- [Credentials]：使用されたログイン情報の名前が提供されます。
- [History]：実行された各ディスカバリジョブがリストされ、開始時刻やデバイス検出の有無などが表示されます。

  組み込みワイヤレスコントローラを正常に検出するには、NETCONF ポートを設定する必要があります。NETCONF ポートが設定されていない場合、ワイヤレスデータは収集されません。

  [Filter] 機能を使用して、IP アドレスあるいは ICMP、CLI、HTTPS、NETCOMF 値の任意の組み合わせによってデバイスを表示できます。

ネットワーク階層の設計

ネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層には、ビルディングやエリアなどが存在するサイトを含めることができます。

新しいネットワーク インフラストラクチャの設計

[Design]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、**ディスカバリ**機能を使用します。詳細については、「ディスカバリについて （20 ページ）」を参照してください。

これらのタスクは、[Design] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。

ステップ 2 グローバル ネットワーク設定を定義します。

ステップ 3 ネットワーク プロファイルを定義します。

ネットワーク階層について

ネットワークの地理的な場所を表すネットワーク階層を作成できます。ネットワーク階層には、ビルディングやエリアを含むサイトを含めることができます。サイト ID とビルディング ID を作成すると、後で、設計の設定や構成を適用する場所を簡単に特定できます。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。

ネットワーク階層は、次の事前設定された階層をもちます。

- [エリア（Areas）] や [サイト（Sites）] には、物理的なアドレス（例、米国）はありません。エリアは最大の要素だと考えることができます。エリアにはビルディングとサブエリアを含めることができます。たとえば、米国というエリアには、カリフォルニアというサブエリアが含まれ、カリフォルニアというサブエリアにはサンノゼというサブエリアが含まれることができます。
- [ビルディング（Buildings）] には物理アドレスがあり、フロアとフロア プランが含まれています。ビルディングを作成する場合、物理アドレスおよび緯度と経度の座標を指定する必要があります。ビルディングにエリアを含めることはできません。ビルディングを作成することで、特定のエリアに設定を適用できます。
- [フロア（Floors）] は建物内にあり、キュービクル、壁に囲まれたオフィス、配線クローゼットなどで構成されています。フロアはビルディングにのみ追加できます。

プロビジョニングされていないデバイスのサイト階層は、サイトマップ上の AP の場所を維持したまま変更できます。ただし、既存のフロアを別の建物に移動することはできません。

実行できるタスクのリストを以下に示します。

- 新しいネットワーク階層を作成する。詳細については、「ネットワーク階層のサイトの作成 （46 ページ）」を参照してください。
- Cisco Prime Infrastructure から既存のネットワーク階層をアップロードする。詳細については、既存のサイト階層をアップロード （49 ページ）を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

- マップのイメージファイルを .jpg、.gif、.png、.pdf、.dxf、.dwg などの形式で保存できるグラフィカル アプリケーションを使用します。
- イメージ画像の寸法が、キャンパスマップに追加する予定のすべてのビルディングと屋外領域の合計寸法よりも大きいことを確認します。
- マップのイメージファイルのサイズはさまざまです。Cisco DNA Center は元のイメージを完全な定義でデータベースにインポートしますが、表示中は、ワークスペースに合わせてサイズが自動的に変更されます。
- インポートする前に、サイトの縦と横の寸法をフィートまたはメートル単位で取得してください。これにより、マップ インポート時にこれらの寸法を指定できます。

ネットワーク階層のサイトの作成

Cisco DNA Center では、物理サイトを簡単に定義し、それらのサイトの共有リソースを特定することができます。[Design] エリアは、直観的な操作のために階層型になっており、デバイスをプロビジョニングするときに同じリソースを複数の場所で再定義する必要がありません。デフォルトでは、**グローバル**と呼ばれる 1 つのサイトがあります。ネットワーク階層には、複数のサイト、ビルディング、およびエリアを追加できます。プロビジョニング機能を使用する前に、少なくとも 1 つのサイトを作成する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

結果：世界地図が右側のペインに表示されます。

ステップ 2 マップツールバーから [+ Add Site] をクリックし、[Add Area] を選択します。

（注） 左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。

ステップ 3 [Area Name] フィールドにサイトの名前を入力します。

（注） [Area Name] フィールドには、次の制限があります。

- エリア名は 40 文字までです。
- 特殊文字（& > < ? ' " / [ ]）は使用できません。

ステップ 4 [Parent] ドロップダウンリストから、親ノードを選択します。

（注） デフォルトでは、**[グローバル（Global）]** が親ノードです。

ステップ 5 [Add]をクリックします。

結果：左側ペインの親ノードにサイトが作成されます。

建物の追加

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 [Network Hierarchy] ウィンドウで、**[+Add Site]** > **[Add Building]** をクリックします。

（注） または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Building] を選択することもできます。

ステップ 3 [Add Building] ポップアップで建物の詳細を追加します。

a) [Building Name] フィールドに建物の名前を入力します。

（注） [Building Name] フィールドには、次の制限があります。

- 建物名は 40 文字までです。
- 特殊文字（& > < ? ' " / [ ]）は使用できません。

b) [Parent] ドロップダウンリストから、親ノードを選択します。

（注） デフォルトでは、**[グローバル（Global）]** が親ノードです。

c) [Address] フィールドにアドレスを入力します。

（注） また、マップをクリックしてアドレスを入力することもできます。アドレスを追加すると、[Longitude] および [Latitude] の座標フィールドが自動的に設定されます。経度と緯度の座標を手動で変更して、アドレスを変更できます。

ステップ 4 [Add] をクリックします。

結果：左側ペインの親サイトに建物が作成され、表示されます。

ビルディングへのフロアの追加

ビルディングを追加したら、そのビルディングのフロアを作成する必要があります。

ステップ 1 [Menu] アイコン ☰ をクリックして、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左側のペインで、そのフロアのビルディングの横にある省略記号 ••• にカーソルを合わせ、[Add Floor] を選択します。

ステップ 3 [Floor Name] フィールドにフロアの名前を入力します。

（注） [Floor Name] フィールドには、次の制限があります。

- フロア名は 40 文字までです。
- 特殊文字（& > < ? ' " / [ ]）は使用できません。

ステップ 4 [Type (RF Model)] ドロップダウンリストから、フロアに適用する RF モデルを選択します。

（注） RF モデルは、フロアの特性に基づいて RF を計算する方法を決定します。

ステップ 5 [Floor Image] エリアで、フロアプランファイルをドラッグアンドドロップしてフロアプランをアップロードします。

（注） Cisco DNA Center では、フロアプランのファイルタイプとして DXF、DWG、JPG、GIF、PNG、および PDF がサポートされています。

図 *4:* フロア プランの例

（注） フロアプランをインポートしたら、オーバーレイの可視化を有効にしてください（フロアで [View Options] をクリックし、 [Overlay Objects] のオーバーレイトグルをオンにします）。デフォルトでは、マップをインポートした後にオーバーレイは表示されません。

ステップ 6 CAD ファイル（DXF または DWG ファイルタイプ）をアップロードする場合は、[Floormap] ポップアップを使用して、マップにフロア要素として表示する CAD レイヤーを選択します。

a) [2D] 列で、2D ビューに表示する CAD レイヤーのチェックボックスをオンにします。
b) [3D Wall/Shelving Type] 列で、CAD レイヤーのドロップダウンリストを使用して、壁または棚のタイプを指定します。

（注） レイヤーを 3D ビューに表示するには、[3D Wall/Shelving Type] 値が必要です。壁/棚のタイプは、減衰とヒートマップの計算方法に影響します。

c) [Use Selected Layers] をクリックします。

ステップ 7 [Width]、[Length]、および [Height] フィールドにフロアマップの寸法を入力します。

ステップ 8 [Add] をクリックします。

ネットワーク階層の管理

既存のサイト階層をアップロード

既存のネットワーク階層を含んでいる CSV ファイルまたはマップ アーカイブ ファイルをアップロードすることができます。たとえば、Cisco Prime Infrastructure からエクスポートしたロケーション情報を含む CSV ファイルをアップロードできます。Cisco Prime Infrastructure からのマップのエクスポートについては、マップ アーカイブのエクスポート （50 ページ）を参照してください。

（注） マップアーカイブファイルを Cisco DNA Center にインポートする前に、シスコ ワイヤレスコントローラや関連付けられている AP などのデバイスが検出され、Cisco DNA Center インベントリページに一覧になっていることを確認してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 ツールバーから [Import] をクリックし、[Import Sites] を選択します。

ステップ 3 CSV ファイルをドラッグしてドロップするか、または、CSV ファイルがある場所に移動し、[Import] をクリックします。

（注） 既存の CSV ファイルがない場合は、**[テンプレートをダウンロード（Download Template）]** をクリックして、編集可能なCSVファイルをダウンロードして、その後、アップロードすることができます。

ステップ 4 Cisco Prime Infrastructure マップ tar.gz アーカイブファイルをインポートするには**[Import]** > **[Map Import]**を選択します。

ステップ 5 [Import Site Hierarchy Archive] ダイアログボックスのボックスエリアにマップアーカイブファイルをドラッグしてドロップします。

ステップ 6 **[保存]** を選択してファイルをアップロードします。

結果：[Import Preview] ウィンドウが表示され、インポートされたファイルが示されます。

マップ アーカイブのエクスポート

Cisco Prime Infrastructure からマップアーカイブファイルをエクスポートし、それらを Cisco DNA Center にインポートできます。

ステップ 1 Cisco Prime Infrastructure のユーザー インターフェイスから、**[マップ（Map）]**>**[ワイヤレス マップ（Wireless Maps）]** > **[サイト マップ（新規）（Site Maps (New)）]**を選択します。

ステップ 2 **[エクスポート（Export）]** ドロップダウン リストから **[マップ アーカイブ（Map Archive）]** を選択します。

ステップ 3 [サイトの選択（Select Sites）] ウィンドウで、次のように設定します。マップ アーカイブに含めるマップ情報またはキャリブレーション情報を選択できます。

- マップ情報（Map Information）：アーカイブにマップ情報を含めるには、[On] または [Off] ボタンをクリックします。
- キャリブレーション情報（Calibration Information）：キャリブレーション情報をエクスポートするには、[On] または [Off] ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] オプション ボタンか、または [すべてのキャリブレーション情報（All Calibration Information）] オプション ボタンをクリックします。[選択したマップのキャリブレーション情報（Calibration Information for selected maps）] を選択すると、選択したサイト マップのキャリブレーション情報がエクスポートされます。[すべてのキャリブレーション情報（All Calibration Information）] を選択すると、選択したマップとともに、システムで使用可能なその他のキャリブレーション情報もエクスポートされます。
- 左側のペインの [サイト（Sites）] で、エクスポートするサイト、キャンパス、ビルディング フロア、または屋外領域の 1 つ以上のチェックボックスをオンにします。すべてのマップをエクスポートするには、[Select All] チェックボックスをオンにします。

ステップ 4 [マップアーカイブを生成（Generate Map Archive）] をクリックします。「データをエクスポートしています（`Exporting data is in progress`）」というメッセージが表示されます。

結果：tar ファイルが作成され、ローカルマシンに保存されます。

ステップ 5 [Done] をクリックします。

ネットワーク階層の検索

ネットワーク階層を検索し、サイト、ビルディング、またはエリアをすばやく見つけることができます。これは、多くのサイトやエリア、ビルディングを追加した後に特に役立ちます。

ツリー階層を検索するには、左ペインの **[階層の検索（Find Hierarchy）]** で、検索するサイト、ビルディング、フロア名の名称の一部または正式名称をのどちらかを入力します。

結果：ツリー階層が、検索フィールドに入力したテキストに基づいてフィルタ処理されます。

サイトの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Edit Area] を選択します。
ステップ 3 [Edit Area] ポップアップで、必要な編集を行います。
ステップ 4 [Update] をクリックして変更を保存します。

サイトの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Delete Area] を選択します。
ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

ビルディングの編集

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Edit Building] を選択します。
ステップ 3 [Edit Building] ポップアップで、必要な編集を行います。
ステップ 4 [Update] をクリックして変更を保存します。

ビルディングの削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。
ステップ 2 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Delete Building] を選択します。
ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

（注） ビルディングを削除すると、そのコンテナ マップもすべて削除されます。AP は、削除されたマップから未割り当ての状態に移動します。

フロアの編集

フロアを追加したら、フロア上にある障害物、エリア、および AP が含まれるようにフロアマップを編集できます。

ステップ 1 [Menu] アイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**の順に選択します。
ステップ 2 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせて、[Edit Floor] を選択します。
ステップ 3 [Edit Floor] ポップアップで、必要な変更を行います。
ステップ 4 [Update] をクリックして変更を保存します。

2D でのフロアマップのモニタリング

[Floor View] ナビゲーションウィンドウでは、次のような複数のマップ機能にアクセスできます。

- フロア マップ ウィンドウの右上隅にある [Find] 機能を使用して、AP、センサー、クライアントなど特定のフロア要素を検索します。検索基準に一致する要素は、右側のペインでテーブルとともにフロアマップに表示されます。マウスをテーブルの上に置くと、フロアマップ上の検索要素が接続線で示されます。
- フロア マップ ウィンドウの右上隅にある ⋮ アイコンをクリックして、次の作業を行います。
  - フロア プランを PDF としてエクスポートします。
  - フロア マップで距離を測定します。
  - スケールを設定してフロア面積を変更します。
- フロア マップ ウィンドウの右下隅にある ⊕ アイコンをクリックして、場所をズームインします。ズームレベルは画像の解像度によって異なります。高解像度画像では、より高いズーム レベルを使用できます。各ズーム レベルはさまざまなスケールで表示される各種スタイルマップで構成されていて、対応する詳細が表示されます。マップの中にはスケールを小さくしても大きくしても同じ状態のマップもあります。
- ⊖ アイコンをクリックすると、広範囲のマップが表示されます。
- ⓘ アイコンをクリックすると、マップ アイコンの凡例が表示されます。

フロアマップの要素とオーバーレイの編集

フロアマップを表示しているときに、マップツールバーの [Add/Edit] をクリックして編集モードに入ります。編集モードでは、次のことができます。

次のデバイスを追加、配置、および削除します。 • アクセス ポイント（Access Points） • Sensor
次のオーバーレイ オブジェクトを追加、編集、および削除します。 • カバレッジ エリア • Location Regions • 壁 • 棚 • マーカー • GPS マーカー

アクセス ポイントの配置に関するガイドライン

フロア マップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿って AP を設置します。このようなカバレッジ領域の中心に設置された AP からは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関しても有益なデータが得られます。
- AP 全体の密度を高め、AP をカバレッジ エリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイス ロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。
- フロアマップでのヒートマップの表示を最適化するには、AP の高さを約 10 フィート （3 m）以下に設定します。

AP の追加、配置、および削除

Cisco DNA Center Cisco DNA Center によって、カバレッジエリアの無線周波数（RF）信号の相対強度を表示する全体マップのヒートマップが計算されます。2D ワイヤレスマップの場合、このヒートマップは実際の RF 信号強度の近似値にすぎません。信号に影響を与える RF 信号の反射やその他の影響が考慮されていないためです。

始める前に

インベントリにシスコの AP があることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して AP を検出します。「ディスカバリについて」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインでビルディングのフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから [AP] トグルが有効になっていることを確認します。

ステップ 5 マップの左側のペインで、[Add APs] をクリックします。

ステップ 6 [Add Aps] スライドインペインから、アクセスポイントのチェックボックスをオンにして AP を一括で選択し、[Add Selected] をクリックします。または、アクセスポイントの横にある [Add] をクリックします。

（注） 使用可能な検索オプションを使用して、アクセスポイントを検索できます。[フィルタ（Filter）] フィールドを使用し、AP 名、MAC アドレス、モデル、シスコ ワイヤレス コントローラのいずれかを使ってアクセスポイントを検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）] をクリックして、フロア領域に 1 つ以上の AP を追加します。

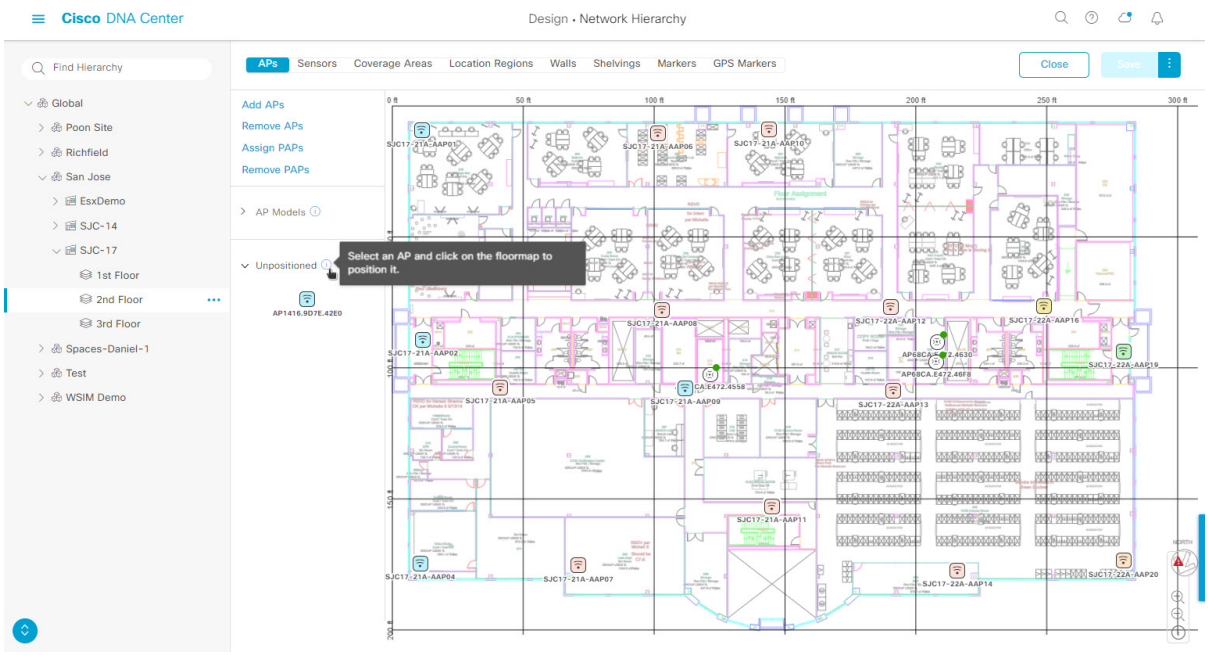
結果：新しく追加された AP は、編集モードのマップの左ペインの [Unpositioned] カテゴリに表示されます。

ステップ 7 フロア領域に AP を割り当てたら、[APの追加（Add APs）] ウィンドウを閉じます。

ステップ 8 マップツールバーから、[Add/Edit] をクリックします。

ステップ 9 マップの左側のペインから、[Unpositioned] カテゴリの AP をクリックして、AP を配置します。

図 *5*：未配置の *AP*



ステップ 10 AP を配置するには、次のいずれかを実行します。

- AP を配置するフロアマップの場所をクリックします。
- [Edit AP] スライドインペインから、対応するフィールドに x 座標と y 座標を入力します。
- フロアマップに 3 つの点を描き、選択した点を使用して AP を配置できます。手順は次のとおりです。

  1. [Edit AP] スライドインペインで、[Position by 3 points] をクリックします。
  2. ポイントを定義するには、フロア マップの任意の場所をクリックして最初のポイントの描画を開始します。ポイントの描画を終了するには、再度をクリックします。最初の点までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[距離の設定（Set Distance）] をクリックします。
  3. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。

- フロアマップに 2 つの壁を定義し、定義した壁の間に AP を配置できます。これによって、2 つの壁の間の AP の位置を把握できるようになります。これは、壁の間の AP の位置を把握するのに役立ちます。

  1. [Edit AP] スライドインペインで、[Position by 2 walls] をクリックします。
  2. 最初の壁を定義するには、フロア マップの任意の場所をクリックして線の描画を開始します。線の描画を終了するには、再度をクリックします。最初の壁までの距離を設定するためにダイアログ ボックスが表示されます。距離をメートル単位で入力し、[Set Distance] をクリックします。
  3. 2 番目の壁を同様の方法で定義し、[保存（Save）] をクリックします。

結果：壁の間の定義された距離に基づいて AP が自動的に配置されます。

ステップ 11 [Edit AP] スライドインペインを使用して、次のような AP の詳細を設定します。

- [AP Name]：AP 名が表示されます。
- [MAC Address]：MAC アドレスが表示されます。
- [AP Model]：選択したアクセスポイントの AP モデルを示します。
- [x]：AP の x 軸座標を示します。値は手動で入力できます。
- [y]：AP の y 軸座標を示します。値は手動で入力できます。
- [AP Height）]：アクセスポイントの高さを示します。値は手動で入力できます。
- [Antenna]：このアクセスポイントのアンテナタイプ。

  （注） 外部の AP の場合は、アンテナを選択する必要があります。選択しないと、AP がマップに表示されません。

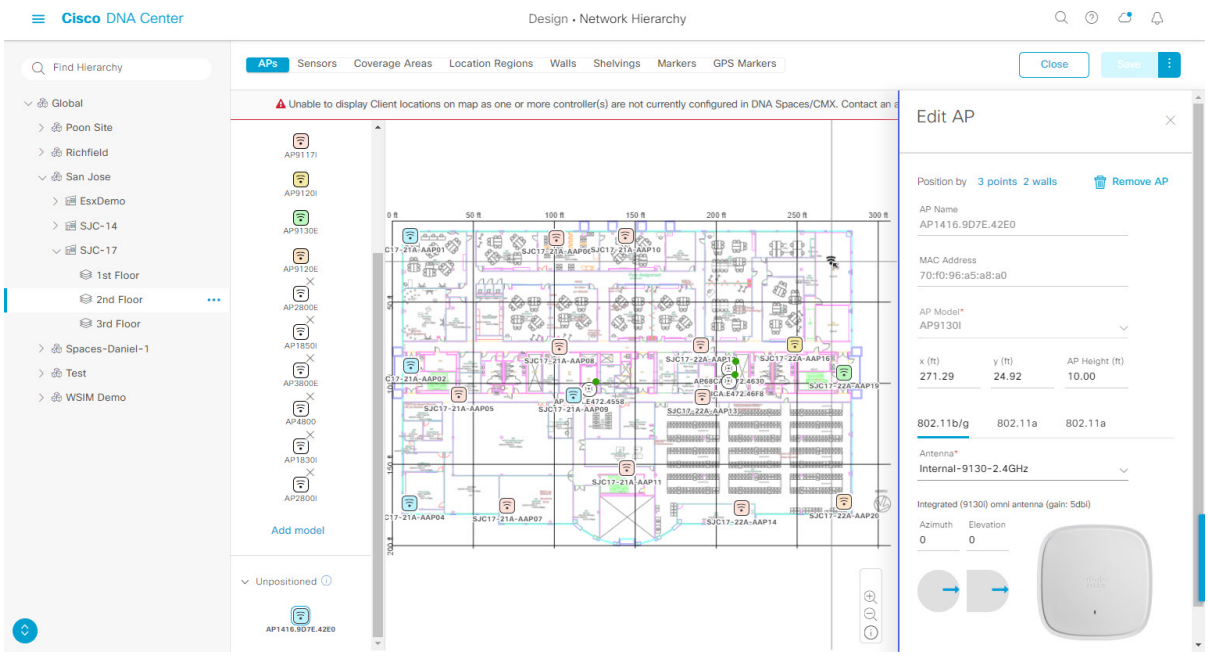
- [Azimuth]：方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Cisco DNA Center では、北は 0 または 360 度で、東は 90 度です。

  値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

  （注） 全方向アンテナのパターンでは方位角が存在しなくなるため、このオプションは表示されません。

- [Elevation]：仰角を度数で表示します。値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。

図 *6 : AP* スライドインペインの編集



ステップ 12 アクセスポイントの配置と設定が完了したら、マップツールバーから [Save] をクリックします。

（注） Cisco Connected Mobile experience（CMX）が Cisco DNA Center と同期されている場合は、ヒートマップ上のクライアントの場所を表示できます。Cisco CMX 設定の作成 （380 ページ）を参照してください。

結果：AP の新しい位置に基づいてヒートマップが生成されます。

ステップ 13 フロアマップから AP を削除するには、編集モードの間に、マップの左側のペインから [Remove APs] をクリックします。

ステップ 14 [Delete APs] スライドインペインから、削除するアクセスポイントの横にあるチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのアクセスポイントを削除するには、[Select All] をクリックし、[Delete Selected] をクリックします。
- フロアからアクセス ポイントを削除するには、[削除（Delete）] アイコンをクリックします。
- [Quick Filter] を使用し、AP 名、MAC アドレス、モデル、コントローラのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果が表に表示されます。[削除（Delete）] アイコンをクリックしてフロア領域から AP を削除します。

AP のクイック ビュー

フロアマップ上の AP アイコンにカーソルを合わせると、AP の詳細、Rx ネイバーの情報、クライアントの情報、およびデバイス 360 の情報が表示されます。

- [Info] をクリックすると、次の AP の詳細が表示されます。
  - [Associated]：AP が関連付けられているかどうかを示します。
  - [Name]：AP 名。
  - [MAC Address]：AP の MAC アドレス。
  - [Model]：AP モデル番号。
  - [Admin/Mode]：AP モードの管理ステータス。
  - [Type]：無線タイプ。
  - [OP/Admin]：動作ステータスおよび AP モード。
  - [Channel]：AP のチャネル番号。
  - [Antenna]：アンテナ名。
  - [Azimuth]：アンテナの方向。
- [Rx Neighbors] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネイバーが接続回線とともに表示されます。また、フロア マップには AP が関連付けられているかどうかも AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコ ワイヤレス コントローラ）の 360 度ビューが表示されます。Cisco DNA Assurance ユーザガイドの「デバイスの健全性のモニターとトラブルシューティング」トピックを参照してください。

（注） デバイス 360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。

センサーの追加、配置、および削除

（注） インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco Aironet 1800s アクティブセンサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。Cisco DNA Assurance ユーザガイドのトピック「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」を参照してください。

センサーデバイスは AP 1800s センサー専用です。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。アシュアランス サーバーに到達可能かどうかの詳細情報を取得してから アシュアランス サーバーと直接通信します。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインでビルディングのフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Sensors] トグルをクリックします。

ステップ 5 [Add Sensors] スライドインペインから、追加するセンサーのチェックボックスをオンにするか、またはセンサー行の横にある [Add] をクリックしてセンサーを追加します。

（注） 検索オプションを使用して、特定のセンサーを検索できます。[Filter] フィールドを使用し、センサーの名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[追加（Add）] をクリックして、フロア領域に 1 つ以上のセンサーを追加します。

結果：新しく追加されたセンサーは、編集モードのマップの左ペインの [Unpositioned] カテゴリに表示されます。

ステップ 6 フロアマップへセンサーを割り当てたら、[Add Sensors] スライドインペインを閉じます。

ステップ 7 マップツールバーから、[Add/Edit] をクリックします。

ステップ 8 マップの左側のペインから、[Unpositioned] カテゴリのセンサーをクリックして、センサーを配置します。

ステップ 9 センサーを配置するフロアマップの場所をクリックします。

- [Sensor Details] スライドインペインの [x]、[y]、および [sensorHeight] フィールドを使用して、センサーの正確な x、y、および z 座標を入力できます。

ステップ 10 センサーの設定と調整が完了したら、[保存（Save）] をクリックします。

ステップ 11 フロアマップからセンサーを削除するには、編集モードの間に、マップの左側のペインから [Remove APs] をクリックします。

ステップ 12 削除するセンサーのチェックボックスをオンにし、[Delete Selected] をクリックします。

- すべてのセンサーを削除するには、[すべて選択（Select All）] をクリックし、[選択済みの削除（Delete Selected）] をクリックします。
- フロアからセンサーを削除するには、そのセンサーの横にある [削除（Delete）] アイコンをクリックします。
- [Quick Filter] を使用して、名前、MAC アドレス、モデルのいずれかで検索します。検索では大文字と小文字は区別されません。検索結果がテーブルに表示されます。[Delete] アイコンをクリックして、フロア領域から 1 つ以上のセンサーを削除します。

カバレッジ エリアの追加

既定では、フロア領域やビルディングマップの一部として定義されている外部エリアが無線カバレッジ エリアと見なされます。

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、マップ エディタを使用してカバレッジ領域または多角形の領域を描画できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインでビルディングのフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Coverage Areas] トグルをクリックします。

ステップ 5 マップの左側のペインから、[Coverage Area] アイコンをクリックします。

ステップ 6 [Coverage Area] ポップアップウィンドウで、フィールドにカバレッジエリアの名前を入力し、[Add Coverage] をクリックします。

ステップ 7 描画ツールを使用して、カバレッジエリアの形状を作成します。

a) マップをクリックしてポイントを作成し、引き続きポイントを作成してカバレッジエリアの形状を定義します。

（注） カバレッジエリアの形状には、少なくとも 3 つのポイントが必要です。

b) 任意のポイントをクリックしてドラッグすると、カバレッジエリアの形状を定義し直すことができます。

c) ダブルクリックして描画ツールを終了し、カバレッジエリアの形状を確定します。

ステップ 8 カバレッジエリアの作成が完了したら、マップツールバーの [Save] をクリックします。

ステップ 9 カバレッジエリアを編集するには、次の手順を実行します。

a) マップツールバーから、[Add/Edit] をクリックします。

b) マップツールバーから、[Coverage Areas] トグルをクリックします。

c) カバレッジエリアのポイントをクリックしてドラッグすると、形状を定義し直すことができます。

d) カバレッジエリアの名前を編集するには、カバレッジエリアを右クリックして [Edit] を選択します。

e) 編集が完了したら、マップツールバーの [Save] をクリックします。

ステップ 10 カバレッジエリアを削除するには、次の手順を実行します。

a) マップツールバーから、[Add/Edit] をクリックします。

b) マップツールバーから、[Coverage Areas] トグルをクリックします。

c) カバレッジエリアを右クリックし、[Delete] を選択します。

d) 削除が完了したら、マップツールバーの [Save] をクリックします。

障害物の作成

アクセス ポイントの RF 予測ヒートマップを計算する際に考慮するための障害を作成することができます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 [Obstacles] の横にある [Overlays] パネルで、[Add] をクリックします。

ステップ 5 [Obstacle Creation] ダイアログ ボックスで、[Obstacle Type] ドロップダウン リストから障害のタイプを選択します。作成可能な障害のタイプは、[Thick Wall]、[Light Wall]、[Heavy Door]、[Light Door]、[Cubicle]、および [Glass] です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。

ステップ 6 [Add Obstacle] をクリックします。

ステップ 7 障害物を作成する領域に描画ツールを移動します。

ステップ 8 描画ツールをクリックして、描線を開始および停止します。

ステップ 9 エリアの輪郭を描画したら、そのエリアをダブルクリックして強調表示します。

ステップ 10 [Obstacle Creation] ウィンドウで [Done] をクリックします。

ステップ 11 [Save] をクリックして、障害をフロア マップに保存します。

ステップ 12 障害を編集するには、[Obstacles] の隣にある [Overlays] パネルで、[Edit] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 13 変更が完了したら、[Save] をクリックします。

ステップ 14 障害を削除するには、[Obstacles] の隣にある [Overlays] パネルで、[Delete] をクリックします。

すべての使用可能な障害物がマップ上で強調表示されます。

ステップ 15 障害にマウス カーソルを合わせ、クリックして削除します。

ステップ 16 [Save] をクリックします。

ロケーション リージョンの作成

包含領域および除外領域を作成して、フロア上のロケーション計算の精度をさらに高めることができます。計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

フロア マップ上に包含領域と除外領域を配置するためのガイドライン

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。
- フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロア領域が作成されるときに、各フロア領域に対して包含領域が定義されます。包含領域は、水色の実線で示され、通常はフロア領域全体の輪郭を描きます。
- フロア領域に複数の除外領域を定義することができます。

フロア上の包含リージョンの定義

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで建物のフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Location Regions] トグルをクリックします。

ステップ 5 マップの左側のペインから、[Inclusion] アイコンをクリックします。

ステップ 6 描画ツールを使用して包含領域を作成します。

- マップをクリックしてポイントを作成し、包含領域の形状ができるまでポイントの作成を続けます。
- 形状を完成させるには、左側のペインで [Inclusion] アイコンをクリックして、描画モードを終了します。または、マップをダブルクリックして形状を確定することもできます。形状をキャンセルする場合は、マップ上で右クリックします。
- 既存の包含領域を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の包含領域を削除するには、形状を右クリックして [Delete] を選択します。

ステップ 7 包含領域の作成が完了したら、マップツールバーの [Save] をクリックします。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない領域（除外領域）を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。原則として、除外領域は包含領域の境界内に定義されます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで建物のフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Location Regions] トグルをクリックします。

ステップ 5 マップの左側のペインから、[Exclusion] アイコンをクリックします。

ステップ 6 描画ツールを使用して除外領域を作成します。

- マップをクリックしてポイントを作成し、除外領域の形状ができるまでポイントの作成を続けます。
- 形状を完成させるには、左側のペインで [Exclusion] アイコンをクリックして、描画モードを終了します。または、マップをダブルクリックして形状を確定することもできます。形状をキャンセルする場合は、マップ上で右クリックします。
- 既存の除外領域を移動するには、形状を新しい場所にドラッグアンドドロップします。
- 既存の除外領域を削除するには、形状を右クリックして [Delete] を選択します。

ステップ 7 除外領域の作成が完了したら、マップツールバーの [Save] をクリックします。

ロケーション リージョンの編集

ステップ 1 **[Overlays]** パネルで、**[Location Regions]** の横にある **[Edit]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 必要な変更を行って、**[Save]** をクリックします。

ロケーション リージョンの削除

ステップ 1 **[Overlays]**パネルで、**[Location Regions]** の横にある **[Delete]** をクリックします。
使用可能なロケーション リージョンがマップ上で強調表示されます。

ステップ 2 削除する領域の上にマウスのカーソルを合わせ、**[Delete]** をクリックします。

ステップ 3 [Save] をクリックします。

レールの作成

フロア上にコンベヤベルトを表すレールラインを定義できます。また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算をさらにサポートする領域を定義できます。この領域は、クライアントが表示されると予測される領域を表します。スナップ幅の領域内に配置されたクライアントは、レールライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

スナップ幅領域は、フィートまたはメートル（ユーザー定義）単位で定義され、レールの片側（東および西、または北および南）からモニターされる距離を表します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 中央のペインのフロア プランの上にある [Edit] をクリックします。

ステップ 4 [Rails] の横にある [Overlays] パネルで、[Add] をクリックします。

ステップ 5 レールのスナップ幅（フィートまたはメートル）を入力し、[Add Rail] をクリックします。

描画アイコンが表示されます。

ステップ 6 レール ラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。

ステップ 7 フロア マップ上にレール ラインを描画したら、描画アイコンを 2 回クリックします。レールラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。

ステップ 8 [Save] をクリックします。

ステップ 9 [Overlays] パネルで、[Rails] の横にある [Edit] をクリックします。

使用可能なレールがマップ上で強調表示されます。

ステップ 10 変更を加えて、[Save] をクリックします。

ステップ 11 [Overlays] パネルで、[Rails] の横にある [Delete] をクリックします。

使用可能なすべてのレール ラインがマップ上で強調表示されます。

ステップ 12 削除するレールラインの上にマウスのカーソルを合わせ、[Delete] をクリックします。

ステップ 13 [Save] をクリックします。

マーカーの配置

ステップ 1 メニューアイコン（☰）をクリックして、**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側のペインで建物のフロアをクリックします。

ステップ 3 マップツールバーから、[Add/Edit] をクリックします。

ステップ 4 マップツールバーから、[Markers] トグルをクリックします。

ステップ 5 マーカーの名前を入力し、[Add Marker] をクリックします。

ステップ 6 描画ツールを使用してマーカーを配置します。

- マーカーを配置するにはマップをクリックします。
- マーカーを移動するには、
- 既存のマーカーを編集するには、マーカーを右クリックして [Edit] を選択します。
- 既存のマーカーを削除するには、マーカーを右クリックして [Delete] を選択します。

ステップ 7 マップツールバーの [Save] をクリックします。

フロア ビュー オプション

中央のペインのフロア プランの上にある **[View Options]** をクリックします。フロア マップと [Access Points]、[Sensor]、[Overlay Objects]、[Map Properties]、および [Global Map Properties]の各パネルが右側のペインに表示されます。

フロアマップの外観を変更するには、さまざまなパラメータを選択または選択解除します。たとえば、フロアマップ上のアクセスポイント情報だけを表示する場合は、[Access Point]チェックボックスをオンにします。各パネルを展開して、各フロア要素で使用可能なさまざまな設定を構成できます。

アクセス ポイントの表示オプション

アクセスポイントをマップ上に表示するには、[Access Points] の横にある [On/Off] ボタンをクリックします。[Access Points] パネルを展開して、次の設定を行います。

- [Display Label]：ドロップダウンリストから、AP に関してフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - [None]：選択したアクセスポイントに関してラベルが表示されません。
  - [Name]：AP 名。
  - [AP MAC Address]：AP の MAC アドレス。
  - [Controller IP]：アクセスポイントが接続されているシスコ ワイヤレス コントローラの IP アドレス。
  - [Radio MAC Address]：無線 MAC アドレス。
  - [IP Address]
  - [Channel]：Cisco Radio のチャネル番号または [Unavailable]（アクセスポイントが接続されていない場合）。
  - [Coverage Holes]：クライアントが接続を失うまで信号が弱まったクライアントのパーセンテージ。接続されていないアクセス ポイントについては [Unavailable]、monitor-only モードのアクセス ポイントについては [MonitorOnly] と表示されます。
  - [TX Power]：現在の Cisco Radio の送信電力レベル（1 が高い）または [Unavailable]（アクセスポイントが接続されていない場合）。無線帯域を変更すると、マップ上の情報もそれに応じて変更されます。

    電力レベルはアクセス ポイントのタイプによって異なります。Cisco Aironet 1000 シリーズ Lightweight アクセスポイントは **1** ～ **5** の値を受け入れます。Cisco Aironet 1230AG シリーズアクセスポイントは **1** ～ **7** の値を受け入れます。Cisco Aironet 1240AG シリーズ アクセスポイントおよび Cisco Aironet 1100 シリーズ アクセスポイントは **1** ～ **8** の値を受け入れます。
  - [Channel and Tx Power]：チャネルと送信電力レベルまたは [Unavailable]（アクセスポイントが接続されていない場合）。
  - [Utilization]：関連付けられたクライアントデバイスで使用されている帯域幅のパーセンテージ（受信、送信、およびチャネル使用率を含む）。アソシエーションを解除されたアクセス ポイントでは [Unavailable]、monitor-only モードのアクセス ポイントでは [MonitorOnly] が表示されます。
  - [Tx Utilization]：指定されたインターフェイスの送信（Tx）使用率。
  - [Rx Utilization]：指定されたインターフェイスの受信（Rx）使用率。
  - [Ch Utilization]：指定されたアクセスポイントのチャネル使用率。
  - [Assoc.Clients]：関連付けられたクライアントの総数。
  - [Dual-Band Radios]：Cisco Aironet 2800 および 3800 シリーズ アクセスポイント上の XOR デュアルバンド無線を識別してマークします。
  - [Health Score]：AP の正常性スコア。

- **Issue Count**
- [Coverage Issues]
- [AP Down Issues]

- [Heatmap Type]：ヒートマップは、変数から取得した値をマップに色として表した、無線周波数（RF）ワイヤレスデータのグラフィック表示です。現在のヒートマップは、RSSI 予測モデル、アンテナの方向、および AP 送信電力に基づいて計算されます。[Heatmap Type] ドロップダウンリストからヒートマップのタイプを選択してください。ヒートマップのタイプは次のとおりです。
  - [None]
  - [AP RSSI]：特定の帯域のワイヤレス信号の強度を特定するカバレッジヒートマップ。
    - [RSSI Cut off（dBm）]：スライダをドラッグして RSSI カットオフレベルを設定します。RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
    - [Heatmap Opacity（%）]：スライダを 0 ～ 100 の範囲でドラッグして、ヒートマップの不透明度を設定します。
    - [Heatmap Color Scheme]：緑色はヒートマップカバレッジ状態が良好であることを示し、赤色はヒートマップカバレッジ状態が悪いことを示します。
  - [Client Density]：関連付けられたクライアントの密度。
    - [Map Opacity（%）]：スライダをドラッグしてマップの不透明度を設定します。
  - [IDS]：ワイヤレスクライアントに提供されるモニターモードアクセスポイントカバレッジをフロアマップ上に示すヒートマップ。
  - [Planned Heatmap]：計画ヒートマップは、フロアマップ上の計画アクセスポイントの可能なカバレッジを示す架空のヒートマップです。
  - [Coverage]：モニターモードアクセスポイントが除外されたヒートマップ（モニターモード アクセス ポイントがフロアプラン上にある場合にのみ利用可能）。

AP の詳細はすぐにマップに反映されます。マップ上の AP アイコンにカーソルを合わせると、AP の詳細、RX ネイバーの詳細、クライアントの詳細、およびスイッチの情報が表示されます。

センサーオプションの表示

[Sensors] ボタンをクリックすると、マップ上にセンサーが表示されます。[Sensors] パネルを展開して、次の設定を行います。

- [Display Label]：ドロップダウンリストから、選択したアクセスポイントに関してフロアマップに表示するテキストラベルを選択します。使用可能な表示ラベルは次のとおりです。
  - [None]

- [Name]：センサー名。
- [Sensor MAC Address]：センサーの MAC アドレス。

オーバーレイ オブジェクトの表示オプション

オーバーレイオブジェクト をこれらの設定を構成するパネルに展開します。[On]/[Off] ボタンを使用して、これらのオーバーレイオブジェクトをマップ上に表示します。

- [Coverage Areas]
- [Location Regions]
- [Obstacles]
- [Rails]
- [Markers]

マップ プロパティの設定

[Map Properties] パネルを展開して、以下を構成します。

- [Auto Refresh]：間隔のドロップダウンリストを使用して、データベースからマップデータを更新する頻度を設定できます。[Auto Refresh] ドロップダウンリストから、時間間隔（[None]、[1 min]、[2 mins]、[5 mins]、または [15 mins]）を設定してください。

グローバルマッププロパティの設定

[Global Map Properties] パネルを展開し、次のように設定します。

- [Unit of Measure]：ドロップダウンリストを使用して、マップの寸法測定値を [Feet] または [Meters] のいずれかに設定します。

ネットワーク階層マップでのデバイスデータのフィルタ処理

2D ワイヤレスマップの場合、アクセスポイントやセンサーにさまざまなフィルタを適用できます。開始するには、マップツールバーの [Data] をクリックします。フィルタ条件に基づいて、検索結果がテーブルに表示されます。

インベントリの管理

インベントリ機能は、ホストの IP アドレス、MAC アドレス、およびそのデータベース内のデバイスに関するネットワーク アタッチメント ポイントなどの詳細を取得して保存します。

インベントリについて

インベントリ機能は、ホストの IP アドレス、MAC アドレス、およびそのデータベース内のデバイスに関するネットワーク アタッチメント ポイントなどの詳細を取得して保存します。

また、インベントリ機能は、デバイスの制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（ネットワーク設定がデバイスにまだ存在しない場合）。

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery （このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （21 ページ） を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は6時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最高 24 時間まで変更できます。詳細については、デバイスポーリング間隔の更新（68 ページ）を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイスデータが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

デバイスポーリング間隔の更新

[System] > **[Settings]** > **[Network Resync Interval]** の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 更新するデバイスを選択します。

ステップ 3 [Update Polling Interval] をクリックします

ステップ 4 [Update Resync Interval] ダイアログボックスの [Status] フィールドで、[Enabled] をクリックしてポーリングを有効にするか、[Disabled] をクリックしてポーリングを無効にします。

ステップ 5 [Polling Time] フィールドには、継続的なポーリングサイクルの間隔（分単位）を入力します。有効な値は、25 ～ 1,440 分（24 時間）です。

（注） デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco DNA Center は引き続きデバイス固有のポーリング時間を使用します。

ステップ 6 [更新（Update）] をクリックします。

インベントリに関する情報の表示

[Inventory] テーブルには、検出された各デバイスの情報が表示されます。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

テーブルで表示または非表示にする列を選択するには、 をクリックします。列の選択はセッション間では保持されない点に注意してください。

デバイスを選択し、[Focus] ドロップダウンリストから別のビューを選択すると、選択内容は新しい各ビューに保持されます。

デフォルトでは、[Inventory] テーブルに 25 のエントリが表示されます。追加のエントリを表示するには、[Show More] をクリックします。[Inventory] テーブルには最大 200 のエントリを表示できます。

[Inventory] テーブルに 25 を超えるエントリがあり、[Focus] ドロップダウンリストから別のビューを選択した場合、エントリの数は新しい各ビューで保持されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。次の表に、使用できる情報を記載します。

表 *20* : インベントリ

カラム	説明
Device Name	

カラム	説明
	デバイスの名前。 デバイス名をクリックすると、デバイスの次の詳細が表示されます。 [Details]：デバイス名、到達可能性ステータス、管理性ステータス、IP アドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。 • [View Assurance 360]：[Assurance 360] ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 • **Interfaces** • [Ethernet Ports]（すべてのデバイスが対象）：イーサネットポートの動作ステータスと管理ステータスが表示されます。 Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチとアグリゲーション サービス ルータ（ASR）1000 シリーズ ルータの場合、ポートビューにはラインカードとスーパーバイザカードの詳細が表示されます（使用可能な場合）。 ラインカードには、プラットフォーム、アドレス、シリアル番号、ロール、およびスタックメンバー番号の詳細が含まれます。スーパーバイザカードには、部品番号、シリアル番号、スイッチ番号、およびスロット番号の詳細が含まれます。 [Ports] テーブルには、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、MTU および説明が表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。 • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID Cisco Catalyst 2000、3000、および 9000 シリーズ スイッチの場合は、ポートビューでポートをクリックするか、[Ports] テーブルのポート名をクリックして、ポートの最大割り当て電力、および消費電力の詳細を表示します。 • [Color Code] ドロップダウンリストには、次のビューが用意されています。 • [Status]：イーサネットポートのデフォルトビューを表示します。 • [VLANs]：特定のポートに割り当てられている VLAN を表示します。[VLANs] ビューでは、最大 5 つの VLAN を選択し、ポートに関連付けられている VLAN のみを一覧表示できます。 [VLANs] ビューには、VLAN ポートマッピングの [Selected]、[Not Configured]、[Default]、および [VLAN] カラーコードが表示されま

カラム	説明
	す。 • [Port Channels]：デバイスで設定されている上位 5 つのポートチャネルを表示します。 ポートチャネルビューには、デバイスで設定されているポートチャネルの [Selected] および [Port-channel] カラーコードが表示されます。 • [Port Actions]： • [Clear Mac Address]：ポートの MAC アドレスをクリアできます。ポートビューでポートをクリックします。次に、[Port Actions] ドロップダウンリストから [Clear Mac Address] を選択します。 • [Port Shut]：ポートをシャットダウンできます。ポートビューでポートをクリックします。次に、[Port Actions] ドロップダウンリストから [Port Shut] を選択します。警告メッセージには [OK] をクリックします。ポートの管理ステータスが [Down] になります。 ポートの管理ステータスを [Up] にするには、[Port Actions] ドロップダウンリストから [Port No Shut] を選択します。警告メッセージには [OK] をクリックします。 error-disabled ポートは黄色で表示されます。ポートビューで error-disabled ポートをクリックして、エラーの理由を表示します。error-disabled ポートをアクティブにするには、MAC アドレスをクリアして、ポートをシャットダウンします。 • [Port Description]：[PORT DESCRIPTION] の横にある [Edit] アイコンをクリックし、説明を入力して [Save] をクリックし、[Okay] をクリックしてポートに説明を追加します。説明を削除するには、[Delete] アイコンをクリックします。

カラム	説明
	• [Update VLAN]：[VLAN] の横にある編集アイコンをクリックし、[Edit VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。2 つの VLAN が事前設定されているポートの VLAN を更新することはできません。 • VLAN の更新、ポートの説明の追加、MAC アドレスのクリア、およびポートのシャットダウンを行うには、デバイスソフトウェアタイプが IOS/IOS-XE である必要があります。 • ワイヤレスコントローラ（WLC）デバイスでは、VLAN の更新、MAC アドレスのクリア、およびポートのシャットはサポートされていません。 • VLAN の更新、MAC アドレスのクリア、およびポートのシャットは、アクセスポートでのみサポートされます。 • ポートをシャットダウンすると、ポートのトラフィックが中断されます。 • [VLANs]（スイッチとハブのみが対象）：VLAN のテーブルに、動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。 • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID [Search] や [Filter] のオプションをクリックして、目的の VLAN の詳細を表示できます。 • [Virtual Ports]（ワイヤレスデバイス、コントローラ、ルータのみが対象）：ポートのテーブルに、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [Hardware and Software]：デバイスのハードウェアとソフトウェアの詳細が表示されます。 • [Configuration]：**show running-config** コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。 この機能は、アクセスポイント (AP) とワイヤレス コントローラにはサポートされていません。したがって、これらのデバイス タイプの場合は設定データは返されません。

カラム	説明
	• [Power]：デバイスに割り当てられている電力、消費電力、および残りの電力に関する詳細が表示されます。[Power Supplies] テーブルに、動作ステータス、シリアル番号、およびベンダー機器タイプの詳細が表示されます。 • [Fans]：ファンの動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [SFP Modules]：プラットフォーム、シリアル番号、製造元、および Small Form-Factor Pluggable（SFP）モジュールの接続先ポートの詳細を表示します。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。 • [User Defined Fields]：デバイスに関連付けられているユーザー定義フィールドが表示されます。 • [Config Drift]：構成の変更を表示し、同じデバイスの任意の 2 つのバージョンを選択して、各バージョンの実行中の構成データを比較できます。 （注） 実行中の構成データは、ワイヤレスコントローラやレガシーコントローラなどのデバイスではサポートされません。 • [Wireless Info]：プライマリとセカンダリの管理対象ロケーションが表示されます。 • [Mobility]：モビリティグループ名、RF グループ名、仮想 IP、およびモビリティ MAC アドレスが表示されます。 （注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。
IP Address	デバイスの IP アドレス。

カラム	説明
Support Type	以下に示すデバイスのサポートレベルが表示されます。 • [Supported]：Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Unsupported]：Cisco DNA Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party]：デバイスパックは、お客様またはビジネスパートナーによって構築され、認定プロセスを経ています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡する必要があります。
Reachability	以下は、さまざまなステータスのリストです。 • [Reachable]：Cisco DNA Center から SNMP、HTTP（S）、および NETCONF ポーリングを使用してデバイスに到達できます。 • [Ping Reachable]：Cisco DNA Center から ICMP ポーリングを使用してデバイスに到達できます。SNMP、HTTP（S）、および NETCONF ポーリングでは到達できません。 • [Unreachable]：SNMP、HTTP（S）、NETCONF、ICMP のいずれのポーリングでもデバイスに到達できません。
Manageability	デバイスのステータスが次のように示されます。 • [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、NETCONF ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 • [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。
MAC Address	デバイスの MAC アドレス。

カラム	説明
Image Version	デバイスで現在実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。
Serial Number	シスコ デバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している時間。
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。 （注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。 必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。 • **Unknown** • **Access** • **Core** • **Distribution** • **Border Router**
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、ネットワーク階層について （45 ページ）を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号（たとえば、Cisco Catalyst 4500 シリーズスイッチ）。
Resync Interval	デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

カラム	説明
Last Sync Status	デバイス最終検出のスキャン状態。 • [Managed]：デバイスは完全に管理された状態です。 • [Partial Collection Failure]：デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information]（i）アイコンにマウスを合わせます。 • [Unreachable]：デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials]：デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が実行されています。

ネットワーク デバイスの削除

デバイスがまだサイトに追加されていない場合に限り、Cisco DNA Center データベースからデバイスを削除できます。

インベントリからワイヤレスセンサーを削除すると、センサーは工場出荷時のデフォルト状態にリセットされるため、再接続すると現在の構成が採用されます。

始める前に

この手順を実行するには、管理者（ROLE_ADMIN）権限、およびすべてのデバイスへのアクセス権（[RBAC Scope] を [ALL] に設定）が必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 削除するデバイスの横にあるチェックボックスをオンにします。

（注） さらにチェック ボックスをオンにして複数のデバイスを選択できますが、リストの上部にあるチェック ボックスをクリックしてすべてのデバイスを選択できます。

ステップ 3 [Actions] ドロップダウンリストから [Inventory] > [Delete Device] > の順に選択します。

ステップ 4 [Warning] ウィンドウで、[Config Clean-Up] チェックボックスをオンにして、選択したデバイスからネットワーク設定およびテレメトリ設定を削除します。

ステップ 5 [OK] をクリックして、アクションを確認します。

デバイスをサイトに追加する

デバイスをサイトに追加すると、Syslog サーバーおよび SNMP トラップサーバーとして Cisco DNA Center が設定されます。Syslog レベル 2 が有効になり、グローバルテレメトリを設定できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。

ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドイン ペインが表示されます。

ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。

ステップ 6 [Save] をクリックします。

ステップ 7 （任意） 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。

ステップ 8 [**Assign**] をクリックします。

ステップ 9 サイトにデバイスを割り当てるときにデバイスの可制御性が有効になっていると、ワークフローが自動的にトリガーされ、サイトからデバイスにデバイス設定がプッシュされます。
[Focus] ドロップダウンリストから [Provision] を選択し、[Provision Status] 列の [See Details] をクリックします。デバイスの可制御性を有効にしている場合、デバイスにプッシュされる設定が別のウィンドウに表示されます。

Cisco DNA Center 向けの Cisco ISE の設定について

ネットワークでのユーザー認証に Cisco ISE を使用している場合、Cisco DNA Center を設定して Cisco ISE を統合できます。統合することで、ユーザー名やオペレーティングシステムなど、有線クライアントの詳細な情報を参照できます。

Cisco ISE の設定は NCP（ネットワーク制御プラットフォーム）内に一元化されているため、単一の GUI で Cisco ISE を設定できます。Cisco ISE の設定ワークフローは次のとおりです。

1. メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** の順に選択して、Cisco ISE サーバーの詳細を入力します。

2. Cisco ISE サーバーが正常に追加されると、NCP は NDP（ネットワーク データ プラットフォーム）との接続を確立し、pxGrid ノード、キーストア、およびトラストストアファイルの詳細を送信します。
3. NDP は、NCP から受信した設定に基づき、pxGrid セッションを確立します。
4. NCP が pxGrid ノードのフェールオーバーを自動的に検出すると、ペルソナが稼働し、NDP に通信します。
5. ISE 環境に変化があると、NDP は新しい pxGrid アクティブノードと新しい pxGrid セッションを開始します。

認証サーバとポリシー サーバの設定

Cisco DNA Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center および Cisco ISE が統合されていることを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバーで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- Cisco ISE を設定する前に、以下の点を確認してください。
  - Cisco ISE をネットワークに展開していること。サポート対象の Cisco ISE バージョンの詳細については、「Cisco DNA Center のサポート対象デバイス」を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
  - スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

（注） pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合：

- Cisco DNA Center をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

（注） PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

  - 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
  - TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の SAN フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、Cisco Cloud APIC リリースノート [英語] を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address]：ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。
- [Username]：Cisco ISE CLI にログインするために使用するユーザー名。

  （注） このユーザーにはスーパーユーザーの管理権限が必要です。

- [Password]：Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN]：Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。

  （注）
  - Cisco ISE（**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[List]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
  - 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります。

  FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

  hostname.domainname.com

  たとえば、Cisco ISE サーバーの FQDN は ise.cisco.com である可能性があります。

- [Virtual IP Address（es）]：Cisco ISE ポリシーサービスノード（PSN）が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

ステップ 5 [Advanced Settings] をクリックして、設定を構成します。

- [Connect to pxGrid]：pxGrid 接続を有効にするには、このチェックボックスをオンにします。

  Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合（pxGrid クライアントとして Cisco DNA Center システムを認証するために ISE に送信）、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局（CA）によって生成されていること（そうでない場合、pxGrid 認証は失敗します）。
- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。

- [Protocol]：[TACACS] と [RADIUS]（デフォルト）。両方のプロトコルを選択できます。

  注目 ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design]** > **[Network Settings]** > **[Network]**で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- [Authentication Port]：AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port]：AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port]：デフォルトの TACACS ポートは 49 です。
- [Retries]：接続の試行が中止される前に、Cisco DNA Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- [Timeout]：接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

（注） 必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Cisco DNA Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、次のように [Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「進行中」
- [System 360] ウィンドウ：「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「アクティブ」
- [System 360] ウィンドウ：「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により [FAILED] と表示されている場合は、[Retry] をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

テレメトリを使用したSyslog、SNMPトラップ、NetFlowコレクタサーバー、および有線クライアントデータ収集の設定

Cisco DNA Center では、デバイスを特定のサイトに割り当てる際のグローバルネットワーク設定を構成できます。テレメトリを使用すると、ネットワークデバイスがポーリングされ、SNMP サーバー、syslog サーバー、NetFlow コレクタ、または有線クライアントの設定に従ってテレメトリデータが収集されます。

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『ネットワーク階層のサイトの作成（46 ページ）』を参照してください。

ステップ 1 [Design] > [Network Settings] > [Telemetry] の順に選択します。メニューアイコン（☰）をクリックして、

ステップ 2 [NMP Traps] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Cisco DNA Center as SNMP trap server] チェックボックスをオンにします。

b) [Add an external SNMP trap server] チェックボックスをオンにし、外部 SNMP トラップサーバーの IP アドレスを入力します。

選択したサーバーによってネットワークデバイスから SNMP トラップとメッセージが収集されます。

ステップ 3 [Syslogs] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Use Cisco DNA Center as syslog server] チェックボックスをオンにします。

b) [Add an external syslog server] チェックボックスをオンにし、外部 syslog サーバーの IP アドレスを入力します。

ステップ 4 [NetFlow] 領域が表示されていない場合は展開し、次のいずれかを実行します。

a) [Use Cisco DNA Center as NetFlow collector server] チェックボックスをオンにします。

デバイスインターフェイスの NetFlow の構成は、デバイスでアプリケーションテレメトリを有効にした場合にのみ完了します。NetFlow の宛先サーバーをデバイスに設定するには、サイトレベルで NetFlow コレクタを選択します。

b) [Add an external NetFlow collector server] チェックボックスをオンにし、NetFlow コレクタサーバーの IP アドレスとポート番号を入力します。

選択したサーバーがネットワークデバイスからの NetFlow エクスポートの宛先サーバーになります。NetFlow コレクタが選択されていない場合、アプリケーションテレメトリは有効になりません。

ステップ 5 [Wired Client Data Collection] 領域を展開し、[Monitor wired clients] チェックボックスをオンにします。

この選択により、サイトのアクセスデバイスで IP デバイストラッキング（IPDT）がオンになります。

デフォルトでは、サイトの IPDT は無効になっています。

注：CLI 構成をプレビューするには、IPDT を有効にする必要があります。デバイスをプロビジョニングする場合、デバイスに展開する前に CLI 構成をプレビューできます。

ステップ 6 [Wireless Controller, Access Point and Wireless Clients Health] 領域を展開し、[Enable Wireless Telemetry] チェックボックスをオンにします。

オンにすると、ネットワークのワイヤレスコントローラ、アクセスポイント、およびワイヤレスクライアントの正常性をモニターできます。

ステップ 7 [Save] をクリックします。

Cisco AI Network Analytics データ収集の設定

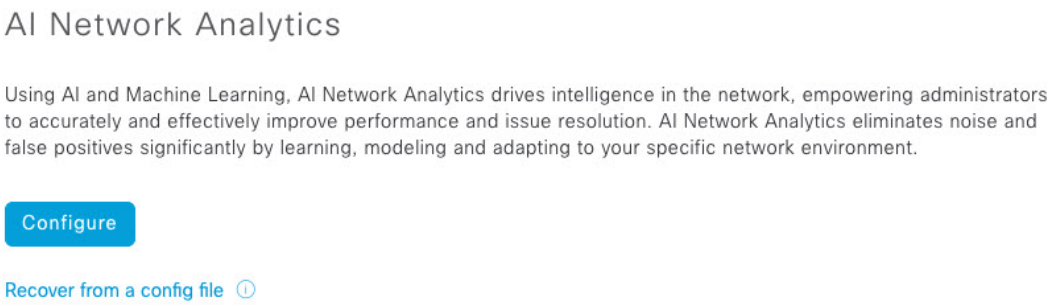
Cisco AI Network Analytics が、ワイヤレスコントローラおよびサイト階層から Cisco DNA Center にネットワークイベントデータをエクスポートできるようにするには、次の手順を実行します。

始める前に

- Cisco DNA Center 用の Cisco DNA Advantage ソフトウェアライセンスを保有していることを確認してください。**AI ネットワーク分析** アプリケーションは、Cisco DNA Advantage ソフトウェアライセンスに含まれています。
- **AI ネットワーク分析** アプリケーションがダウンロードおよびインストールされていることを確認します。Cisco Digital Network Architecture Center 管理者ガイドの「パッケージと更新のダウンロードとインストール」のトピックを参照してください。
- ネットワークまたは HTTP プロキシが、次のクラウドホストへのアウトバウンド HTTPS（TCP 443）アクセスを許可するように設定されていることを確認します。
  - [api.use1.prd.kairos.ciscolabs.com]（米国東部地域）
  - [api.euc1.prd.kairos.ciscolabs.com]（EU 中央地域）

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
[**AI ネットワーク分析**] ウィンドウが表示されます。



ステップ 3 次のいずれかを実行します。

- アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。

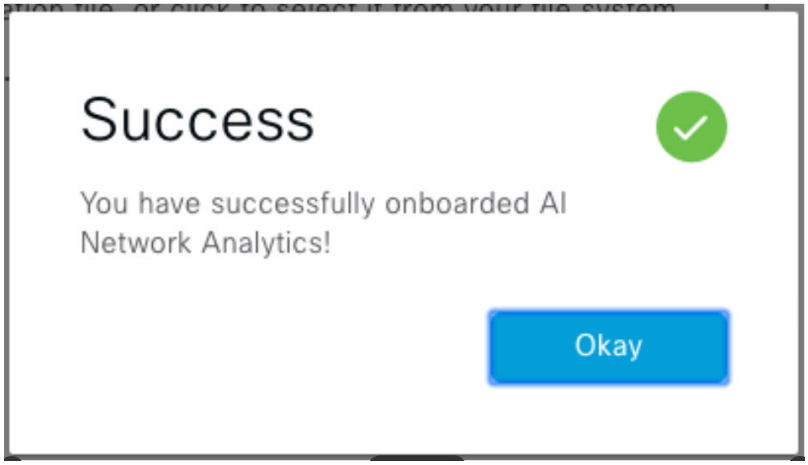
  1. [Recover from a config file] をクリックします。

     [Restore AI ネットワーク分析] ウィンドウが表示されます。

  2. 表示されたエリアにコンフィギュレーション ファイルをドラッグアンドドロップするか、ファイルシステムからファイルを選択します。

  3. [Restore] をクリックします。

     Cisco AI Network Analytics の復元には数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。



- Cisco AI Network Analytics を初めて設定する場合は、次の手順を実行します。

  1. [Configure] をクリックします。

  2. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。

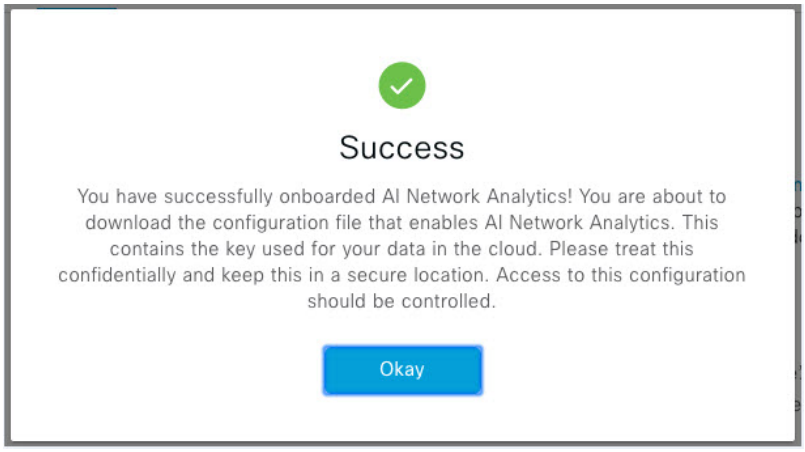
[Testing cloud connectivity...] タブで示されているように、システムはクラウド接続のテストを開始します。クラウド接続のテストが完了すると、[Testing cloud connectivity...] タブが [Cloud connection verified] に変わります。

3. **[次へ (Next)]** をクリックします。

   [terms and conditions] ウィンドウが表示されます。

4. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。

   Cisco AI Network Analytics が有効になるまでに数分かかる場合があり、その後、[Success] ダイアログボックスが表示されます。



ステップ 4 [Success] ダイアログボックスで [Okay] をクリックします。
AI ネットワーク分析 ウィンドウが表示され、[Cloud Connection] エリアに が表示されます。

ステップ 5 （推奨）**AI ネットワーク分析** ウィンドウで、[Download Configuration] ファイルをクリックします。

Cisco AI Network Analytics データ収集の無効化

Cisco AI Network Analytics データ収集を無効にするには、 Cisco AI Network Analytics クラウドサービスへの接続をオフ（無効）にする必要があります。これにより、AI駆動型の問題、ネットワークヒートマップ、サイトの比較、ピアの比較など、Cisco AI Network Analytics 関連のすべての機能が無効になります。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
[**AI ネットワーク分析**] ウィンドウが表示されます。

ステップ 3 [Cloud Connection] エリアで、 が表示されるように、ボタンをクリックしてオフにします。

ステップ 4 [Update] をクリックします。

ステップ 5 Cisco AI Network Analytics クラウドからネットワークデータを削除するには、Cisco Technical Response Center（TAC）に連絡してサポートリクエストをオープンします。

ステップ 6 （オプション）以前の設定が間違って配置されている場合は、[Download configuration file] をクリックします。

機械推論ナレッジベースの更新

機械推論ナレッジパックは、機械推論エンジン（MRE）がセキュリティの問題を特定し、根本原因の自動分析を改善するために使用する、段階的なワークフローです。これらのナレッジパックは、より多くの情報を受信しながら継続的に更新されます。機械推論ナレッジベースは、これらのナレッジパック（ワークフロー）のリポジトリです。最新のナレッジパックにアクセスするために、機械推論ナレッジベースを毎日自動更新するように Cisco DNA Center を設定することもできれば、手動更新を実行することもできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] まで下にスクロールし、[Machine Reasoning Knowledge Base]を選択します。
[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。

- [INSTALLED]：インストールされている機械推論ナレッジベースパッケージのバージョンとインストール日が表示されます。

機械推論ナレッジベースの新しいアップデートがある場合は、[Machine Reasoning Knowledge Base] ウィンドウに [AVAILABLE UPDATE] 領域が表示され、アップデートの [Version] と [Details] が示されます。

- [AUTO UPDATE]：機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。

ステップ 3 （推奨）[AUTO UPDATE] チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。
[Next Attempt] 領域に、次回の更新の日付と時刻が表示されます。

自動更新は、Cisco DNA Center がクラウドの機械推論エンジンに正常に接続されている場合にのみ実行できます。

ステップ 4 機械推論ナレッジベースを Cisco DNA Center で手動で更新するには 、次のいずれかを実行します。

- [AVAILABLE UPDATES] の下にある [Update] をクリックします。[Success] ポップアップウィンドウが表示され、更新のステータスが表示されます。
- 機械推論ナレッジベースをローカルマシンに手動でダウンロードして Cisco DNA Center にインポートします。次の手順を実行します。

  1. [Download] をクリックします。

     [Opening mre_workflow_signed] ダイアログボックスが表示されます。

2. ダウンロードしたファイルを開くか、ローカルマシンの目的の場所に保存して、[OK] をクリックします。
3. [Import] をクリックして、ダウンロードした機械推論ナレッジベースをローカルマシンから Cisco DNA Center にインポートします。

ローカリゼーションの有効化

Cisco DNA Center の GUI 画面は、英語（デフォルト）、中国語、日本語または韓国語で表示できます。

デフォルトの言語を変更するには、次のタスクを実行します。

ステップ 1 ブラウザで、サポートされている言語（中国語、日本語、または韓国語）のいずれかにロケールを変更します。

- Google Chrome から、次の手順を実行します。

1. 右上隅にある ⋮ アイコンをクリックし、[Settings] を選択します。
2. 下にスクロールして [Advanced] をクリックします。
3. **[Languages]** > **[Language]** ドロップダウンリストから、[Add languages] を選択します。

   [Add languages] ポップアップウィンドウが表示されます。
4. [Chinese]、[Japanese]、または [Korean] を選択して、[Add] をクリックします。

- Mozilla Firefox から、次の手順を実行します。

1. 右上隅にある ☰ アイコンをクリックし、[Options] を選択します。
2. **[Language and Appearance]** > **[Language]** エリアから、[Search for more languages] を選択します。

   [Firefox Language Settings] ポップアップウィンドウが表示されます。
3. [Select a language to add] ドロップダウンリストから、[Chinese]、[Japanese]、または [Korean] を選択します。
4. [OK] をクリックします。

ステップ 2 Cisco DNA Center にログインします。

GUI 画面は、選択した言語で表示されます。

図 7: ローカライズされたログイン画面の例

ロールベース アクセス コントロールのサポート アシュアランス

アシュアランス は、ロールベース アクセス コントロール（RBAC）をサポートしています。これにより、スーパー管理者ロールの権限を持つユーザーは、特定の アシュアランス 機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

詳細については、『*Cisco DNA Center* 管理者ガイド』の「Manage Users」の章を参照してください。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、次の手順を実行します。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。

ステップ 1 カスタムロールを定義します。

a) メニューアイコン（☰）をクリックして、**[System]** > **[Users and Roles]** > **[Role Based Access Control]** の順に選択します。

b) [+ Create New Role] をクリックします。

[Create a Role] ウィンドウが表示されます。新しいロールを作成すると、新しいロールにユーザーを割り当てるように求められます。

c) [Let's Do it] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Create a New Role] ウィンドウが表示されます。

d) ロール名を入力し、[Next] をクリックします。
[Define the Access] ウィンドウにオプションのリストが表示されます。

e) リストを展開するには、**アシュアランス** の横にある [>] をクリックします。

次のオプションが表示されます。このオプションを使用して、新しいロールに対して [Deny]、[Read]（デフォルト）、[Write] 権限を設定できます。

- [Monitor and Troubleshooting]：[Health]、[Issues]、[Sensors] ダッシュボードを使用してネットワークをモニターできます。また、360 度ビューや問題の詳細からトレンドを分析し、洞察を得ることができます。

  権限レベルを [Deny] に設定すると、このロールを割り当てられたユーザーは、アシュアランス のどの機能も表示できません。

- [Monitoring Settings]：データの保持と正常性の設定を管理できます。

  データ保持の設定を管理するには、システム権限が必要です。

- [Troubleshooting Tools]：センサーテストを作成およびスケジュールし、インテリジェントキャプチャの設定を管理できます。

f) [Next] をクリックします。
[Summary] ウィンドウが表示されます。

g) サマリーを確認します。情報が正しい場合は、[Create Role] をクリックします。誤りがある場合は、[Edit] をクリックして適切な変更を行います。
[Done, Role-Name] ウィンドウが表示されます。

ステップ 2 作成したカスタムロールにユーザーを割り当てるには、[Add Users] をクリックします。

[User Management] > **[Internal Users]**] ウィンドウが表示されます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。

  1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザーの横にあるオプションボタンをクリックし、次に [Edit] をクリックします。

     [Update Internal User] スライドインペインが表示されます。

  2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。

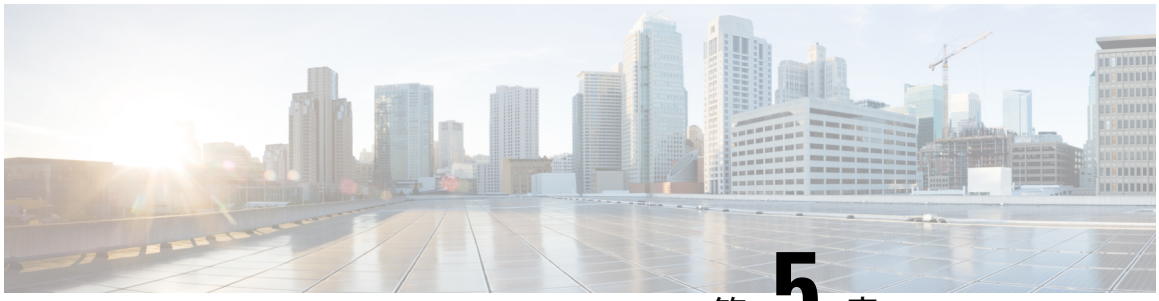
- カスタムロールを新規ユーザーに割り当てるには、次の手順を実行します。

  1. **[+ Add]** をクリックします。

[Create Internal User] スライドインペインが表示されます。

2. 表示されるフィールドに氏名とユーザー名を入力します。
3. [Role List] ドロップダウンリストから、新規ユーザーに割り当てるカスタムロールを選択します。
4. 新しいパスワードを入力し、確認のために再度入力します。
5. [Save] をクリックします。

ステップ 3 既存のユーザーがログイン中に、管理者がそのユーザーのアクセス権限を変更した場合、新しい権限設定を有効にするには、ユーザーが Cisco DNA Center からログアウトして、ログインし直す必要があります。



第 5 章

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

ネットワークについて

ネットワークは、ルータ、スイッチ、ワイヤレス コントローラ、アクセス ポイントを含む、1 つまたは複数のデバイスで構成されています。

ネットワークの健全性のモニターとトラブルシューティング

この手順を使用してネットワークの概要を把握して、対処する必要がある潜在的な問題があるかどうかを判断します。

ネットワークは、ルータ、スイッチ、ワイヤレス コントローラ、アクセス ポイントを含む、1 つまたは複数のデバイスで構成されています。

（注） ネットワークの正常性スコアは、場所のみに基づいて計算されます。デバイスの場所が不明な場合、そのデバイスはネットワーク ヘルス スコアに考慮されません。

始める前に

アシュアランスを設定します。「基本的な設定のワークフロー （17 ページ）」を参照してください。

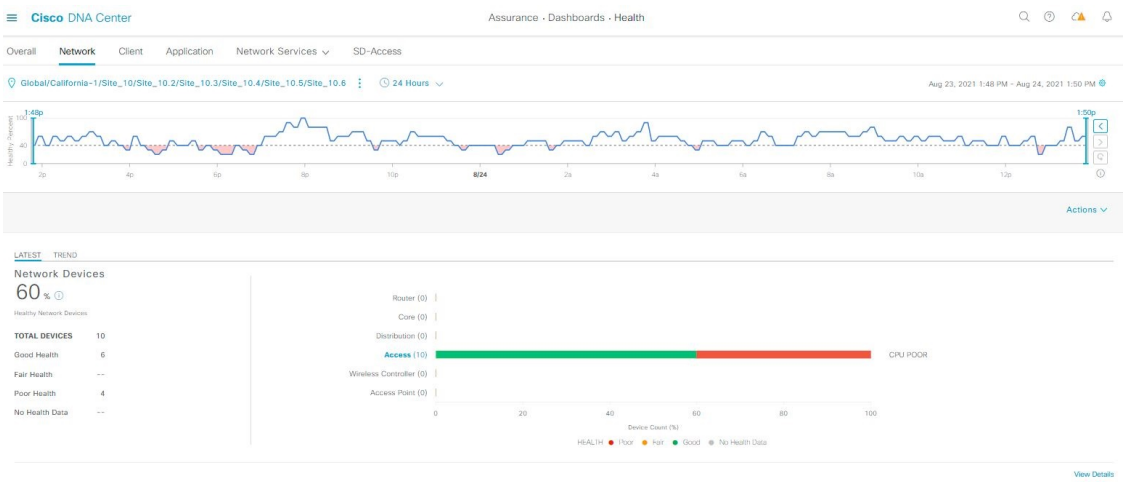
ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network] タブをクリックします。

[Network health] ダッシュボードが表示されます。

図 *8 : [Network Health]* ダッシュボード



ステップ 3 上部のメニューバーで場所オプション（ Global ）をクリックして、サイト階層からサイト、建物、またはフロアを選択します。

ステップ 4 ロケーションアイコンの横にある ⋮ をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。

ロケーションペインには、次の機能があります。

ロケーションオプション	
アイテム	**説明**
 トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。 ドロップダウンリストをクリックして、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [Building View]：リストをビルディングレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。
 トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。
	[Hide Sites] アイコンをクリックして、サイトテーブルを非表示にします。
 **トポロジ**ツール	このアイコンをクリックすると、次のビューがある [Topology] ウィンドウが開きます。 • [Geographical View]：このトグルボタンをクリックすると、ネットワークが地理的マップで表示されます。  ロケーションにカーソルを合わせると、正常なデバイスの割合が表示されます。 •  [Topology View]：このトグルボタンをクリックすると、ネットワークにおけるコンポーネントの接続状況を示すトポロジが表示されます。 デバイスにカーソルを重ねると、デバイスロール、IP アドレス、ソフトウェアバージョンなどのデバイス情報が表示されます。デバイスの 360 度ビューを取得するには、[View Details 360] をクリックします。

ステップ 5 上部のメニューバーにある時間範囲設定（  ）をクリックして、ダッシュボード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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 6 上部のメニューバーにある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- [Export Dashboard]：ネットワークダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ） およびカスタム ダッシュボードの作成 （313 ページ） を参照してください。

ステップ 7 次の機能には、[Network Health] タイムラインを使用します。

より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、ダッシュボードにカスタムチャート用の内容が設定されます。

タイムラインの右側にある矢印ボタンを使用して、最大 30 日間のデータを表示できます。

タイムラインチャート内でカーソルを重ねると、特定の時刻のネットワークデバイスのヘルススコアパーセンテージが表示されます。

点線の横線は、正常なネットワークのしきい値を表します。デフォルトでは、40%に設定されています。

しきい値を変更するには、次の手順を実行します。

1. 情報アイコン（ⓘ）にカーソルを合わせます。
2. ツールチップで、編集アイコン（✎）をクリックします。
3. [Network Health Threshold] スライドインペインで、青色の線をクリックしてドラッグし、しきい値のパーセンテージを設定します。
4. [Save] をクリックします。

（注） [Network Device Summary] の [Health Score] が赤色で表示されている場合、カスタムしきい値を変更すると、結果が変わります。カスタムしきい値によって、正常または異常なデバイスの数が変わることはありません。

ステップ 8 次の機能には、[Network Devices Health Summary] ダッシュレットを使用します。

[Network Device Health Summary] ダッシュレット	
アイテム	説明
[Network Device Health Summary] エリア	

[Network Device Health Summary] ダッシュレット	
アイテム	説明
	次のタブが含まれます。 • [Latest]：デフォルトで表示されます。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • **ネットワーク正常性概要スコア**：ネットワークの正常性の概要スコアは、ネットワーク全体または選択したサイトにおける正常（良好）なデバイスの割合です。ネットワーク ヘルス スコア （124 ページ） を参照してください。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数が表示されます。 • [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間の各デバイスカテゴリ（アクセス、コア、ディストリビューション、ルータ、ワイヤレスコントローラ、アクセスポイント）のパフォーマンスを示します。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスのヘルス スコアと数が表示されます。 チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。たとえば、リンクエラー、高い CPU 使用率、高いメモリ使用率、高ノイズ、低い電波品質などがあります。 ハイパーリンク付きのデバイスカテゴリ（[Access]、[Core]、[Distribution]、[Router]、[Wireless Controller]、[Access Point]）をクリックして、スライドインペインに追加の詳細情報を表示できます。 • **トレンド**：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 で

[Network Device Health Summary] ダッシュレット	
アイテム	説明
	す。 ●：正常性データなし。ヘルス スコアは 0 です。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 9 [AP] ダッシュレットを使用して、次の情報を確認できます。

[Total APs Up/Down] ダッシュレット
次の AP のステータス情報（ネットワークに接続している AP の数とネットワークに接続されていない AP の数）を示す、色分けされたチャート。 [Latest] タブには、5 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

[Top N APs by Client Count] ダッシュレット
最も多くのクライアントを持つ AP に関する情報を示すチャート。 [Latest] タブには、5 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

高干渉の上位 N の AP ダッシュレット
高干渉の AP に関する情報。2.4 GHz または 5 GHz を選択できます。 [Latest] タブには、5 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 10 次の機能には、[Network Devices] ダッシュレットを使用します。

[Networks Devices] ダッシュレット	
アイテム	**説明**
[Type]	[All]、[Access]、[Core]、[Distribution]、[Router]、[WLC]、および [AP] の各オプションを使用して、デバイスタイプに基づいてテーブルをフィルタリングします。 SDA ファブリックドメインの場合、オプション（[All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric WLC]、[Fabric AP]、[Extended Node]）を使用して、ファブリックタイプに基づいてテーブルをフィルタ処理します。
全体的な正常性	次のオプションを使用して、デバイスの全体的な正常性スコアに基づいてテーブルをフィルタリングします。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。
[Network Devices] テーブル	ネットワーク内のすべてのデバイス、または選択したサイトのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、システムの正常性、データプレーンの接続性、およびコントロールプレーンの接続性の KPI メトリックの最小サブスコアです。 [Overall Health Score] 列で、正常性スコアの上にマウスカーソルを合わせます。デバイスの正常性スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。**デバイスの正常性**は、KPI メトリックの最小サブスコアです（デバイスのタイプに基づく）。ルータおよびスイッチの場合、次の KPI メトリックがあります。システムリソース（メモリ使用率と CPU 使用率）、データプレーン（アップリンクの可用性とリンクエラー）、ファブリック（コントロールプレーン到達可能性）。[Fabric Domain Name]、[Fabric Name]、および [Fabric Role] 列には、ファブリックドメイン名、ファブリック名、およびファブリックロール（エッジ、ボーダー、マップサーバーなど）が表示されます。 [Reachability] 列には、デバイスのステータス（到達可能、アップ、到達不能、再起動など）が表示されます。

[Networks Devices] ダッシュレット	
アイテム	説明
デバイス 360	[Device] 列でデバイスの名前をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。

ステップ 11 [Network Devices Reachability] ダッシュレットを使用して、次の情報を表示します。

[Network Devices Reachability] ダッシュレット
色分けされたチャートには、ルータ、スイッチ、およびワイヤレスコントローラの到達可能性ステータスが表示されます。 • **Reachable** • **Unreachable** [Latest] タブには、5 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインで、タイムラインスライダにカーソルを合わせると、一定期間の到達可能性ステータスを表示できます。ロールとロケーションに基づく上位デバイスの到達可能性ステータス数が、水平バーグラフとしてタイムラインスライダの下に表示されます。 水平バーとして表示されるデータを選択し、[All]、[Access]、[Core]、[Distribution]、[Router]、[WLC] の各オプションを指定すると、到達可能性ステータス、デバイスタイプ、およびロケーションに基づいてテーブルをフィルタ処理できます。

ステップ 12 [WAN Link Utilization] ダッシュレットを使用して、次の情報を確認できます。

[WAN Link Utilization] ダッシュレット
棒グラフには、使用可能な WAN リンクの WAN リンク使用率のみのステータスが表示されます。 [Latest] タブには、[Available] および [Not Available] の WAN リンクの 10 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの要素を選択して、より詳細なデータを表示できます。 タイムラインスライダの下に水平バーとして表示されるデータを選択して、上位の場所、デバイスタイプ、および場所に基づいてテーブルをフィルタ処理できます。

ステップ 13 [WAN Link Availability] ダッシュレットを使用して、次の情報を確認できます。

[WAN Link Availability] ダッシュレット
色分けされたチャートには、ネットワークで使用可能な WAN リンクの情報が表示されます。 [Latest] タブには、使用されている WAN リンクの割合が表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの要素を選択して、より詳細なデータを表示できます。 タイムラインスライダの下に水平バーとして表示されるデータを選択して、上位の場所（リンク数）とデバイスタイプ（リンク数）に基づいてテーブルをフィルタ処理できます。

デバイスの健全性のモニターとトラブルシューティング

この手順を使用して特定のデバイスに関する詳細情報を表示して、対処する必要がある潜在的な問題が存在するかどうかを判断します。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network] タブをクリックします。

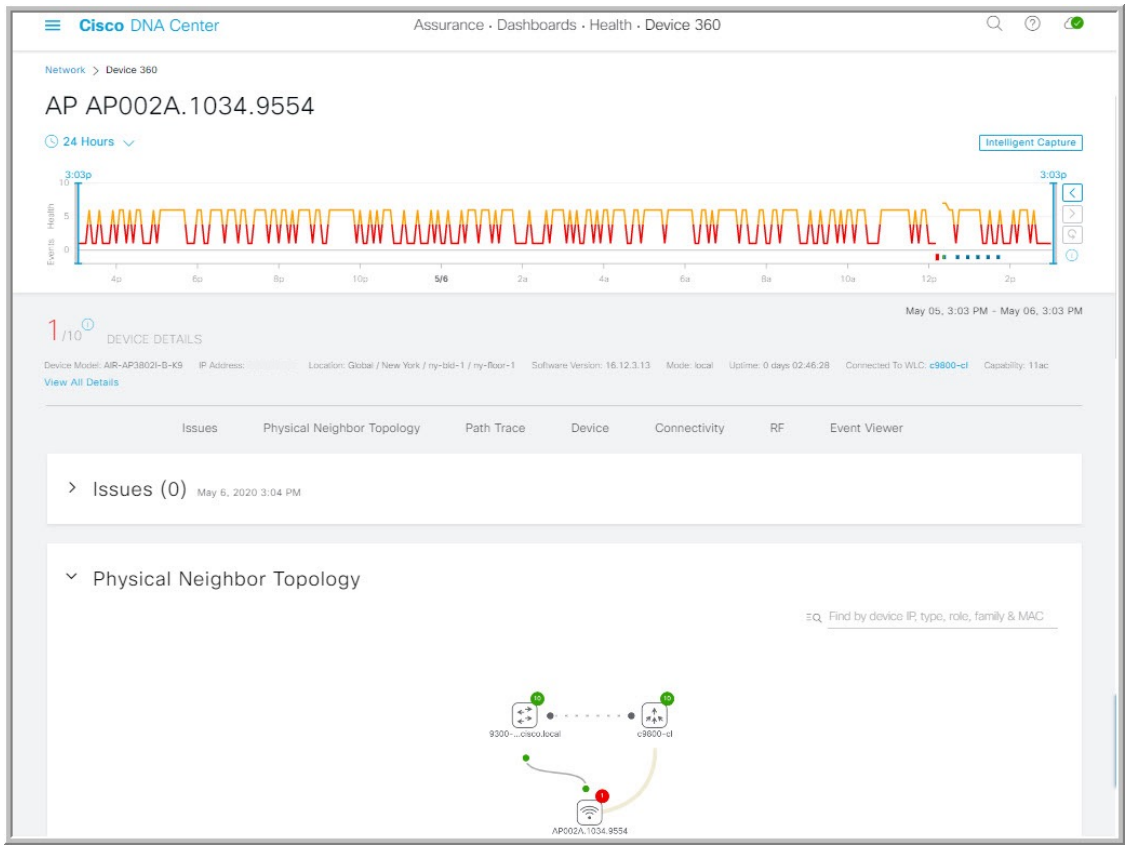
ステップ 3 [Network] 正常性ダッシュボードで、次のいずれかを実行します。

- [Network Devices] ダッシュレットの [Device Name] 列で、デバイス名をクリックします。
- [Search] フィールドで、デバイス名、IP アドレス、または MAC アドレスを入力します。

[Device 360] ウィンドウに、ネットワークデバイスの 360 度ビューが表示されます。

（注）　デフォルトでは [Map View] が表示されます。

図 *9 : [Device 360]* ウィンドウ



ステップ 4　時間範囲設定（ 24 Hours ）をクリックして、ウィンドウに表示され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 5　[Intelligent Capture] をクリックすると、特定のネットワークデバイスのキャプチャされたオンボーディングおよびデータパケットを表示、モニターリング、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。RF統計情報の表示とアクセスポイントのスペクトル解析データの管理 （364 ページ）を参照してください。

（注）　インテリジェント キャプチャはすべての AP モデルでサポートされていません。[Intelligent Capture] が表示されない場合は、AP がサポート対象のモデルであること、また AP が [Network Health] ダッシュボード上の場所に割り当てられていることを確認します。

ステップ 6　タイムラインスライダを使用すると、一定期間のネットワークデバイスに関する正常性およびイベント情報を表示できます。

タイムラインスライダには、次の機能があります。

- [Health]：タイムラインスライダの上にカーソルを合わせると、5 分の時間枠におけるクライアントの正常性スコアと KPI が表示されます。デバイスの正常性スコアは、すべての KPI 正常性スコアの最小値です。

  グラフをダブルクリックすると、1 時間の期間のタイムラインスライダが表示されます。

  （注） 1 時間を超えて情報を表示する場合は、タイムラインスライダを必要な時間範囲に手動で移動します。

  タイムラインをダブルクリックすると、1 時間の期間のタイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。各カテゴリ（[Issues]、[Connectivity] など）の横にあるタイムスタンプも更新されることに注意してください。

- [Events]：イベントデータは、色分けされた垂直バーとしてグラフに表示されます。緑の垂直バーは、成功したイベントを示し、赤の垂直バーは失敗したイベントを示します。

  各垂直バーは、5 分の時間枠を表します。各 5 分間ウィンドウに、複数の重要イベントが生成される場合があります。垂直バーにマウスカーソルを合わせると、イベントに関する詳細情報を取得できます。

ステップ 7 タイムラインの下の [Device Details] 領域で、デバイスの正常性スコアを確認できます。

デバイスの正常性スコアの詳細は次のとおりです。

- [Switch]：スイッチの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、CPU 使用率、リンクエラー、リンク破棄、アップリンクの可用性、コントロールパネルへの到達可能性。また、ファブリックデバイスの場合は、ファブリックの正常性が含まれます。詳細については、「スイッチ ヘルス スコア （125 ページ）」を参照してください。

  （注） [Switches]：アップリンク可用性は、インフラストラクチャのリンクに基づいています。

  [Cisco StackWise Virtual]：アップリンクの可用性は、インフラストラクチャリンク、Cisco StackWise Virtual リンク（SVL）、およびデュアルアクティブ検出（DAD）リンクに基づいています。Cisco StackWise Virtual と制限事項について （116 ページ）を参照してください。

  [Cisco StackWise]：アップリンクの可用性は、インフラストラクチャリンクおよび Cisco StackWise リンクに基づいています。Cisco StackWise と制限事項について （117 ページ）を参照してください。

- [Router]：ルータの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、CPU 使用率、リンクエラー、リンク破棄、アップリンクの可用性、コントロールパネルへの到達可能性。詳細については、「ルータ ヘルス スコア （127 ページ）」を参照してください。

  （注） アップリンクの可用性は、インフラストラクチャリンクに基づいています。

- [AP]：AP の正常性スコアは次のパラメータの最小サブスコアです。メモリ使用率、CPU 使用率、リンクエラー、無線使用率、干渉、ノイズ、電波品質。詳細については、「AP ヘルス スコア （127 ページ）」を参照してください。

- [Wireless Controller]：WLC の正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、空きタイマー、空きメモリバッファ（MBufs）、作業キュー要素（WQE）プール、パケットプー

ル、リンクエラー。ファブリック ワイヤレス コントローラの場合、ファブリックヘルスが含まれます。詳細については、ワイヤレス コントローラのヘルス スコア（129ページ）を参照してください。

ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、データを取得できなかったことを示します。

- ●：重大レベルの問題。ヘルス スコアの範囲は 1 ～ 3 です。
- ●：警告。ヘルス スコアの範囲は 4 ～ 7 です。
- ●：エラーまたは警告はありません。ヘルス スコアの範囲は 8 ～ 10 です。
- ●：使用可能なデータがありません。ヘルス スコアは 0 です。

ステップ 8 タイムラインの下の [Device Details] エリアを使用して、デバイスに関する最新情報を確認できます。これには、デバイスが配置されているビルディングやフロア、デバイスモデル、IP アドレス、デバイスにインストールされているソフトウェアのバージョン、デバイスロール、HA ステータス、IP アドレスまたは MAC アドレス、稼働時間などが含まれます。

（注） [Fabric] の場合、[Fabric Role]、[Fabric Domain]、[Fabric Site]、[System Resources]、[Data Plane]、[Virtual Network]、および [Events] の各要素がデバイス詳細エリアに表示されます。

Cisco StackWise Virtual の場合、[Stack Status: Stackwise Virtual] と [StackWise Virtual Domain] の 2 つの追加要素が表示されます。

[Cisco StackWise] の場合、[StackWise] という追加要素と、[StackWise (2)] のように、スタック内のスイッチ数が表示されます。スタックには最大 8 台のスイッチを設定できます。

PoE 対応デバイスの場合、[IEEE Class]、[Negotiated Power Level]、および [PoE Status] の各要素がデバイス詳細エリアに表示されます。

ステップ 9 [View Details] 領域で [View All Details] をクリックすると、一般的な情報、ネットワーク情報、ラックロケーションなど、デバイスの他の属性を表示するスライドインペインが開きます。

ステップ 10 [Issues] カテゴリを使用して、対処する必要がある問題を確認できます。

問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。

問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。

スライドインペインでは、次の操作を実行できます。

- この問題を解決するには、次の手順を実行します。
  1. ドロップダウンリストから [Resolve] を選択します。
  2. [Resolved Issues] をクリックすると、解決済みの問題が表示されます。
- 問題を無視するには、次の手順を実行します。
  1. ドロップダウンリストから [Ignore] を選択します。
  2. スライダで問題を無視する時間数を設定します。
  3. [Confirm] をクリックします。

4. 無視された問題を表示するには、[Ignored Issues] をクリックします。

ステップ 11 [Physical Neighbor Topology] カテゴリを使用して、デバイスのトポロジと隣接するデバイスへの接続方法を確認できます。

次を実行できます。

- ノードをクリックして、ノードに関する情報が表示されたスライドインペインを表示します。
- 2 つのデバイス間のリンクをクリックすると、その特定のリンクに関する詳細（リンクに対応するポート/インターフェイス、管理ステータス、ポートモードなど）が表示されます。
- リンクエンド（ドット）にカーソルを合わせると、リンクのステータスが表示されます。
- デバイスのグループにカーソルを合わせて [View Devices List] をクリックすると、デバイスのリストとその詳細が表示されます。
- [Onboarding] エリアの [Search] フィールドで、特定のデバイスを検索できます。特定のノードが選択され、デバイスの対応する情報が表示されます。

（注） AP 360 では、2 GHz および 5 GHz のクライアントが表示されます。これら 2 つのクライアントからの点線のリンク回線はクリックできません。また、APからワイヤレスコントローラへのリンク回線とワイヤレスコントローラから AP へのリンク回線はクリックできません。

（注） SD-Accessファブリックの場合、ファブリックグループはファブリックバッジアイコンで表示されます。

（注） Cisco StackWise Virtual および Cisco StackWise には、スタックのアイコン（  ）が表示されます。

Cisco StackWise Virtual または Cisco StackWise が含まれているパスには、パストレースでスイッチのアイコンが表示されます。

ステップ 12 [Event View] カテゴリを使用して、デバイスのイベントの監査証跡を確認できます。イベントビューアテーブルは、イベントが発生したときの理由コードやタイムスタンプなどの問題に関する情報を提供します。イベントをクリックすると、右側のペインにそのイベントに関する詳細情報が表示されます。

- [For APs]：シナリオと、各シナリオにつながる一連のサブイベントが表示されます。これにより、どのサブイベントの間に問題が発生したのかを特定できます。
- [For switches and routers]：クリティカル以上の重大度（致命的およびアラート）を示すすべての syslog、アップ/ダウンしているあらゆるリンクのイベント、到達可能デバイスまたは非到達可能デバイスのイベントが表示されます。また、クリティカルレベルより重大度が低い syslog（エラー、注意、通知、および情報）も表示されます。詳細については、スイッチおよびルータの重大レベルに満たない選択済み Syslog （114 ページ）を参照してください。

ステップ 13 [Path Trace] カテゴリを使用して、パストレースを実行できます。

[Run New Path Trace] をクリックすると、指定した送信元デバイスと接続先デバイス間のネットワークトポロジが表示されます。トポロジには、パスの方向とパスに沿ったデバイスが、その IP アドレスを含めて含まれます。ディスプレイには、パスに沿ったデバイスのプロトコル（**Switched**、**STP**、**ECMP**、**Routed**、**Trace Route**）や、その他のソース タイプも表示されます。

パス トレースの実行 （375 ページ）を参照してください。

ステップ 14 [Application Experience] カテゴリをクリックすると、ネットワークで実行中のアプリケーションが表示されます。

メトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。関連する情報を示すスライドインペインが開きます。

アプリケーション エクスペリエンスとアプリケーションの可視性について （163 ページ）およびホストのアプリケーション エクスペリエンスの表示 （172 ページ）を参照してください。

（注） このカテゴリは、ルータのみに表示されます。

ステップ 15 [Detail Information] カテゴリを使用して、デバイスの KPI の一定期間の履歴を確認できます。

次の各タブをクリックすると、対応する詳細が表示されます。

[Device Info] タブ
デバイスの CPU、メモリ、稼働時間、温度などに関する情報を表示します。 （注） 帯域外で設定されたネットワークデバイスの場合、稼働時間のチャートは正常性スコアやその他のデータと正しく相関しません。たとえば、24 時間ウィンドウの稼働時間のチャートで、午前 11 時 39 分と午後 2 時 40 分にデバイスがダウンしたことが示されていたとします。その場合、午前 11 時 00 分ー 午後 2 時 00 分の 3 時間ウィンドウを選択（タイムラインスライダを使用）しても、ダウンタイムが表示されません。この問題は、Cisco DNA Center がデバイスからシステム稼働時間情報を受信できないために発生します。この問題を回避するには、デバイスと Cisco DNA Center の間で構成を同期させます。

[Connectivity] タブ

デバイスのネットワークとの接続の正常性に関する情報が表示されます。このタブは、AP に対して表示されます。

[Connectivity] タブには、[Radio 0]、[Radio 1]、[Radio 2] のように、無線固有の KPI に対応するタブがあります。適切な無線をクリックして、[Current Channel]、[Extended Channel（s）]、[RF Profile]、[Band]、[Mode]、[Current Channel Width] などの情報を表示します。また、[Traffic]、[Client Count] などのチャートも表示できます。

- [Traffic]：無線のトラフィック（Mbps 単位）が表示されます。Rx（レシーバ）データ パケットと Tx（トランスミッタ）データ パケット（バイト単位）が、色分けされた線でチャートに表示されます。

  グラフの時間インスタンスの上にカーソルを重ねて、特定の日時に送信または受信されたトラフィック量（Rx または Tx）を表示します。

- [Client Count]：無線対応のクライアントの数が表示されます。クライアント数は、チャート上に色分けされた線で表示されます。

  グラフの時間インスタンスの上にカーソルを重ねて、特定の日時に AP に接続されたクライアント数を表示します。

- [Link Error]：インターフェイスに関する情報を表示するには、チャートの右側にあるインターフェイスの横のチェックボックスをオンにします。選択したインターフェイスに基づき、各インターフェイスのエラー割合が、チャート上に色分けされた線で表示されます。

  グラフの時間インスタンスの上にカーソルを重ねて、特定の日時のエラー割合を表示します。最大 5 つのインターフェイスを選択できます。

- [Ethernet Interface KPI]：[Ethernet Interface KPI] には、[GigabitEthernet0] や [GigabitEthernet1] などのインターフェイスが含まれています。適切なインターフェイスをクリックして、[Utilization]、[Error]、および [Rate] のチャートを表示します。また、AP 360 の上部で選択された時間範囲について集計された KPI の合計値と平均値も表示できます。

  （注） スイッチに接続されているインターフェイスには、[Connected Switch] バナーが表示されます。

- [Retries]：無線接続の再試行回数が再試行チャートに表示されます。

  （注） リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレス コントローラ、AP など）を接続するトポロジカルリンクを指します。

[Fabric Site] タブ

このタブは、SD-Access ファブリックで使用できます。

ファブリック KPI は、[Fabric Site Connectivity]、[Fabric Infrastructure] および [Fabric Control Plane] の各カテゴリにグループ化されます。これらのカテゴリに基づいてフィルタ処理して、それぞれの KPI、つまり [CP Reachability]、[LISP Session Status] および [Pub-Sub Session Status for INFRA VN] を表示できます。これらのカテゴリに基づいて、接続先、IP アドレス、タイプなどの到達可能性情報を含むテーブルを表示します。コントロールプレーンの到達可能性ステータス、lisp、および pubsub セッションのステータスチャートを表示するには、接続先の横にあるチェックボックスをオンにします。

（注） アップリンク ステータス チャートには、ファブリックアンダーレイの自動化を使用してファブリックをプロビジョニングする場合にのみデータが表示されます。

[Interfaces] タブ

名前、説明、動作ステータス、リンク速度など、選択したインターフェイスに関する情報が含まれます。

特定のポートタイプに関する情報を表示するには、[PORT TYPE] タブを使用します。表示されるタブは、選択されたデバイスのタイプによって異なります。

- [Switches and Routers]：[All]、[Access]、[Auto]、[Routed]、および [Trunk] ポートタイプを表示します。
- [Cisco StackWise Virtual]：[All]、[Access]、[Auto]、[Routed]、[Trunk]、[SVL]、および [DAD] ポートタイプを表示します。
- [Cisco StackWise]：[All]、[Access]、[Auto]、[Routed]、[Trunk]、および [StackWisePort] ポートタイプを表示します。

テーブルにはソート可能な列が含まれています。ただし、新しいパラメータを使用して列をソートしようとすると、拡張インターフェイスリストが折りたたまれます。

（注） [Link Speed] データの列には、インターフェイスまたは物理ポートの速度容量が表示されます。ポートが特定の速度にネゴシエートされた場合は、ネゴシエートされた速度が表示されます。

特定の日時のインターフェイスに関する動作ステータスをチャート形式で表示するには、インターフェイスの横にあるチェックボックスをオンにします。最大 5 つのインターフェイスを選択できます。デフォルトでは、テーブル内の最初のインターフェイスが選択されます。

[Interface Availability]、[Utilization]、[Error]、および [Link Discard] チャートがテーブルの下に表示されます。

[Tx Utilization] チャートと [Rx Utilization] チャートの値が [Percentage] と [Rate（bps）] に入力されます。[Percentage] と [Rate] を切り替えて使用状況の値を表示できます。

[PoE] タブ

このタブは、PoE 対応スイッチおよび AP で使用できます。

デバイスの Power over Ethernet（PoE）テレメトリを表示します。

スイッチ

[POWER SUMMARY] セクションには、スイッチの全体的な PoE テレメトリが表示されます。

- [Power Budget]：PoE 対応デバイス用にスイッチから割り当てられている合計電力。
- [Used Power]：PoE 対応デバイスにスイッチから供給されている電力。
- [Remaining Power]：PoE 対応デバイスで使用可能な未使用の電力。
- [Power Usage]：PoE 対応デバイスにスイッチから供給されている電力の割合。この値は、[Used Power] の値を [Power Budget] の値で割った値になります。

[Power Stack] セクションには、PoE に接続された電源スタックデバイスが一覧表示され、電源スタック名、スタックモード、スタックトポロジ、割り当てられた電力、消費電力、残りの電力などが示されます。

[Module Power Details] セクションには、PoE に電力を供給するスイッチのコンポーネントのリストが表示されます。

[PoE Interfaces] セクションには、スイッチのインターフェイスに接続されている PoE 対応デバイスが一覧表示されます。セクションの上部に、現在オフになっているインターフェイスの数が表示されます。

このテーブルは次の方法でカスタマイズできます。

- テーブルの上にある [POE CONFIG]、[ADMIN STATUS]、および [POE OPER STATUS（SIGNAL PAIR）] のフィルタを使用して、インターフェイスをフィルタ処理できます。
- 検索バーを使用して、特定のインターフェイス、PoE 対応デバイス、またはその他の値を検索できます。
- ⋮ をクリックするとメニューが開き、特定のデータの種類の列を追加および削除できます。

AP

[Detail Information] セクションには、IEEE PD クラス、電力レベル、PoE 管理ステータス、PoE 動作ステータス、PoE ポリシングステータス、スイッチ名、インターフェイス名、割り当て電力、消費電力、最大使用電力、PoE 優先順位、PoE 構成、無停止型 PoE など、AP の PoE テレメトリが表示されます。

[Power Distribution] セクションには、選択された時間範囲の配電（割り当て済み電力と消費電力）のトレンドチャートが表示されます。

[StackWise] タブ

このタブは、Cisco StackWise に対して表示されます。

Cisco StackWise に関する情報（シリアル番号、製品 ID、MAC アドレス、ロール、状態、優先順位、隣接するスイッチの番号など）が表示されます。

[StackWise Virtual] タブ
このタブは、Cisco StackWise Virtual に対して表示されます。 Cisco StackWise Virtual に関する情報（シリアル番号、製品 ID、MAC アドレス、ロール、状態、優先順位、稼働時間、ポート番号など）が表示されます。

[RF] タブ

このタブは、AP とワイヤレスクライアントに対して表示されます。

- [RF] タブには、[Radio 0]、[Radio 1]、[Radio 2] のように、無線固有の KPI に対応するタブがあります。それぞれの無線のタブをクリックすると、その無線のチャネル使用率、干渉、ノイズ、電波品質、通信時間の効率、クライアントごとのワイヤレス遅延の分布、送信出力、チャネル情報などのチャートが表示されます。

  （注） **[RF] タブの制限**

  3 つの無線がある AP（Cisco Catalyst 9130 AP など）を 17.2 以降のバージョンのワイヤレスコントローラに接続した場合、デバイスで3つすべての無線がサポートされ、[RF] タブに 3 つの無線（無線 0、無線 1、および無線 2）が表示されます。

  同じ AP を 17.1 以前のバージョンのワイヤレスコントローラに接続した場合、デバイスでは 2 つの無線がサポートされ、[RF] タブに 2 つの無線（無線 0 と無線 1）が表示されます。

  ただし、AP を新しいバージョンから古いバージョンのワイヤレスコントローラ（17.2 以降から 17.1 以前）に移行した場合は、最初に検出された 3 つの無線（無線 0、無線 1、無線 2）が [RF] タブにそのまま表示されます。

- AP の 5 GHz 無線については、[DFS] タブに動的周波数選択（DFS）レーダーイベントに関する情報が表示されます。

- AP 360 については、[RF] タブに [Neighbors and Rogues] タブが含まれます。そのタブには、[Band]（2 GHz および 5 GHz 無線周波数）、[Type]（All、Neighbor、Rogue）および [RSSI Range]（0 ～ 100 dBm）フィルタが含まれます。選択されたフィルタに応じて、AP テーブルが更新されます。

  AP テーブルデータには、識別子、無線、RSSI（dBm）、チャネル、タイプ、SSID、クライアント数、および送信出力（dBm）が含まれます。AP デバイス、無線、または他の値の検索を実行するには、検索バーを使用します。

  ⚙ をクリックしてメニューを開き、[Edit Table Column] を使用して特定の列を有効または無効にできます。

  CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。

- 選択されたフィルタに応じて、Wi-Fi Analyzer のグラフがテーブルの下に表示されます。Wi-Fi グラフでは、AP 360 タイムラインスライダの上部で選択された時間範囲について、集計された KPI の合計値と平均値の要約が示されます。

  特定の AP に関する Wi-Fi Analyzer のグラフを表示するには、AP の横にあるチェックボックスをオンにします。詳細を表示するには、チャートにカーソルを合わせます。

  [Chart Setting] アイコンをクリックして、各 AP のグラフに表示される [Access Point Label] を有効または無効にします。

[Virtual Network] タブ
このタブは、SD-Access ファブリックで使用できます。 KPI は、[VN Services] カテゴリと [Fabric Control Plane] カテゴリにグループ化されます。カテゴリを選択して、[Multicast（external RP）] と [Pub-Sub Session Status] の両方の KPI を表示できます。これらのカテゴリをフィルタ処理して、接続先、IPアドレス、タイプなどの到達可能性情報を含むテーブルを表示できます。コントロールプレーンの到達可能性ステータス、lisp、およびpubsubセッションのステータスチャートを表示するには、接続先の横にあるチェックボックスをオンにします。

[Transits and Peers Network] タブ
このタブは、SD-Access ファブリックで使用できます。 [Transits and Peers Network] タブには、[Transit Site Control Plane] の KPI である [LISP Session from Border to Transit Site Control Plane] と [Pub-Sub Session from Border to Transit Site Control Plane] が含まれています。適切な KPI チェックボックスをオンにして、接続先、IP アドレス、タイプなどの到達可能性情報を含むチャートとテーブルを表示します。

ステップ 16 建物内のフロア全体にわたるAP無線の正常性を比較するには、右上隅のトグルボタンをクリックして、[Map View] と [Map and Comparison View] を切り替えます。

[Map and Comparison View] には、AP 無線が配置されたフロアマップが表示されます。

ステップ 17 [View Floor] ドロップダウンリストから、AP 無線を比較するフロアを選択します。

フロアマップ上の AP アイコンにカーソルを合わせると、AP 無線のデバイスの詳細（[MAC Address]、[Model]、[Mode]、[Issue Count] など）が表示されます。

ステップ 18 [Compare AP Radios] をクリックしてフロアマップ上の AP 無線を比較します。

[Map View] がデフォルトで表示され、最後の 5 分間の AP 無線データが表示されます。

ステップ 19 フロアマップ上の AP アイコンをクリックします。

比較する無線を選択または選択解除するためのダイアログボックスが表示されます。

ステップ 20 フロアで比較する無線のリストの横にあるチェックボックスをオンにします。

（注）
- デフォルトでは、それぞれの AP の最初の無線がモニターモードの場合にのみ、Cisco DNA Center は現在の AP を比較対象として選択します。
- 比較に使用可能な AP 無線のモードは、[Local]、[Remote]、[Hybrid] モードのみです。
- 一度に最大 5 つの AP 無線を比較のために選択できます。

ステップ 21 [AP Radio Compatibility] を使用して、比較のために選択された AP 無線のリストを表示します。

[Radio]、[IP Address]、[Model]、[Uptime]、[Connected to WLC]、[Floor] を比較できます。

ステップ 22 [Comparative Metrics] を使用して、選択された KPI の比較メトリックを表示します。

ステップ 23 [Select KPI] ドロップダウンリストから、比較マトリックスを表示する KPI を選択します。

次の KPI から選択できます。

- チャネル情報
- トラフィック（受信レート）
- 接続されているクライアントの数
- 無線の再試行
- チャネルの使用率
- Interference
- Noise
- 電波品質
- クライアント数ごとのワイヤレス遅延
- 管理フレーム
- データフレーム
- Tx Errors
- Rx Errors
- Tx Power
- マルチキャストカウンタ

ステップ 24 トグルボタンをクリックして [Map View] と [Table View] を切り替えます。

[Access Point Radios] テーブルビューには AP 無線が一覧表示されます。

ステップ 25 フロアマップで比較する AP 無線の横にあるチェックボックスをオンにします。

ステップ 26 [AP Radio Comparison] エリアの比較からすべての無線を削除するには、[Clear Selection] をクリックします。

ステップ 27 [Exit Comparison] をクリックして終了します。

スイッチおよびルータの重大レベルに満たない選択済み Syslog

次の表に、[Device 360] ウィンドウの [Event Viewer] に表示される、クリティカルレベルに満たない syslog メッセージ（エラー、注意、通知、情報）の選択済みリストを示します。

プロトコルイベント	レイヤ 2 イベント
OSPF-5-OSPF-5-ADJCHG	SW_MATM-4-MACFLAP_NOTIF
IFDAMP 5-UPDOWN	MAC_LIMIT-4-PORT_EXCEED
BGP-5-ADJCHANGE	MAC_LIMIT-4-VLAN_EXCEED
DUAL-5-NBRCHANGE	IGMP-6-IGMP_GROUP_LIMIT
BGP-5-ADJCHANGE-bfd	SPANTREE-5-ROOTCHANGE
CLNS-5-ADJCHANGE	UDLD-4-UDLD_PORT_DISABLED
LDP-5-NBRCHG-TDP	PM-4-ERR_DISABLE
LDP-5-NBRCHG-LDP	CDP-4-DUPLEX_MISMATCH
CDP-4-NATIVE_VLAN_MISMATCH	LINK-5-CHANGED
LISP-4-LOCAL_EID_RLOC_INCONSISTENCY	PORT-5-IF_DOWN
LISP-4-LOCAL_EID_NO_ROUTE	PORT-5-IF_UP
LISP-4-CEF_DISABLED	
LISP-4-LOCAL_EID_MAP_REGISTER_FAILURE	
LISP-4-MAP_CACHE_WARNING_THRESHOLD_REACHED	

ハードウェア プラットフォーム イベント
SYS-5-CONFIG_I
SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-6-REMCARD
OIR-SP-6-INSCARD
OIR-SP-6-REMCARD
PLATFORM_STACKPOWER-6-CABLE_EVENT
PLATFORM_STACKPOWER-6-LINK_EVENT
PLATFORM_STACKPOWER-4-TOO_MANY_ERRORS
PLATFORM_STACKPOWER-4-VERSION_MISMATCH
PLATFORM_STACKPOWER-4-UNDER_BUDGET
PLATFORM_STACKPOWER-4-INSUFFICIENT_PWR
PLATFORM_STACKPOWER-4-REDUNDANCY_LOSS
ILPOWER-5-POWER_GRANTED
ILPOWER-5-LINKDOWN_DISCONNECT
ILPOWER-5-IEEE_DISCONNECT
ILPOWER-5-INVALID_IEEE_CLASS
ILPOWER-4-LOG_OVERDRAWN
ILPOWER-5-CLR_OVERDRAWN

Cisco StackWise Virtual と制限事項について

Cisco StackWise Virtual はネットワークシステムの可視化技術です。2 台の物理スイッチが 40-G または 10-G イーサネット接続を使用して 1 台の論理的な仮想スイッチとして動作することを可能にします。

StackWise Virtual 対応デバイス

次の表に、StackWise Virtual をサポートする Cisco Catalyst スイッチを示します。

デバイス	サポート対象 IOS-XE ソフトウェアの最小バージョン
Cisco Catalyst 9300 シリーズ スイッチ	16.11 +
Cisco Catalyst 9400 シリーズ スイッチ	16.11 +

デバイス	サポート対象 IOS-XE ソフトウェアの最小バージョン
Cisco Catalyst 9500 シリーズ スイッチ	16.11+

StackWise Virtual の制限事項

Cisco StackWise Virtual には、次の既知の制限事項があります。

- Cisco StackWise Virtual を設定した後も、2 番目のスイッチはインベントリに表示されたままになります。独自の IP アドレスがないため、応答を停止します。回避策として、次が可能です。

  1. インベントリから 両方のスイッチを削除します。ネットワーク デバイスの削除 （77 ページ）を参照してください。
  2. StackWise Virtual を設定します（2 つのスイッチを 1 つの仮想スイッチに設定します）。
  3. デバイスを検出します。IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。

（注） StackWise Virtual が検出されると、1 台のスイッチがアクティブな役割を果たし、もう 1 台はスタンバイの役割を果たします。スタック内の両方のスイッチは、1 つのプライマリ管理 IP アドレスに関連付けられます。

- Cisco StackWise Virtual を削除すると、2 つのスイッチは独立します。両方が同じ IP アドレスを持ち、デュアルアクティブ検出（DAD）状態で動作します。回避策として、次が可能です。

  1. 2 番目のスイッチで別の IP アドレスを設定します。
  2. デバイスをもう一度検出します。IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。

Cisco StackWise と制限事項について

Cisco StackWise テクノロジーは、スイッチで構成されるスタックの能力をまとめて活用する革新的な新しい手段を提供します。個別のスイッチがインテリジェントに結合され、32 Gbps のスイッチングスタックの相互接続により 1 つのスイッチングユニットが形成されます。スタック内のすべてのスイッチが設定情報とルーティング情報を共有することで、単一のスイッチングユニットを作り上げます。

Cisco StackWise 対応デバイス

Cisco StackWise をサポートするデバイスを次に示します。

- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ

StackWise の制限事項

Cisco StackWise には、次の既知の制限事項があります。

- リングのステータスが **Device 360** ヘッダーに表示されません。
- リンク速度の情報は、**[Detail Information]** > **[Interfaces]** タブに表示されません。

ネットワークデバイスの正常性スコアの設定

ネットワークデバイスの正常性スコアを設定するには、次の手順を実行します。KPI のしきい値を変更し、計算に含める KPI を指定すると、ネットワークデバイスの正常性スコアの計算をカスタマイズできます。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Manage]** > **[Health Score Settings]** の順に選択します。

[Health Score] ウィンドウが表示されます。

ステップ 2 ネットワークデバイス カテゴリのタブをクリックして、正常性スコアの計算設定をカスタマイズします。

このタブには、ネットワークデバイスタイプの正常性スコアの計算に影響する KPI が表示されます。

ステップ 3 [KPI Name] 列で、KPI 名のリンクをクリックします。

KPI のスライドインペインが表示されます。

ステップ 4 KPI の正常性スコアを次のように設定します。

a) 定量的 KPI しきい値の場合は、良好な正常性スコアと見なすしきい値をカスタマイズできます。
b) 正常性と問題の設定の間で共通の KPI しきい値を同期または同期解除するには、[Synced] トグルボタンを使用します。正常性または問題の設定ページから同期した場合は、逆に同期されます。
c) 正常性スコアの計算から KPI を削除するには、[Included in Device health Score] チェックボックスをオフにします。

（注）	ネットワークデバイスの正常性スコアは、含まれるすべての KPI の中で最も低いスコアです。
制約事項	正常性スコアの計算には、少なくとも 1 つの KPI を含める必要があります。
注目	ネットワークデバイスの KPI 正常性スコアを表示する際、除外された KPI には正常性スコアの代わりに「NA」と表示されます。

d) デフォルト設定に戻すには、カーソルを [View Default Setting] の上に置いて、[✓ Use default] をクリックします。

ステップ 5 [Apply] をクリックします。

確認のダイアログボックスが表示されます。

ファブリックネットワークについて

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Cisco DNA Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、新しいファブリックサイトを作成できます。つまり、サイトのテレメトリ設定を構成するときには、[Monitor wired clients] を有効にしておく必要があります。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[SD ACCESS]** > **[Fabric Sites]** の順に選択します。

ステップ 2 [Fabric Sites] タブで、[Add fabric site] をクリックします。

または、最初の 2 つの手順の代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** を選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let's Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 （オプション）ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、表示されたネットワーク階層からファブリックサイトを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウでファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 8 [作成（Create）] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」というメッセージが表示されます。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）
- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

1. メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
2. [Inventory] ウィンドウに、検出されたデバイスが表示されます。
3. ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
4. ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
5. 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで**[Inventory]** > **[Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 [SD ACCESS] の下でメニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 3 デバイスをクリックします。スライドインペインには、次の [Fabric] オプションが表示されます。

オプション	説明
エッジ	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
Border	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスを一体型ファブリックとして設定するには、[Control Plane]、[Border]、および [Edge] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane] と [Border] の両方を選択します。

ステップ 4 [Add] をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ファブリック デバイスで SNMP コレクタ メトリックを有効化

ファブリック デバイスのヘルス スコアが正しく入力されるようにするには、SNMP コレクタ メトリックを有効化する必要があります。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

ステップ 2 [Collectors] をクリックします。

コレクタのリストが表示されます。

ステップ 3 [COLLECTOR-SNMP] をクリックします。

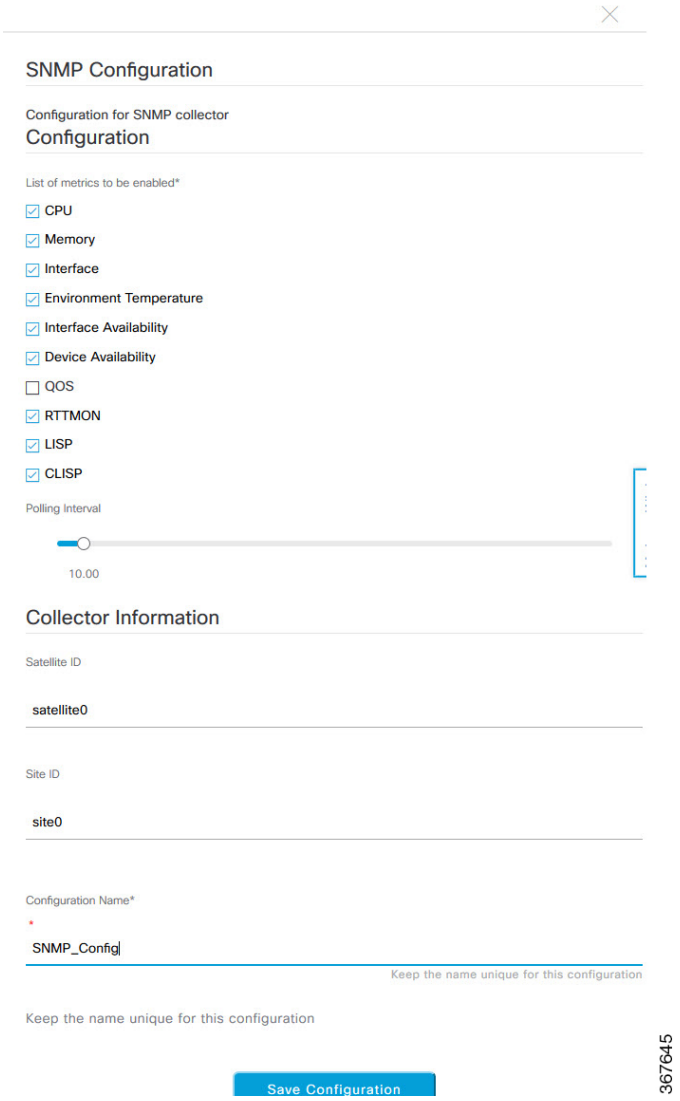
[COLLECTOR-SNMP] ウィンドウが開きます。

ステップ 4 **[+ Add]** をクリックします。

[SNMP Configuration] ダイアログ ボックスが開きます。

ステップ 5 QOS を除くすべてのメトリックの横にあるチェックボックスをオンにします。

図 *10 : SNMP* の設定



ステップ 6 [Configuration Name] フィールドに、SNMP 設定の一意の名前を入力します。

ステップ 7 [Save Configuration] をクリックします。

ネットワークの正常性スコアと KPI メトリックについて

ここでは、ネットワーク正常性スコアと KPI メトリックの計算方法について説明します。

ネットワーク ヘルス スコア

ネットワーク ヘルス スコアは、健全なネットワーク デバイス（ヘルス スコアが 8～10）の数をネットワーク デバイスの総数で割ったパーセンテージです。スコアは 5 分ごとに計算されます。

例：90%（ヘルス スコア）＝90（ヘルス スコア 8 ～ 10 のネットワーク デバイス）÷100（ネットワーク デバイスの総数）

デバイスカテゴリの正常性スコア

デバイスカテゴリの正常性スコア（アクセス、コア、ディストリビューション、ルータ、ワイヤレス）は、ターゲットカテゴリ内の正常なネットワークデバイスの数（正常性スコアが 8 ～ 10）をそのカテゴリのネットワークデバイスの総数で割ったパーセンテージですスコアは 5 分ごとに計算されます。

例：90 %（正常性スコア）＝90（ターゲットカテゴリ正常性スコアが 8 ー 10 のネットワーク デバイス）÷100（そのカテゴリのネットワークデバイス）

個別のデバイス正常性スコア

個別のデバイスの正常性スコアは、KPI メトリック正常値スコア（システムの正常性、データ プレーンの接続性、コントロールプレーンの接続性）の内の最小スコアになります。KPI メトリックスコアは、KPI ごとに定義されるしきい値に基づきます。

デバイス正常性スコア＝MIN（システムの正常性、データプレーンの接続性、コントロールプレーンの接続性）

デバイスのタイプに応じて、メトリックは変わります。

システムの正常性	
デバイス タイプ	**説明**
スイッチ（アクセスおよび配信）	CPU 使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。
ワイヤレス	次のシステムモニターリング メトリックが含まれます。 • ワイヤレスコントローラの場合、メモリ使用率、空きタイマー、空き Mbuf が含まれます。 • AP の場合、CPU 使用率とメモリ使用率が含まれます。
ルータ	CPU 使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。
ファブリック	CPU 使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。

データプレーンの接続性	
デバイス タイプ	**説明**
スイッチ（アクセスおよび配信）	リンクエラーやリンクステータスなどのメトリックが含まれます。 スイッチの場合、デバイス間リンク可用性メトリックは、物理スタックポート、ネットワークデバイスに接続されたリンク、およびファブリックエッジ側のポートチャネルをカウントします。
ワイヤレス	次のシステムモニターリング メトリックが含まれます。 • ワイヤレスコントローラの場合、WQE プール、パケットプール、リンクエラーなどのメトリックが含まれます。 • AP の場合、インターフェイス、ノイズ、電波品質、無線利用率などの RF メトリックが含まれます。
ルータ	リンクエラーなどのメトリックが含まれます。

コントロールプレーンの接続性	
デバイス タイプ	**説明**
ワイヤレス	次の KPI が含まれます。 • ワイヤレスコントローラの場合、コントロールプレーン ノード サーバーへの接続性が含まれます。 • ファブリックデバイスの場合、コントロールプレーンノードへの接続性などのメトリックが含まれます。

スイッチ ヘルス スコア

スイッチ ヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 95 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 95 パーセント以上の場合、スコアは 1 です。
メモリ使用率	• メモリ使用率が 95 パーセント以下の場合、スコアは 10 です。 • メモリ使用率が 95 パーセント以上の場合、スコアは 1 です。

パラメータ	スコアの計算
リンクエラー（Rx および Tx）	リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、APなど）間のトポロジリンクを指します。 物理インフラストラクチャ インターフェイスにエラーがある場合のスコアは 8、すべてのリンクがダウンしている場合は 1、それ以外の場合は 10 です。
リンク破棄	リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、AP など）間のトポロジリンクを指します。 物理インフラリンクにパケットドロップ（廃棄）がある場合、すべてのリンクで廃棄が発生した場合のスコアは8、それ以外の場合は 10 です。
リンク ステータス	リンクステータスのアップ/ダウンについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、AP など）間のトポロジリンクを指します。 物理インフラストラクチャ インターフェイスがダウンしている場合のスコアは8、すべてのインターフェイスがダウンしている場合は 1、それ以外の場合は 10 です。
コントロールプレーンノードへの接続 - ファブリックデバイスのみ（エッジおよびボーダー）	• コントロール プレーン ノードが到達可能な場合、スコアは 10 です。 • コントロール プレーン ノードが到達不能な場合、スコアは 1 です。 （注） ファブリックネットワークに 1 つ以上のコントロールプレーンノードが存在し、すべてのコントロールプレーンノードに到達可能な場合、スコアは 10 です。そうでない場合、スコアは 1 です。 （注） ヘルス スコアをファブリック デバイス向けに正しく入力するには、SNMP コレクタ メトリックを有効にします。ファブリック デバイスで SNMP コレクタ メトリックを有効化 （122 ページ）を参照してください。

ルータ ヘルス スコア

ルータ ヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 95 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 95 パーセント以上の場合、スコアは 1 です。
メモリ使用率	• メモリ使用率が 95 パーセント以下の場合、スコアは 10 です。 • メモリ使用率が 95 パーセント以上の場合、スコアは 1 です。
WAN 接続	• WAN 接続がダウンした場合、スコアは 1 です。 • WAN 接続がアップしている場合、スコアは 10 です。
リンクエラー	リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、APなど）間のトポロジリンクを指します。 物理インフラストラクチャ インターフェイスにエラーがある場合のスコアは 8、すべてのリンクがダウンしている場合は 1、それ以外の場合は 10 です。
リンク破棄	リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、AP など）間のトポロジリンクを指します。 物理インフラリンクにパケットドロップ（廃棄）がある場合、すべてのリンクで廃棄が発生した場合のスコアは 8、それ以外の場合は 10 です。

AP ヘルス スコア

AP ヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 90 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 90 パーセント以上の場合、スコアは 1 です。

パラメータ	スコアの計算
メモリ使用率	• メモリ使用率が 90 パーセント未満の場合、スコアは 10 です。 • 利用可能メモリ率が 90 パーセント以上の場合、スコアは 1 です。
無線使用率スコア	スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。 • 無線使用率が 70 パーセント未満の場合、スコアは 10 です。 • 無線使用率が 70 パーセント以上の場合、スコアは 1 です。
干渉スコア	スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。 2.4 GHz 無線の場合： • 干渉が 50 パーセント以下の場合、スコアは 10 です。 • 干渉が 50 パーセントを超える場合、スコアは 1 です。 5 GHz 無線の場合： • 干渉が 20 パーセント以下の場合、スコアは 10 です。 • 干渉が 20 パーセントを超える場合、スコアは 1 です。
RF ノイズスコア	スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。 2.4 GHz 無線の場合： • RF ノイズが -81 dBm 未満の場合、スコアは 10 です。 • RF ノイズが -81 dBm 以上の場合、スコアは 1 です。 5 GHz 無線の場合： • RF ノイズが -83 dBm 未満の場合、スコアは 10 です。 • RF ノイズが -83 dBm 以上の場合、スコアは 1 です。

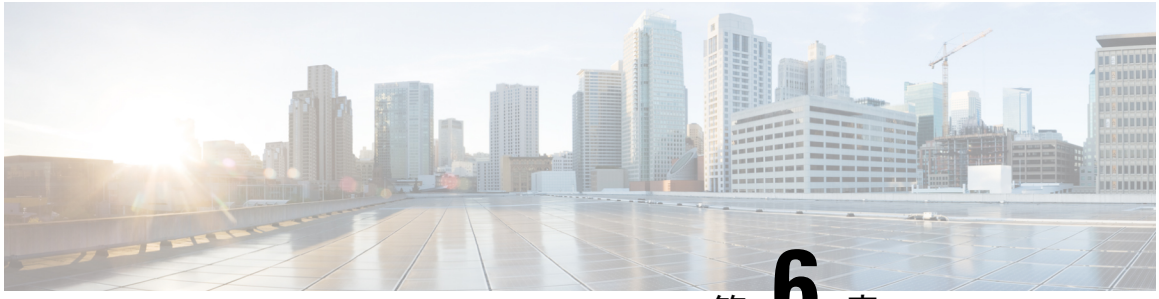
パラメータ	スコアの計算
電波品質スコア	スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。 2.4 GHz 無線の場合： • 電波品質が 60 パーセント以上の場合、スコアは 10 です。 • 電波品質が 60 パーセント未満の場合、スコアは 1 です。 5 GHz 無線の場合： • 電波品質が 75 パーセント以上の場合、スコアは 10 です。 • 電波品質が 75 パーセント未満の場合、スコアは 1 です。

ワイヤレス コントローラのヘルス スコア

ワイヤレス コントローラのヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
メモリ使用率	• メモリ使用率が 90 パーセント未満の場合、スコアは 10 です。 • 利用可能メモリ率が 90 パーセント以上の場合、スコアは 1 です。
空きタイマースコア	• 空きタイマーの数が 20 パーセント以上の場合、スコアは 10 です。 • 空きタイマーの数が 20 パーセント以下の場合、スコアは 1 です。
空きメモリバッファ（**MBufs**）	• 空きメモリ バッファの数が 20 パーセント以上の場合、スコアは 10 です。 • 空きメモリ バッファの数が 20 パーセント以下の場合、スコアは 1 です。
作業キュー要素（**WQE**）のプールスコア	• WQE プールが WQE プールのしきい値より大きい場合、スコアは 10 です。 • WQE プールが WQE プールのしきい値と同じレベルかこれより低い場合、スコアは 1 です。

パラメータ	スコアの計算
パケットプール	• パケット プールがパケット プールのしきい値より大きい場合、スコアは 10 です。 • パケット プールがパケット プールのしきい値と同じレベルかこれより低い場合、スコアは 1 です。
Link Errors	• リンク エラーが 1 パーセント以下の場合、スコアは 10 です。 • リンク エラーが 1 パーセント以上の場合、スコアは 1 です。
コントロールプレーンノードへの接続 - ファブリック ワイヤレス コントローラのみ	• コントロール プレーン ノードが到達可能な場合、スコアは良好です。 • コントロール プレーン ノードが到達不能な場合、スコアは不良です。 （注） ファブリックネットワークに 1 つ以上のコントロールプレーンノードが存在し、すべてのコントロールプレーンノードに到達可能な場合、スコアは 10 です。そうでない場合、スコアは 1 です。



第 6 章

企業全体の健全性のモニターとトラブルシューティング

企業について

企業全体の健全性のモニターとトラブルシューティングに、アシュアランスを使用できます。企業はネットワークデバイスとクライアントで構成されています。

ネットワークは、ルータ、スイッチ、ワイヤレスコントローラ、アクセスポイントを含む、1つまたは複数のデバイスで構成されています。

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

企業の全体的な健全性のモニターとトラブルシューティング

この手順を使用して、ネットワークデバイスやクライアントを含む企業の健全性の概要を把握し、対処する必要がある潜在的な問題があるかどうかを判断します。

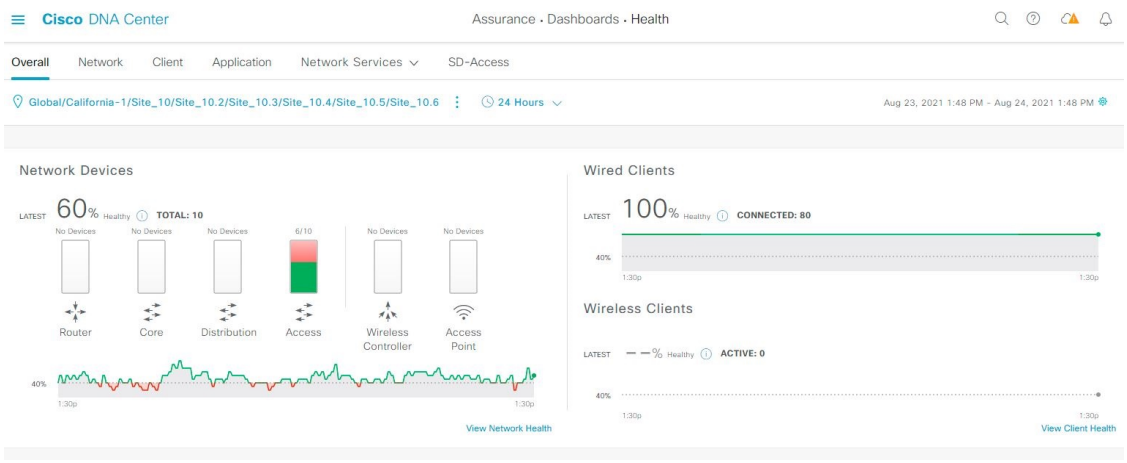
始める前に

アシュアランスを設定します。「基本的な設定のワークフロー （17 ページ）」を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Health]**。

[Overall health] ダッシュボードが表示されます。

図 *11 : [Overall Health]* ダッシュボード



ステップ 2 次の機能には、[Overall] 正常性ダッシュボードの上部のメニューバーを使用します。

[Overall] 正常性ダッシュボードの上部のメニューバー	
アイテム	説明
Global [Location] ペイン	• Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • Hide Sites をクリックして [Sites] テーブルを非表示にします。 • : このトグルボタンをクリックして、ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。テーブルには、特定のロケーションの正常なクライアントとネットワークデバイスの割合が選択に基づいて表示されます。 • : このトグルボタンをクリックすると、企業のすべてのサイトの正常性が、地理的ロケーションに基づいた正常性マップで表示されます。デフォルトでは、提示されるサイトは問題の重大度に従って色分けされています。 ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、データを取得できなかったことを示します。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Overall] ダッシュボードに表示されます。
時間範囲	過去 3 時間、24 時間、または 7 日間のデータを表示できます。
[Actions] ドロップダウン リスト	ドロップダウンリストから [Edit Dashboards] を選択すると、ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317ページ）およびカスタム ダッシュボードの作成 （313 ページ）を参照してください。

ステップ 3 次の機能には、[Overall Health 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
[Network Devices]	Network Score：企業全体での正常（良好）なデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アクセスポイント）の割合。ネットワーク ヘルス スコア （124 ページ）を参照してください。 Device Category Health Score：デバイスカテゴリ（[Router]、[Core]、[Distribution]、[Access]、[Controller]、[Access Point]) で正常（良好）なネットワークデバイスの割合。 （注） SD-Access ファブリックを選択すると、このエリアには [Fabric Edge]、[Fabric Border]、および [Fabric Control Plane] のカテゴリで正常なネットワークデバイスの割合が表示されます。 [View Network Health] をクリックして、[Network Health] ダッシュボードを開きます。ネットワークの健全性のモニターとトラブルシューティング （93 ページ）を参照してください。
[Wired Clients] と [Wireless Clients]	有線クライアントとワイヤレスクライアントの間のスコア分布を示します。[Wired] スコアまたは [Wireless] スコアは、企業全体の正常（良好）な有線またはワイヤレスのクライアントデバイスの割合です。クライアント ヘルス スコア （159 ページ）を参照してください。 [View Client Health] をクリックすると、[Client Health] ダッシュボードが開きます。すべてのクライアント デバイスの健全性のモニターとトラブルシューティング （137 ページ）を参照してください。

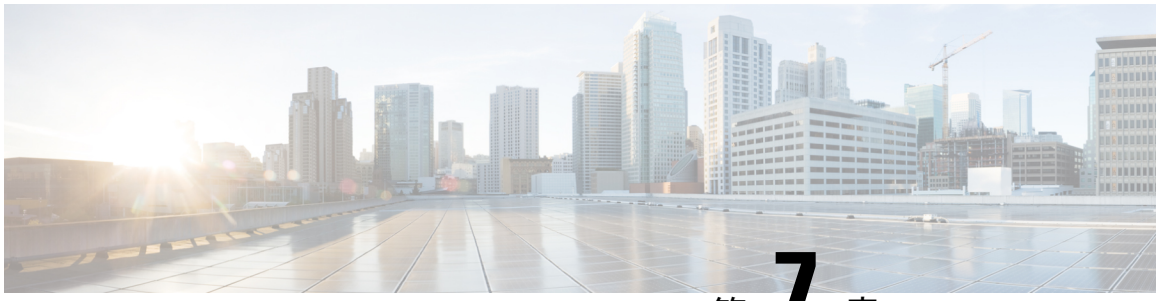
ステップ 4 次の機能には、[Network Services] ダッシュレットを使用します。

[Network Services] ダッシュレット	
アイテム	説明
AAA	企業全体のすべての AAA サーバーについて、成功したトランザクションと失敗したトランザクションの合計パーセンテージを示します。 [View AAA Dashboard] をクリックして、[Network Services AAA] ダッシュボードを開きます。AAA ネットワークサービスの監視 （187 ページ）を参照してください。
[DHCP]	企業全体のすべての DHCP サーバーについて、成功したトランザクションと失敗したトランザクションの合計パーセンテージを示します。 [View DHCP Dashboard] をクリックして、[Network Services DHCP] ダッシュボードを開きます。DHCP ネットワークサービスの監視 （190 ページ）を参照してください。

ステップ 5 次の機能には、[Top 10 Issue Type] ダッシュレットを使用します。

[Top 10 Issues] ダッシュレット
対処する必要がある上位 10 件の問題を表示します（存在する場合）。問題は色分けされ、事前割り当てされた P1 から始まる優先度レベルで並び替えられます。 問題をクリックすると、スライドインペインが開き、問題のタイプに関する追加の詳細が表示されます。スライドインペインで問題のインスタンスをクリックします。必要に応じて、次の操作を実行できます。 • 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 • 問題のインスタンスを無視するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 [View All Issues] をクリックすると、[Open Issues] ウィンドウが開きます。 問題の詳細については、未解決の問題を表示 （217 ページ）を参照してください。

企業の全体的な健全性のモニターとトラブルシューティング



第 7 章

クライアント正常性のモニターとトラブルシューティング

クライアントについて

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

すべてのクライアントデバイスの健全性のモニターとトラブルシューティング

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

この手順を使用して、すべての有線およびワイヤレスのクライアントの正常性の概要を把握し、対処する必要がある潜在的な問題があるかどうかを判断します。

アシュアランス 機械学習（ML）アルゴリズムを使用してネットワーク内の動作パターンを抽出し、トレンドを予測します。これらのトレンドは、[Client Onboarding Time] ダッシュレットおよび [Client Count Per SSID] ダッシュレットに基準として表示されます。

（注） HA フェールオーバーが発生した場合、クライアントの正常性データの表示に 1 時間かかることがあります。

始める前に

アシュアランスを設定します。「基本的な設定のワークフロー （17 ページ）」を参照してください。

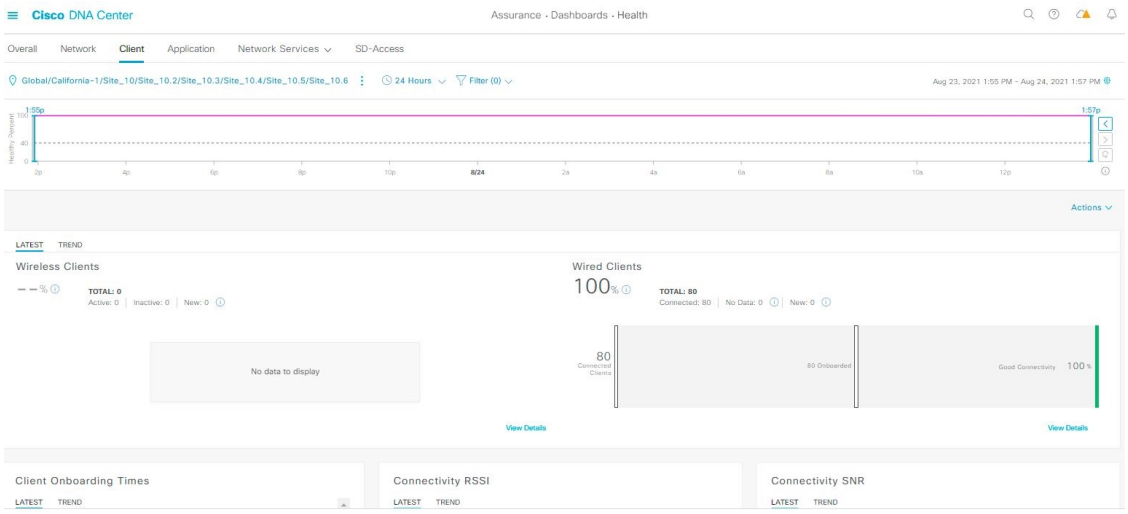
ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

図 *12*：クライアントの正常性ダッシュボード



ステップ 3 次の機能には、[Client] 正常性ダッシュボードの上部メニューバーを使用します。

[Client] 正常性ダッシュボードの上部メニューバー	
アイテム	説明
Global [Location] ペイン	クリックすると、次のアイコンが表示されます。 • Global をクリックして、左側の階層ツリーペインからエリア/サイト、または建物を選択します。グローバルから下矢印をクリックして、関連するエリア、サイト、および建物に移動することもできます。 ネットワーク階層からフロアを選択することはできません。 • ロケーションアイコンの横にある をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • Hide Sites をクリックして [Sites] テーブルを非表示にします。 • ：このトグルボタンをクリックすると、ドロップダウンリストを使用して、サイトまたは建物ごとの正常なクライアントの割合をテーブル形式で表示できます。ロケーションに対して [Apply] をクリックすると、[Client Health] ダッシュボードにはそのロケーションのクライアント情報のみが表示されます。 • ：このトグルボタンをクリックすると、すべてのクライアントサイトの正常性が、地理的ロケーションに基づいたクライアント正常性マップで表示されます。デフォルトでは、クライアントサイトは問題の重大度に従って色分けされています。 ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、クライアントが非アクティブであることを示します。 [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Client Health] ダッシュボードに表示されます。
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。 **1.** 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。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。

[Client] 正常性ダッシュボードの上部メニューバー	
アイテム	説明
[Filter] アイコン	[SSID] および [Band] オプションが含まれます。ドロップダウンリストから SSID と帯域周波数の隣にあるチェックボックスをオンにして選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。 （注） 複数の SSID を選択できます。たとえば、クラス 1 およびクラス 2 の SSID を選択した場合、ダッシュボードには、クラス 1 SSID とクラス 2 SSID に接続されているクライアントの情報が表示されます。
[Actions] ドロップダウン リスト	ドロップダウンリストから [Edit Dashboards] を選択すると、ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317ページ）およびカスタム ダッシュボードの作成 （313 ページ）を参照してください。

ステップ 4 **タイムラインスライダ**を使用すると、正常なクライアント比率をより詳細な時間範囲で表示できます。

タイムライン内でマウスのカーソルを合わせると、特定の時点のワイヤレスおよび有線クライアントの正常性スコアのパーセンテージが表示されます。

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、ダッシュボード ダッシュレットに表示されるクライアントデータのコンテキストが設定されます。

タイムラインの右にある矢印ボタンを使用して、最大 30 日分のデータを表示できます。

点線の横線は、正常なクライアントのしきい値を表します。デフォルトでは、40% に設定されています。

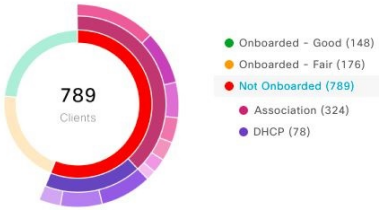
しきい値を変更するには、次の手順を実行します。

1. 情報アイコン（）にカーソルを合わせます。
2. ツールチップで、編集アイコン（）をクリックします。
3. [Client Health Threshold] スライドインペインで、青色の線をクリックしてドラッグし、しきい値のパーセンテージを設定します。
4. [Save] をクリックします。

（注） [Client Summary] の [Health Score] が赤色で表示される場合、カスタムしきい値の変更に影響が出ます。カスタムしきい値によって、正常または異常なデバイスの数が変わることはありません。

ステップ 5 次の機能には、[Client Health] ダッシュレットを使用します。

[Client Health Summary] ダッシュレット	
アイテム	説明
[Client Health Summary] エリア	次のタブが含まれます。 • [Latest]：デフォルトで表示されます。主要な構成は以下のとおりです。 • [Wireless Clients] と [Wired Clients Health Summary Score]：ワイヤレスおよび有線クライアントの正常性スコアは、正常にオンボードされ接続性が良好なクライアントの割合です。クライアント ヘルス スコア （159 ページ） を参照してください。 • [Total Devices]：クライアントの合計数、およびアクティブ、非アクティブ、新しいクライアントの数が表示されます。Cisco DNA Center は、5 分間の正常性スコア計算ウィンドウ内のアクティビティに基づいて、アクティブなクライアント、非アクティブなクライアント、および新しいクライアントを次のように定義します。 • [Active]：正常にオンボードし、データしきい値を満たすのに十分なデータを送信しているクライアント、正常にオンボードしたが切断されたクライアント、オンボードを試行したが失敗したクライアント、オンボードを試行したが除外されたクライアント。 • [Inactive]：データしきい値を満たすのに十分なデータを送信していないクライアント。ユーザー アイドル タイムアウト期間が経過すると、ワイヤレスコントローラは非アクティブなクライアントの認証を解除します。 • [New]：オンボーディング中のクライアント。これらのクライアントの正常性スコアは、次回の 5 分間の計算ウィンドウに含まれます。 • [Charts]：このスナップショットビュー チャートでは、過去 5 分間でオンボードに成功または失敗したクライアントの分布が示されます。次に、正常にオンボードしたクライアントの数を使用して、このチャートでは接続性が良好または中程度のクライアントの割合が示されます。 • [Trend]：一定の期間にわたるクライアントの健全性を示すトレンドチャートを表示します。 オンボードに失敗したクライアントの場合、オンボーディング失敗の理由が示されます。例には、AAA、DHCP、およびその他が含まれます。 チャート内の色は、クライアントデバイスの正常性を示しています。 ●：クライアントデバイスが不適切です。ヘルス スコアの範囲は 1 ～ 3 です。 ●：クライアントデバイスが適切です。ヘルス スコアの範囲は 4 ～ 7 です。 ●：クライアントデバイスが良好です。ヘルス スコアの範囲は 8 ～ 10 です。 ●：クライアントデバイスが非アクティブです。ヘルス スコアは 0 です。

[Client Health Summary] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 放射状棒チャートは、オンボーディングに失敗したクライアントの分布と、オンボーディング失敗の理由を示します。各セグメントをクリックして、失敗の理由を表示できます。  • そのセグメントのクライアント数別のデータタイプカテゴリ。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

ステップ 6 ネットワーク内のクライアントの特定の KPI とメトリックを表示するには、KPI ダッシュレットを使用します。次の表では、KPI ダッシュレットについて説明します。

（注） チャートデータは 5 分ごとに更新されます。

[Client Onboarding Times] ダッシュレット	
アイテム	説明
[Client Onboarding Times] チャート	すべてのサイトまたは選択したサイトでの、すべてのクライアントオンボード試行の時系列分布。このダッシュレットには、10秒以内にオンボードに成功したクライアントの割合が示されます。クライアントのオンボーディングは、関連付け、認証、アドレッシング、Web 認証、および DNS の各フェーズを対象としています。 チャートには、次の 2 種類があります。 • [Latest]：デフォルトで表示されます。このスナップショットビューチャートでは、過去 5 分間オンボードに成功または失敗したクライアントの分布が示されます。次に、正常にオンボードしたクライアントの数を使用して、このチャートでは接続性が良好または中程度のクライアントの割合が示されます。 • [Trend]：[Client Count] タブと [Baseline] タブがあります。[Baseline] タブをクリックすると、機械学習によって生成されるオンボーディング時間のチャートが表示されます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 （84 ページ）およびCisco AI Network Analytics の概要 （11 ページ）を参照してください。 **重要** 基準チャートを表示するには、[Filter] オプションからサイトと SSID を選択する必要があります。 基準チャートの詳細は、異なる色で表示されます。 • **緑色のバンド**：予測基準値。 • **青色の実線**：実際の値。 オンボードに失敗したクライアントの場合、オンボーディング失敗の理由が示されます。例には、AAA、DHCP、およびその他が含まれます。

[Client Onboarding Times] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 • 左側のペインには、[Overall]、[Association]、[Authentication]、[DHCP] タブが表示されます。タブをクリックすると、右側のペインにチャートが表示されます。 • 右側のペインに表示される [Charts] には、次のタブがあります。 • [Latest]：全体の平均オンボーディング時間が表示されます。 [Authentication] および [DHCP] の場合、[Latest] タブには、[Avg Latency Time]、[Authentication] の [Avg Authentication Time]、および [DHCP] の [Avg DHCP Time] に基づいてデータをフィルタリングするためのドロップダウンリストが表示されます。 • [Trend]：[Baseline] タブが含まれます。このタブでは、機械学習の基準チャートを表示できます。 左ペインで選択したタブに応じて、**[Trend]** > **[Baseline]**の下に追加のタブが表示されます。たとえば、[Association]、[Authentication]、または [DHCP] データの [Authentication]、[Time Baseline]、または [Failure Baseline] タブが表示されます。 （注） [Failure Baseline] データは、グローバルサイトの場合にのみ表示されます。 （注） [Baseline] 、[Time Baseline]、および [Failure Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 （84 ページ）およびCisco AI Network Analytics の概要 （11 ページ）を参照してください。 • チャートの上にマウスカーソルを合わせると、選択した時点の情報が同期化されたツールチップに表示されます。 • チャート内の色付きセグメントをクリックすると、次の情報が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Connectivity RSSI] ダッシュレット	
アイテム	説明
[Connectivity RSSI] チャート	すべてのサイトまたは選択したサイト内に配置されたすべてのクライアントの受信信号強度表示（RSSI）分布。このダッシュレットには、RSSI 測定値が -72 dBm（しきい値）より大きいすべてのクライアントの RSSI 測定値の割合が示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Connectivity SNR] ダッシュレット	
アイテム	説明
[Connectivity SNR] チャート	すべてのサイトまたは選択したサイト内に配置されたすべてのクライアントの信号対雑音比（SNR）分布。このダッシュレットには、SNR 測定値が 10 dBm（しきい値）より大きいすべてのクライアントの SNR 測定値の割合が示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Roaming Times] ダッシュレット	
アイテム	説明
[Client Roaming Times] チャート	ローミング時間および障害別のクライアント分布。このダッシュレットには、ローミング時間が 3000 ミリ秒未満のクライアントの割合が表示されます。

[Client Roaming Times] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Access Points]、[Top SSIDs]、[Top Host Device Types]、[Top Bands]、[Top Locations]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Count per SSID] ダッシュレット	
アイテム	説明
[Client Count per SSID] チャート	すべてのサイトまたは選択したサイトにおけるSSID別のクライアント数の時系列分布。 チャートには、次の 2 種類があります。 • [Latest]：デフォルトで表示されます。このスナップショットビューチャートには、SSID または選択したサイトごとのクライアントの分布が表示されます。 • [Trend]：[Client Count] タブと [Baseline] タブがあります。[Baseline] タブをクリックすると、機械学習によって生成される SSID 基準チャートが表示されます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 （84 ページ）およびCisco AI Network Analytics の概要 （11 ページ）を参照してください。 **重要** SSID 機械学習の基準チャートを表示するには、[Filter] オプションからサイトと SSID を選択する必要があります。 • 基準チャートの詳細は、異なる色で表示されます。 • **緑色のバンド**：予測基準値。 • **青色の実線**：実際の値。

[Client Count per SSID] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 次の 2 種類のチャートから構成されます。 • **Latest** • [Trend]：[Baseline] タブが含まれます。このタブでは、機械学習の基準チャートを表示できます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 （84 ページ）およびCisco AI Network Analytics の概要 （11 ページ）を参照してください。 チャートの上にマウスカーソルを合わせると、選択した時点の情報が同期化されたツールチップに表示されます。 チャート内の色付きセグメントをクリックすると、次の情報が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のワイヤレスクライアントの詳細データが格納されたテーブル。

[Connectivity Physical Link] ダッシュレット	
アイテム	説明
[Connectivity Physical Link] チャート	有線クライアントデバイスのリンクステートの分布。これは、物理リンクがアップ、ダウン、およびエラーであるクライアントデバイスの数です。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Switches]、[Top Host Device Types]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Count per Band] ダッシュレット	
アイテム	説明
[Client Count per Band] チャート	2.4 GHz 帯域または 5 GHz 帯域に接続されたワイヤレスクライアントの分布。 セグメントの上にカーソルを合わせると、特定の帯域に接続されているクライアントの割合と数が表示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Data Rate] ダッシュレット	
アイテム	説明
[Client Data Rate] チャート	クライアントのデータレートの分布。 使用しているクライアントプロトコルに基づいてクライアントをフィルタ処理するには、[Client Protocol] ドロップダウンリストを使用します。[802.11 n/ac/ax] または [802.11 a/b/g] を選択できます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

ステップ 7 ネットワーク内のクライアントに関する詳細情報を表示するには、[Client Devices] ダッシュレットを使用します。このダッシュレットには、次の機能があります。

[Client Devices] ダッシュレット	
アイテム	説明
[Type]	クライアントのタイプに基づいてテーブルをフィルタ処理します。オプションは、[Wired] および [Wireless] クライアントです。

[Client Devices] ダッシュレット	
アイテム	説明
ヘルス（**Health**）	次のオプションを使用して、クライアントの正常性を基にテーブルをフィルタリングします。 • すべて • Inactive：正常性スコアが 0 のクライアントデバイス。 • Poor：正常性スコアが 1 ～ 3 のクライアントデバイス。 • Fair：正常性スコアが 4 ～ 7 のクライアントデバイス。 • Good：正常性スコアが 8 ～ 10 のクライアントデバイス。 • No Data：データのないクライアントデバイス。
データ	次のオプションを使用して、データタイプを基にテーブルをフィルタリングします。 • [Onboarding Time >= 10 s]：オンボーディング時間が 10 秒（しきい値）以上。 • [Association >= 5 s]：関連付け時間が 5 秒（しきい値）以上。 • [DHCP >= 5 s]：DHCP 時間が 5 秒（しきい値）以上。 • [Authentication >= 5 s]：認証時間が 5 秒以上。 • [RSSI <= -72 dBm]：RSSI が -72 dBm（しきい値）以下。 • [SNR <= 9 dB]：SNR が 9 dB（しきい値）以下。

[Client Devices] ダッシュレット	
アイテム	説明
[Client Device] テーブル	

[Client Devices] ダッシュレット	
アイテム	説明
	詳細なクライアントデバイス情報を表形式で表示します。デフォルトでは、[Client Device] テーブルに次の情報が表示されます。 • [Identifier]：クライアントのユーザー ID、ホスト名、または MAC アドレスが、可用性に基づいてこの順序で表示されます。たとえば、ユーザー ID が使用不可能な場合は、ホスト名が表示されます。ユーザー ID とホスト名が使用不可能な場合は、MAC アドレスが表示されます。 [Identifier] 列には、クライアントデバイスが有線と無線のどちらであるかを判別できる固有のアイコンも表示されます。 • [MAC Address]：デバイスの MAC および Randomized and Changing MAC Address（RCM）を含む MAC アドレスが表示されます。プライベート MAC アイコンが RCM の前に表示されます。MAC アドレスのタイプ（すべて、デバイス MAC、RCM など）に基づいてテーブルをフィルタ処理できます。 • [IPv4 Address]：クライアントの IPv4 アドレスが、可用性に基づいて表示されます。 （注） メニューで [IPv6 Address] チェックボックスをオンにすると、クライアントの IPv6 アドレスを表示できます。 • [Device Type]：デバイスタイプが表示されます。 • [Health]：オンボーディングスコアと接続済みスコアの平均が表示されます。クライアント ヘルス スコアは 5 分ごとに計算されます。 （注） スコアが -- の場合、これはクライアントが直近でオンボーディングした（新規）ことを示します。新しいクライアントは、健全性スコア計算ウィンドウの開始5分後に、オンボードを試行するクライアントです。これらの新規クライアントのヘルススコアは、次回の5分間の計算ウィンドウに含まれます。 • **Last Seen** • [AP Name]（ワイヤレスクライアントの場合のみ）：アクセスポイントの名前が表示されます。 • [Switch]（有線クライアントの場合のみ） • [Port]（有線クライアントの場合のみ） • [Location]：クライアントの割り当て済みロケーションが表示されます。 • [Link Speed]（有線クライアントの場合のみ）：インターフェイスまたは物理ポートの速度容量を示します。ポートが特定の速度にネゴシエートされた場合は、ネゴシエートされた速度が表示されます。 （注）

[Client Devices] ダッシュレット	
アイテム	説明
	メニューで [Link Speed] チェックボックスをオンにすると、リンク速度を表示できます。
クライアントの [Client 360] の表示	クライアントデバイスの MAC アドレスまたは識別子をクリックすると、クライアントの 360 度ビューが表示されます。 [Client 360] には、クライアント接続の問題のトラブルシューティングに関する詳細情報が記載されています。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 2. 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。 3. [Apply] をクリックします。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。

クライアントデバイスの健全性のモニターとトラブルシューティング

この手順を使用して特定のクライアントデバイスに関する詳細情報を表示して、対処する必要がある潜在的な問題が存在するかどうかを判断します。

（注） HA フェールオーバーが発生した場合、クライアントの正常性データの表示に 1 時間かかることがあります。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

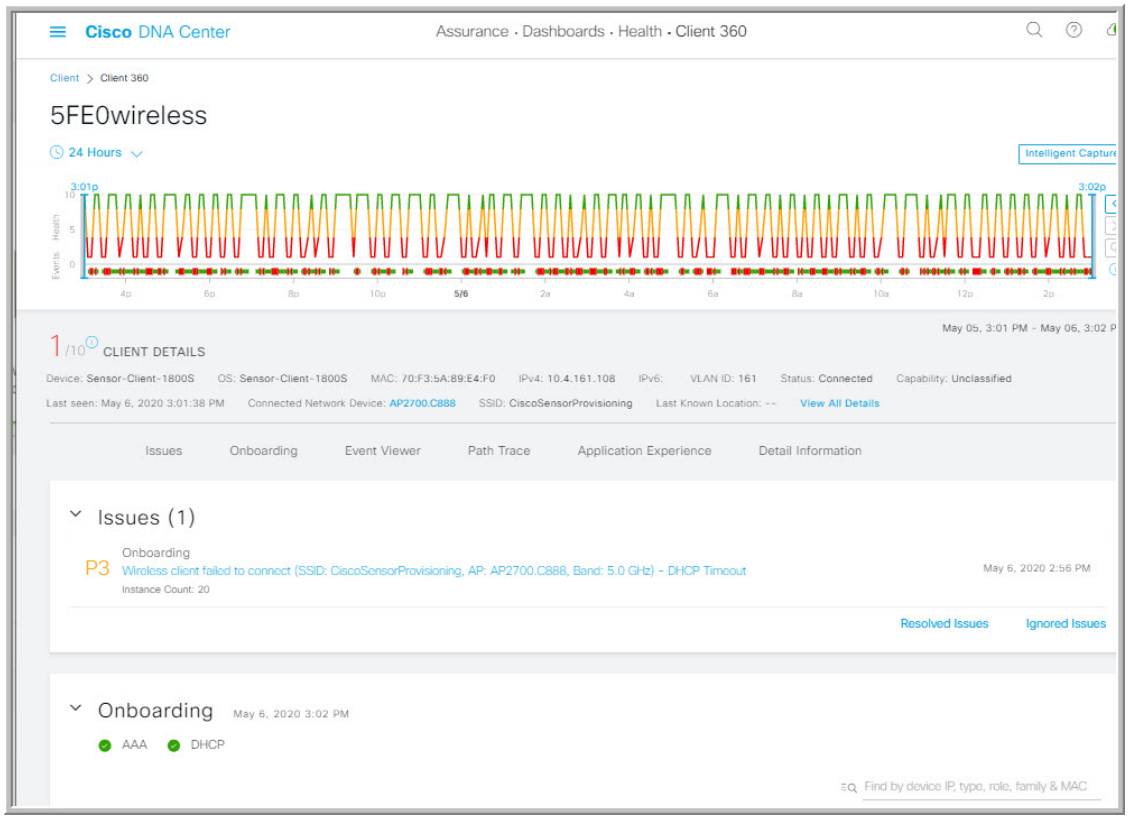
[Client Health] ダッシュボードが表示されます。

ステップ 3 次のいずれかを実行します。

- **[クライアントデバイス（Client Devices）]** 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索（Search）] フィールド（右上端）に次のいずれかを入力します。ユーザ ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレス。

[Client 360] ウィンドウに、クライアントデバイスの 360 度ビューが表示されます。

図 *13 : [クライアント 360（Client 360）] ウィンドウ*



ステップ 4 左上隅にある時間範囲設定（）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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 5 右上隅にある [Intelligent Capture] をクリックすると、特定のクライアントデバイスのキャプチャされたオンボーディングやデータパケットを表示、モニター、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。クライアントデバイスのライブキャプチャセッションの有効化 （346 ページ）を参照してください。

（注） インテリジェント キャプチャはすべての AP モデルでサポートされていません。[Intelligent Capture] が表示されない場合は、クライアントがサポート対象の AP モデルに接続されていること、また AP が [Network Health] ダッシュボード上の場所に割り当てられていることを確認します。

ステップ 6 タイムラインスライダの右上隅にある [Webex 360] をクリックして、クライアントの Webex ミーティングを表示し、監視します。ミーティング検索ポップアップウィンドウが表示されます。

a) クライアントの Webex ミーティングに関連付けられた電子メールアドレスを入力します。

b) [Search Meetings] をクリックします。[Application Experience for Webex] スライドインペインが表示されます。

c) このアプリケーション エクスペリエンス スライドインペインでは、次の機能を利用できます。

- **検索バー**：表示されたテーブルでミーティングを検索できます。
- **時間範囲フィルタ**：時間フィルタをクリックして、テーブルに表示するデータの時間範囲を指定します。
- クライアント ミーティング テーブルが表示されます。これには、ミーティング番号、ミーティング名、アプリケーション、ネットワーク接続時間、開始時刻、終了時刻、およびステータスが含まれます。

  ミーティングを選択して、ミーティングの品質KPIデータを表示できます。これは、アプリケーション（Webex API を使用して取得されたデータ）とネットワーク（NetFlow を使用して取得されたデータ）の遅延に基づくオーディオ品質、ビデオ品質、および共有品質を示す水平バーとしてテーブルの下に表示されます。ドロップダウンリストを使用して、送信および受信オプションに基づいてデータをフィルタ処理し、パケット損失、ジッターなどのメトリックに関連するアプリケーションとネットワークの遅延グラフを表示できます。

ステップ 7 タイムラインスライダを使用すると、一定期間のクライアントデバイスに関する正常性およびイベント情報を表示できます。タイムラインスライダには、次の機能があります。

- [Health]：タイムラインスライダの上にカーソルを合わせると、5 分の時間枠におけるクライアントの正常性スコアと KPI が表示されます。色付きの円が付いた KPI は、個々のクライアントの正常性スコアの算出に使用されます。

  （注） [Speed] KPI には、インターフェイスまたは物理ポートの速度容量が表示されます。ポートが特定の速度にネゴシエートされた場合は、ネゴシエートされた速度が表示されます。

  タイムラインをダブルクリックすると、1時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。各カテゴリ（[Issues]、[Onboarding]、[Event Viewer]、[Connectivity]など）の横にあるタイムスタンプも更新されます。

  （注） 1時間を超えて情報を表示する場合は、タイムラインスライダを必要な時間範囲に手動で移動します。

- [Onboarding]：タイムラインスライダにカーソルを合わせると、関連付け、認証、DHCP を含むクライアントのオンボーディング時間が表示されます。

- [Events]：イベントデータは、色分けされた垂直バーとしてグラフに表示されます。緑の垂直バーは、成功したイベントを示し、赤の垂直バーは失敗したイベントを示します。

  各垂直バーは、5分の時間枠を表します。各5分間ウィンドウに、複数の重要イベントが生成される場合があります。垂直バーにマウスカーソルを合わせると、イベントに関する詳細情報を取得できます。

ステップ 8 タイムラインの下にある [Client Details] 領域で、個々のクライアントの正常性スコアを確認します。

個々のクライアントの正常性スコアは、クライアントのオンボーディングステータス、RSSI、および SNR を集約したものです。

ユーザー ID で検索する場合、表示される個別のクライアント ヘルス スコアは、そのユーザーに関連付けられているすべての監視対象クライアント デバイスの最も低いスコアです。詳細については、「個別のクライアント ヘルス スコア （161 ページ）」を参照してください。

MAC アドレスまたは IP アドレスで検索する場合、個別のクライアント ヘルス スコアはそのクライアント デバイスのヘルス スコアです。

ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで計測されます。10 はベストスコアを示します。0はクライアントデバイスが非アクティブであり、該当する正常性データが存在しないことを示します。

- ●：クライアントデバイスが不適切です。ヘルス スコアの範囲は 1 ～ 3 です。
- ●：クライアントデバイスが適切です。ヘルス スコアの範囲は 4 ～ 7 です。
- ●：クライアントデバイスが良好です。ヘルス スコアの範囲は 8 ～ 10 です。
- ●：クライアントデバイスが非アクティブです。ヘルス スコアは 0 です。

（注） ネットワークから切断されているクライアントの場合、スコアは - と表示されます。

ステップ 9 タイムラインの下にある [Client Details] 領域で、次の情報を確認します。

- ワイヤレスクライアントの場合、このエリアには、その OS バージョン、MAC アドレス（デバイス MAC と RCM を含む）、IPv4 および IPv6 アドレス、接続された VLAN ID、接続ステータス、最終検出タイムスタンプ、接続されたネットワークデバイス、SSID、最後の既知のロケーションなどのクライアントデバイスに関する情報が表示されます。
- 有線クライアントの場合、このエリアには、MAC アドレス、IPv4 および IPv6 アドレス、接続された VLAN ID、接続ステータス、最終検出タイムスタンプ、接続されたネットワークデバイス、ポート、最後の既知のロケーションなどのクライアントデバイスに関する情報が表示されます。
- PoE 対応デバイスの場合、[IEEE Class]、[Negotiated Power Level]、および [PoE Status] の各要素もクライアント詳細エリアに表示されます。

ステップ 10 [Client Details] エリアで [View All Details] をクリックします。クライアントデバイスに関する追加の詳細を含むスライドインペインが開きます。

ステップ 11 問題、オンボーディング、イベントビューア、パストレース、アプリケーション エクスペリエンスに関する情報、および詳細情報を表示するには、折りたたみカテゴリを使用します。

問題のカテゴリ
対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。 問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。 スライドインペインでは、次の操作を実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （215 ページ）を参照してください。

オンボーディングカテゴリ
クライアントがどのようにネットワークに参加したかを示すトポロジ。AAA や DHCP などのサービスの情報も含まれます。 有線クライアントのトポロジの例：クライアント > スイッチ > ルータ ワイヤレス クライアント トポロジの例：クライアント > SSID > アクセス ポイント > ワイヤレス コントローラ トポロジでは、次の操作を実行できます。 • ノードをクリックして、ノードに関する情報が表示されたスライドインウィンドウを表示します。 • リンクの端（ドット）にマウスカーソルを合わせると、リンクのステータスとポートの詳細が表示されます。 • デバイスのグループにカーソルを合わせて、ポップアップから [View Devices List] をクリックすると、デバイスのリストとその詳細が表示されます。 • [Onboarding] エリアの右上隅にある [Search] フィールドで、特定のデバイスを検索できます。特定のノードが選択され、デバイスの対応する情報が表示されます。

イベントビューカテゴリ
[For Wireless Clients]：シナリオと、各シナリオにつながる一連のサブイベントが一覧されます。これにより、どのサブイベントの間に問題が発生したのかを特定できます。次のシナリオがワイヤレスコントローラ向けに用意されています。 • **再認証（Reauthentication）** • [Broadcast Rekey]：同一のキーによる暗号化データ量を制限するため、セッションキー（実行中の通信の暗号化キー）を変更するプロセス。 • **オンボーディング** • **DHCP** • **[Delete]** • **内部ローミング** • **内部ローミング** • **ASSOC** • **AUTH** • **EAP** • **DISASSOC** • **DEAUTH** • **11r 障害** • **OKC 障害** • **EAP 障害** 問題が発生するとイベントは赤色でマークされます。そうでない場合は緑色です。[Event Viewer] テーブルには、障害に関する情報（エラーメッセージ、クライアントが接続されている AP とワイヤレスコントローラ、イベント発生時のタイムスタンプなど）が表示されます。イベントをクリックすると、右側のペインにそのイベントに関する詳細情報が表示されます。 **有線クライアントの場合**:ISE サーバーイベント、スイッチシステムレベルの syslog、スイッチポートまたはインターフェイス固有のイベント、およびクライアント固有のイベントがリストされます。各イベントカテゴリのメッセージのリストについては、「有線クライアントのイベントビューアに表示されるメッセージ （158 ページ）」を参照してください。 成功したイベントは緑色で表示されます。正常性スコアに影響する障害イベントは赤色で表示されます。[Event Viewer] テーブルには、障害に関する情報（メッセージのタイプ、有線クライアントデバイスの接続先のデバイス情報、イベント発生時のタイムスタンプなど）が表示されます。イベントをクリックすると、右側のペインにそのイベントに関する詳細情報が表示されます。

パストレースのカテゴリ
[Run New Path Trace] をクリックすると、指定した送信元デバイスと接続先デバイス間のネットワークトポロジが表示されます。トポロジには、パスの方向とパスに沿ったデバイスが、その IP アドレスを含めて含まれます。ディスプレイには、パスに沿ったデバイスのプロトコル（**Switched**、**STP**、**ECMP**、**Routed**、**Trace Route**）や、その他のソース タイプも表示されます。 パス トレースの実行 （375 ページ） を参照してください。

アプリケーションエクスペリエンスのカテゴリ
クライアント デバイスで実行中のアプリケーション、およびその質的および量的なメトリック。 メトリックをチャート形式で表示するには、テーブル内のアプリケーションの横にあるオプションボタンをクリックします。関連する情報を示すスライドインペインが開きます。 アプリケーション エクスペリエンスとアプリケーションの可視性について （163 ページ）およびホストのアプリケーション エクスペリエンスの表示 （172 ページ）を参照してください。

詳細情報のカテゴリ
次のタブのいずれかをクリックして、対応する情報を表示します。 • [Device Info]：デバイスについての基本情報が表示されます。Samsung デバイスについては、このタブに、ビルド番号、製造元、国番号、デバイスタイプ（モバイル、タブレットなど）、ホストのオペレーティングシステムといった詳細情報が表示されます。 • [RF]：ワイヤレスデバイスでのみ使用できます。 • [User Defined Network]：UDN 対応のネットワークデバイスでのみ使用できます。このタブには、登録済みの UDN、接続された UDN の詳細、デバイスの MAC アドレス、デバイスの所有者、デバイス名、デバイスタイプ、および現在のステータスが表示されます。 • [Connectivity]：[Retries] という新しい接続 KPI が表示されます。無線接続の再試行回数が再試行チャートに表示されます。 • [PoE]：このタブは、PoE 対応クライアントで使用できます。 • [iOS Analytics]：Apple デバイスでのみ使用できます。

有線クライアントのイベントビューアに表示されるメッセージ

[Client 360] ウィンドウで有線クライアントの**イベントビューア**に表示されるメッセージのリストを次の表に示します。

ISE サーバーイベント
Client AUTH FAILURE Client AUTH SUCCESS

スイッチシステムレベルの syslog
ALLDEADSERVER • 到達不可能なデバイス • 到達可能デバイス

スイッチポートまたはインターフェイス固有のイベント
トラップイベント • リンクダウン • リンクアップ PM-4-ERR_DISABLE ILPOWER-5-POWER_GRANTED ILPOWER-5-IEEE_DISCONNECT ILPOWER-5-INVALID_IEEE_CLASS ILPOWER-4-LOG_OVERDRAWN ILPOWER-3-SHUT_OVERDRAWN

クライアント固有のイベント
DOT1X-5-FAIL MAB-5-FAIL

クライアントの正常性スコアと KPI メトリックについて

ここでは、クライアントの正常性スコアと KPI メトリックの計算方法について説明します。

クライアント ヘルス スコア

クライアントの正常性スコア（ワイヤレスまたは有線）は、ターゲットカテゴリ内の正常なクライアントデバイスの数（正常性スコアが 8 ～ 10）をそのカテゴリのクライアントデバイスの総数で割ったパーセンテージです。スコアは 5 分ごとに計算されます。

例：90 %（ヘルス スコア）= 90（ターゲット カテゴリのヘルス スコアが 8 ー 10 のクライアント デバイス）÷ 100（そのカテゴリのクライアント デバイスの総数）

個々のクライアント ヘルス スコアは、クライアント オンボーディング スコアとクライアント接続スコアの合計です。クライアント ヘルス スコアの範囲は 1 ～ 10 で、非アクティブなクライアントのスコアは 0 です。これは、次のとおり計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態で、認証および認可が成功し、IP アドレスを受信しています。クライアント スコアは 10 です。

ワイヤレスクライアント：クライアントがネットワークに参加しており、RSSI および SNR KPI の観点から接続が良好な状態です。

クライアント オンボーディング スコア

クライアント オンボーディング スコアは、ネットワークに接続中のクライアント デバイスのエクスペリエンスを示します。

- クライアントがネットワークに正常に接続している場合、スコアは 4 です。
- クライアントがネットワークに接続できない場合、スコアは 1 です。
- クライアントがアイドル状態の場合、スコアは 0 です。

クライアント オンボーディング スコアは、次のように計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態であり、認証と認可に成功しており、IP アドレスが受信されています。

ワイヤレスクライアント：クライアント オンボーディング スコアの範囲は 1 ー 4 です。クライアントがネットワークに正常に接続している場合、スコアは4です。クライアントがネットワークに接続できない場合、スコアは 1 です。

クライアント接続スコア

クライアント接続スコアは、デバイスがネットワークに接続された後のクライアントデバイスのエクスペリエンスを示します。スコアは、次のように計算されます。

有線クライアント：接続スコアは、2または6になります。リンクエラーにより、次のように、接続スコアとその結果の全体的な正常性スコアが決まります。

- クライアント オンボーディングは正常に行われたもののリンクエラーが発生した場合、接続スコアは 2、全体的な正常性スコアは 6 です。
- クライアント オンボーディングが正常に行われ、クライアントとファーストホップスイッチの間にリンクエラーが発生していない場合、接続スコアは 6、全体的なヘルススコアは 10 です。

ワイヤレスクライアント：接続スコアは、0、4、または 10 になります。RSSI と SNR の範囲によって接続スコアが決定され、その結果の全体的なヘルス スコアは RSSI 主導の接続スコアと SNR 主導の接続スコアの加重平均として計算されます。

RSSI 主導の接続スコア	
クライアントの RSSI	**RSSI 主導の接続スコア**
RSSI が -72 dBm 以下の場合。	クライアントは、RSSI 主導の接続スコア 4 を獲得し、正常性が中程度であると見なされます。
RSSI が -72 dBm より大きい場合。	クライアントは、RSSI 主導の接続スコア 10 を獲得し、正常性が良好であると見なされます。

SNR 主導の接続スコア	
クライアントの SNR	**SNR 主導の接続スコア**
SNR が 9 以下の場合。	クライアントは、SNR 主導の接続スコア 4 を獲得し、正常性が中程度であると見なされます。
SNR が 9 より大きい場合。	クライアントは、SNR 主導の接続スコア 10 を獲得し、正常性が良好であると見なされます。

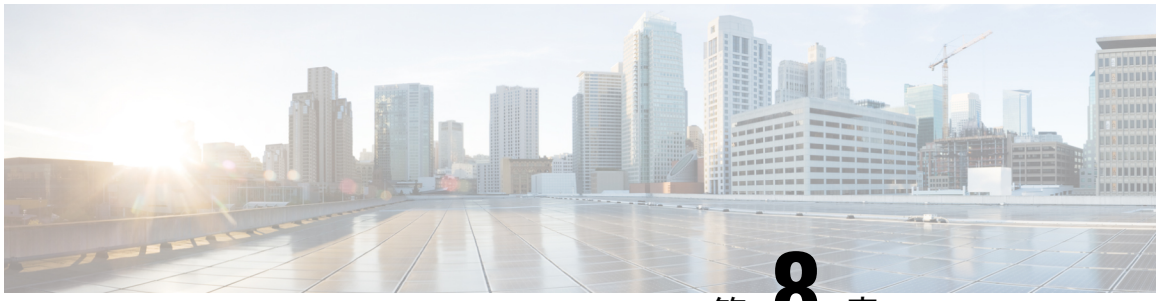
個別のクライアント ヘルス スコア

個々のクライアント ヘルス スコアは、クライアント オンボーディング スコアとクライアント接続スコアの合計です。クライアント ヘルス スコアの範囲は 1 ～ 10 で、非アクティブなクライアントのスコアは 0 です。これは、次のとおり計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態で、認証および認可が成功し、IP アドレスを受信しています。クライアントスコアは 10 です。

ワイヤレスクライアント：クライアントがネットワークに参加しており、RSSI および SNR KPI の観点から接続が良好な状態です。

クライアントのオンボーディングと接続性	クライアント正常性スコアの結果
クライアントがオンボーディングに失敗した場合。	クライアントの正常性スコアは 1 で、不良な状態であると見なされます。
クライアントの RSSI と SNR がしきい値を下回っている場合。	クライアントの正常性スコアは 4 で、正常性が中程度であると見なされます。
クライアントの RSSI と SNR のいずれかがしきい値を下回っている場合。	クライアントの正常性スコアは 7 で、正常性が中程度であると見なされます。
クライアントの RSSI と SNR がしきい値を超えている場合。	クライアントの正常性スコア 10 で、正常性が良好であると見なされます。



第 8 章

アプリケーション健全性のモニター

アプリケーションエクスペリエンスとアプリケーションの可視性について

アシュアランスは、複雑なアプリケーションデータを処理し、その結果をアシュアランス正常性ダッシュボードで提示することで、アプリケーションのパフォーマンスに関するインサイトを提供します。

正常性データは、デバイスの観点（[Device 360] ウィンドウ）、ユーザーの観点（[Client 360] ウィンドウ）、アプリケーションの観点（[Application 360] ウィンドウ）でそれぞれ提供されます。

データの収集元に応じて、次の一部またはすべての情報を確認できます。

- Application Name
- スループット
- DSCP マーキング
- パフォーマンスメトリック（遅延、ジッター、パケット損失）

アプリケーション名とスループットを総称して定量的メトリックと呼びます。定量的メトリックのデータは、アプリケーション可視性を有効にすることで得られます。

DSCP マーキングとパフォーマンスメトリック（遅延、ジッター、パケット損失）は、総称して定性的メトリックと呼ばれます。定性的メトリックのデータは、アプリケーションエクスペリエンスを有効にすることで得られます。

アプリケーションの可視性

アプリケーション可視性のデータは、IOS-XE を実行しているスイッチ、および AireOS を実行しているワイヤレスコントローラから取集されます。

IOS-XE を実行しているスイッチについては、物理レイヤのアクセススイッチポートに双方向（入力および出力）で適用される事前定義された NBAR テンプレートを使用してアプリケーション可視性のデータが収集されます。

AireOS を実行している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でアプリケーション可視性のデータが収集され、そのデータがストリーミングテレメトリを使用して Cisco DNA Center に送られます。

Application Experience

アプリケーションエクスペリエンスのデータは、Cisco IOS-XE ルータプラットフォームから、Cisco Performance Monitor（PerfMon）機能とシスコのアプリケーション応答時間（ART）メトリックを使用して収集されます。

ルータプラットフォームの例には、ASR 1000、ISR 4000、CSR 1000v などがあります。Cisco DNA Center と互換性があるデバイスについては、『Cisco DNA Center Supported Devices』を参照してください。

Cisco Performance Monitor 機能が使用可能かどうかを確認するには、Cisco Feature Navigator ツールを使用します。[Research Features] をクリックし、フィルタフィールドで [Easy Performance Monitor Phase II] を追加します。

最適化アプリケーション パフォーマンス モニタリング

最適化アプリケーションパフォーマンスモニタリング（APM）は、デバイスでの NetFlow データの収集に関連するオーバーヘッドを軽減する機能です。APM は、Cisco IOS-XE ルータ、Cisco 9800 シリーズ ワイヤレス コントローラ、および Cisco DNA トラフィック テレメトリ アプライアンスでサポートされています。最小ソフトウェアバージョンについては、サポートされるプラットフォーム （164 ページ）を参照してください。

サポートされるプラットフォーム

次の表に、サポートされるプラットフォーム、データ収集のタイプ、およびソフトウェアとライセンスの要件を示します。

（注） Cisco DNA Center と互換性があるデバイスについては、『Cisco DNA Center Supported Devices』を参照してください。

シスコのプラットフォームにおけるアプリケーション エクスペリエンスとアプリケーション可視性のサポート **Cisco DNA Center**		
プラットフォーム	**Data Collection**	**注記**
Cisco IOS-XE ルータ	アプリケーション エクスペリエンスのデータ収集	• アクティブな NBAR2 ライセンスが必要。 • IOS XE 16.3 以上のソフトウェアバージョン。 • 最適化 APM の場合：IOS XE 17.3 以上のソフトウェアバージョン。
Catalyst 9000 シリーズ スイッチ	9200、9300、9400 のアプリケーション可視性のデータ収集	• Cisco DNA Advantage ライセンスが必要。 • IOS XE 16.10.1 以上のソフトウェアバージョン。
Cisco AireOS ワイヤレスコントローラ	アプリケーション可視性のデータ収集	• Cisco DNA Advantage ライセンスが必要。 • 8.8 MR2 ソフトウェアが必要：8.8.114.130 以上のバージョン。
Cisco 9800 シリーズ ワイヤレス コントローラ	Flex/Fabric SSID のアプリケーション可視性のデータ収集。 中央スイッチング/ローカル SSID のアプリケーション エクスペリエンスのデータ収集。	• 最適化 APM の場合：IOS XE 16.12.1 以上のソフトウェアバージョン。
Cisco DNA トラフィック テレメトリ アプライアンス	アプリケーション エクスペリエンスのデータ収集。	• Cisco DNA Advantage ライセンスが必要。 • 最適化 APM の場合：IOS XE 17.3 以上のソフトウェアバージョン。

デバイスでのアプリケーションテレメトリ有効化の基準

Cisco DNA Center では、新しい自動選択アルゴリズムに基づいてインターフェイスと WLAN を選択し、該当するすべてのインターフェイスと WLAN でアプリケーションテレメトリを自動的に有効にします。

アプリケーションテレメトリは、Cisco DNA Center を介してプロビジョニングされた WLAN にプッシュされます。

（注）
- 従来のタギングベースのアルゴリズムがサポートされ、インターフェイスまたは WLAN の新しい自動選択アルゴリズムよりも優先されます。
- 自動選択アルゴリズムからタギングベースのアルゴリズムに切り替える場合は、タグ付き SSID をデバイスに対してプロビジョニングする前にテレメトリを無効にする必要があります。

次の表に、サポートされているすべてのプラットフォームについて、従来のタギングベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムに基づくインターフェイスと WLAN の選択基準を示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Router	• インターフェイスの説明に **lan** キーワードが含まれている。[12] • インターフェイスが物理インターフェイスである。 • インターフェイスに管理 IP アドレス以外の IP アドレスがある。	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれでもない。 • WAN （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。 このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。 ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。 • ループバック • 管理インターフェイス：GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム

スイッチ	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2]
	• スイッチポートがアクセスポートとして設定されている。
	• スイッチポートに **switch-mode access** コマンドが設定されている。
		• インターフェイスが物理インターフェイスである。
		• アクセスポートにネイバーがない。
		• インターフェイスが次のいずれでもない。
		  • 管理インターフェイス：FASTETHERNET0、FASTETHERNET1、GIGABITETHERNET0/0、MGMT0
		  • LOOPBACK0、Bluetooth、App Gigabit、WPAN、Cellular、Async
		  • VSL インターフェイス

Cisco AireOS コントローラ	• WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	• ゲスト SSID ではない。
		  • WLAN がゲストタイプとして設定されていない。
		  • SSID の名前に **guest** キーワードが含まれていない。
		• SSID がローカルモードで設定されている。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ と最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS リリース 16.12.1 以降	• WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]
	• WLAN がローカルモードで設定されている。
		• ゲスト SSID ではない。
		  • WLAN がゲストタイプとして設定されていない。
		  • SSID の名前に **guest** キーワードが含まれていない。
		• SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべての SSID がローカルモードの場合、最適化 APM レコードが設定されます。

	（注） テレメトリ設定を更新する場合は、テレメトリを無効にしてから、設定の変更後にテレメトリを有効にする必要があります。	

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Cisco DNA トラフィック テレメトリ アプライアンス と最適化 APM プロファイルおよび IOS リリース 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

[1] **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。
[2] ネットワークデバイスを再同期して、**lan** インターフェイスの説明を読み取ります。

アプリケーションの正常性の前提条件

ここでは、ルータ、AireOS ワイヤレスコントローラ、スイッチのアプリケーションの正常性に関連する前提条件を示します。

ルータのアプリケーション エクスペリエンスの前提条件

- Cisco IOS XE ソフトウェアのアクティブな NBAR2 ライセンスが必要です。
- レイヤ 3 ネットワーク内のアプリケーションフローは可視化されません。
- 管理インターフェイスに関連付けられたトラフィックは、アプリケーションエクスペリエンスに含まれません。
- ポートは ETA に対して有効にできません。
- アシュアランス でアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイスの間でクロックを同期する必要があります。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスと WLAN の新しい自動選択アルゴリズムにより、キーワード「**lan**」でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （166 ページ）を参照してください。

スイッチのアプリケーション可視性の前提条件

- Cisco IOS XE ソフトウェアが必要です。
- Cisco DNA Advantage ライセンスが必要です。
- **switchport mode access** コマンドが含まれているアクセスポートにのみ実装されます。

- L2 論理インターフェイスのサポートは使用できません。
- スイッチポートが AP に接続されて **switchport mode access** が設定されている場合、可視性が制限されます。
- ポートは ETA に対して有効にできません。
- IPv4 フローのみがモニターされます。
- 管理インターフェイス Gig0/0 は、NetFlow エクスポートの送信元インターフェイスとして使用できません。
- アシュアランス でアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイスの間でクロックを同期する必要があります。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスと WLAN の新しい自動選択アルゴリズムにより、キーワード「**lan**」でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （166 ページ）を参照してください。

AireOS ワイヤレスコントローラのアプリケーション可視性の前提条件

- Cisco DNA Advantage ライセンスが必要です。
- AireOS ソフトウェアを搭載したワイヤレスコントローラでのみサポートされ、IOS XE ソフトウェアを搭載したワイヤレスコントローラではサポートされません。
- Cisco AireOS ワイヤレスコントローラでは NetFlow を有効にする必要があります。
- アシュアランス でアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイスの間でクロックを同期する必要があります。
- Flexible NetFlow（FNF）フローモニターは実装されません。代わりに、Client-app-stat-events チャネルに登録することにより、ストリーミングテレメトリを使用してアプリケーション可視性のデータが収集されます。
- SSID は、ローカルモードで設定されています（Flex やファブリックではありません）。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスと WLAN の新しい自動選択アルゴリズムにより、キーワード「**lan**」でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （166 ページ）を参照してください。

Cisco 9800 シリーズ ワイヤレス コントローラのアプリケーション可視性の前提条件

- 最適化 APM には IOS XE ソフトウェアが必要です。デバイスでのアプリケーションテレメトリ有効化の基準 （166 ページ）を参照してください。

- アシュアランス でアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイスの間でクロックを同期する必要があります。

アプリケーション エクスペリエンスの前提条件 Cisco DNA トラフィック テレメトリ アプライアンス

- Cisco DNA Advantage ライセンスが必要です。
- 最適化 APM には IOS XE ソフトウェアが必要です。デバイスでのアプリケーションテレメトリ有効化の基準 （166 ページ）を参照してください。
- アシュアランス でアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイスの間でクロックを同期する必要があります。
- CAPWAP でカプセル化されたワイヤレストラフィックの可視性を有効にするには、Cisco DNA トラフィック テレメトリ アプライアンス で**ip nbar Classification tunneled-traffic CAPWAP** コマンドを手動で入力します。

アプリケーションテレメトリ設定のプロビジョニング

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （83 ページ） の説明に従って、グローバルテレメトリ設定を構成します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、建物、またはフロアを選択します。

ステップ 2 プロビジョニングするデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Telemetry] を選択し、次のいずれかを実行します。

（注） アプリケーションテレメトリのオプションは、Cisco DNA Center からのアプリケーションテレメトリの有効化がデバイスでサポートされている場合にのみ有効になります。

a) [Enable Application Telemetry]：選択したデバイスでアプリケーションテレメトリを設定します。
b) [Disable Application Telemetry]：選択したデバイスからアプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

[Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で

[Application Telemetry] 列が表示されない場合は、列見出しの右端にある [More] アイコン（⋮）をクリックし、[Application Telemetry] チェックボックスをオンにします。

ホストのアプリケーション エクスペリエンスの表示

ホストで稼働しているアプリケーションの質的および量的なメトリックを確認するには、次の手順を実行します。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （171 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （169 ページ）を参照してください。

ステップ 1 [Client 360] ウィンドウで、[Application Experience] カテゴリを展開します。

ステップ 2 [Application Experience] カテゴリから、次の操作を実行できます。

a) 特定のビジネス関連グループから、それに対応するタブをクリックすることで、アプリケーション エクスペリエンス データをテーブル形式で表示します。タブは、[Business Relevant]、[Business Irrelevant]、または [Default] です。

（注） 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]、[7 Days] です。デフォルトは、[24 Hours] です。

b) テーブルでアプリケーション エクスペリエンス データを表示します。

- [Name]：アプリケーション名。
- [Health]：正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。詳細については、個別アプリケーションの正常性スコア （185 ページ）を参照してください。
- [Usage Bytes]：このアプリケーションに対してクライアントが転送したバイト数。
- [Average Throughput]：クライアントとサーバー間を流れているアプリケーション トラフィックのレート（Mbps 単位）。
- [DSCP]：アプリケーションの現在（[Observed]）とデフォルト（[Expected]）の DSCP 値。

  （注） このメトリックは、最適化 APM については提供されません。

- [Packet Loss]：パケット損失のパーセンテージ（最小と平均）。

- [Network Latency]：ネットワーク遅延時間（最大と平均）（ミリ秒単位）。
- [Jitter]：ネットワーク上のデータパケット間の時間遅延のバリアンス（ミリ秒単位）（最大と平均）。

c) アプリケーション エクスペリエンス メトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、および [Application Server Latency] です。

（注） Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレス コントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

ネットワークデバイスのアプリケーションエクスペリエンスの表示

この手順を使用して、ネットワークデバイスで稼働しているアプリケーションの質的および量的なメトリックを表示できます。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （171 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （169 ページ）を参照してください。

ステップ 1 [Device 360] ウィンドウで、[Application Experience] カテゴリを展開します。

ステップ 2 [Application Experience] カテゴリから、次の操作を実行できます。

a) 対応するタブ（[Business Relevant]、[Business Irrelevant]、[Default]）をクリックして、特定のビジネスとの関連性グループからアプリケーション エクスペリエンス データを表形式で表示します。

（注） 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]（デフォルト）、または [7 Days] です。

b) 適切なフィルタ（[All VRFs] および [All Interfaces]）を使用して、特定の VRF または特定のルータインターフェイスのアプリケーション エクスペリエンス データをフィルタ処理します。

（注） [All VRFs] および [All Interfaces] フィルタは、ルータでのみ使用できます。

c) テーブルでアプリケーション エクスペリエンス データを表示します。

- [Name]：アプリケーション名。
- [Health]：正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。

（注） 正常性スコアは、Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレス コントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。

- [Usage Bytes]：このアプリケーションに対してクライアントが転送したバイト数。
- [Average Throughput]：クライアントとサーバー間を流れているアプリケーション トラフィックのレート（Mbps 単位）。
- [DSCP]：アプリケーションの現在（[Observed]）とデフォルト（[Expected]）の DSCP 値。

（注） このメトリックは、最適化 APM については提供されません。

- [Packet Loss]：パケット損失のパーセンテージ（最小と平均）。
- [Network Latency]：ネットワーク遅延時間（最大と平均）（ミリ秒単位）。
- [Jitter]：ネットワーク上のデータパケット間の時間遅延のバリアンス（ミリ秒単位）（最大と平均）。

d) アプリケーション エクスペリエンス メトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、[Application Server Latency]、および [Application Response Time] です。

（注） Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレス コントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

すべてのアプリケーションの健全性のモニター

この手順を使用して、サイトにおけるアプリケーションのグローバルビューを表示します。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲を使用したネットワークの検出 （30 ページ）、CDP を使用したネットワークの検出 （23 ページ）、またはLLDP を使用したネットワークの検出 （36 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （171 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （169 ページ）を参照してください。

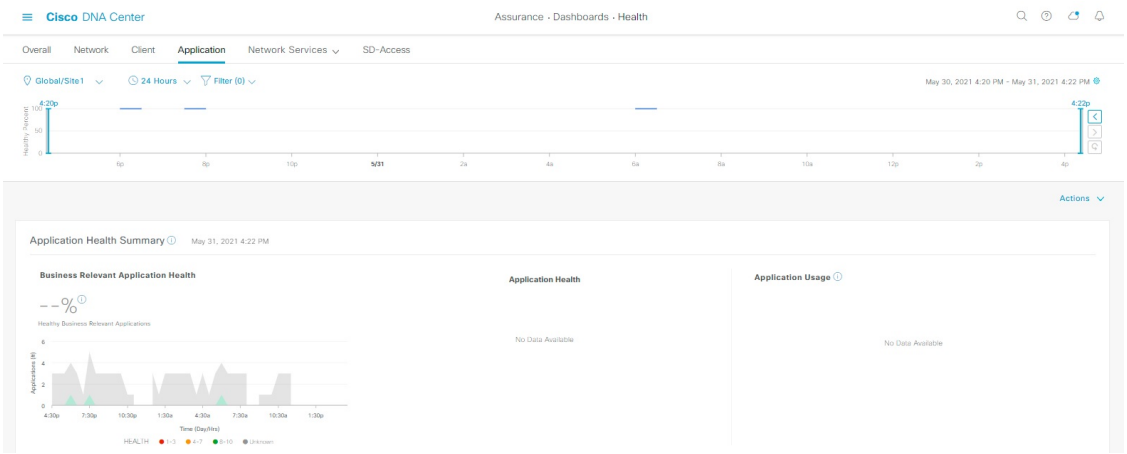
ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

図 *14 : [Application Health]* ダッシュボード



ステップ 3 次の機能には、[Application] 正常性ダッシュボードの上部のメニューバーを使用します。

[Application] 正常性ダッシュボードの上部のメニューバー	
アイテム	**説明**
Global [Location] ドロップダウン リスト	クリックすると、ロケーションアイコンが表示されます。ロケーションアイコンをクリックすると、[Site List View] が表示されます。特定のサイトまたはビルディングからアプリケーション情報を表示するには、適切な行で[Apply] をクリックします。ダッシュボード上の情報が、選択に応じて更新されます。

[Application] 正常性ダッシュボードの上部のメニューバー	
アイテム	説明
 [Time Range] 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。 **1.** 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。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。
Filter	ドロップダウンリストから SSID を選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。
[Actions] ドロップダウン リスト	ドロップダウンリストから [Edit Dashboards] を選択すると、ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ）およびカスタム ダッシュボードの作成 （313 ページ）を参照してください。
アプリケーションの正常性タイムラインスライダ	正常なビジネス関連アプリケーションの割合を、より詳細な時間範囲で表示できます。タイムライン内でマウスカーソルを合わせると、特定の時刻の正常性スコアパーセンテージが表示されます。 時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、ダッシュボードダッシュレットに表示されるアプリケーションデータのコンテキストが設定されます。 タイムラインの右側にある矢印ボタンを使用して、最大 30 日間のデータを表示できます。

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

[Application Health Summary] ダッシュレット	
アイテム	説明
[Business Relevant Application Health]	ビジネス関連アプリケーションの正常性スコアが表示されます。正常性スコアは、ネットワーク全体または選択したサイトにおける正常（良好）なビジネス関連アプリケーションの割合です。アプリケーションのヘルス スコアと KPI メトリックスの理解 （185 ページ）を参照してください。 次のチャートが表示されます。 • アプリケーション数分布トレンドチャートでは、すべてのビジネス関連のアプリケーション数が、正常性スコアに基づき積み上げ面グラフで時系列順に表示されます。 • 円グラフでは、ビジネス関連のアプリケーション数が、アプリケーションの正常性スコア別に分類されて示されます。カテゴリをクリックすると、カテゴリ内で正常性スコアが最も低いアプリケーションのリストが表示されます。
[Application Usage]	• 円グラフ：アプリケーションのビジネス関連性グループによって分類されたアプリケーション使用率の合計が表示されます。カテゴリをクリックすると、カテゴリ内の使用状況別に、上位 10 個のアプリケーションのリストが表示されます。 （注） アプリケーションの使用状況は、アプリケーションの双方向トラフィックから取得されます。 • 詳細の表示：[View Details] をクリックすると、追加の詳細情報を含むスライドインペインが開きます。スライドインペインでは、次の操作を実行できます。 • [All Applications]、[Business Relevant]、[Business Irrelevant]、および [Default] タブをクリックすると、アプリケーションの使用率と使用率別上位 10 個のアプリケーションが記載されたチャートが表示されます。 • スライドインペインの右上にあるドロップダウンリストを使用すると、アプリケーショングループまたはトラフィッククラス別にチャートをフィルタリングできます。 • チャート内のカテゴリをクリックすると、[Application] テーブルにアプリケーションとその詳細情報が表示されます。

ステップ 5 次の機能については、[Application] ダッシュレットを使用します。

[Application] ダッシュレット	
アイテム	**説明**
[Type]	ビジネス関連性グループに基づいてテーブルをフィルタリングします。オプションは、[Business Relevant]、[Business Irrelevant]、および [Default] です。
[Health]	アプリケーションの正常性スコアに基づいてテーブルをフィルタリングします。次のオプションがあります。 • [Poor]：正常性スコアが 1 ～ 3 のアプリケーション。 • [Fair]：正常性スコアが 1 ～ 3 のアプリケーション。 • [Good]：正常性スコアが 8 ～ 10 のアプリケーション。 • [All]：すべてのアプリケーション。 • [Unknown]：アプリケーションに正常性スコアを決定するための定性的なメトリックがありません。

[Application] ダッシュレット	
アイテム	説明
[Applications] テーブル	アプリケーションの詳細情報を表形式で表示します。デフォルトでは、[Application] テーブルには次の情報が表示されます。 • [Name]：アプリケーション名が表示されます。アプリケーション名は、シスコの次世代 Network-Based Application Recognition（NBAR）の標準アプリケーションに基づいています。 （注） アプリケーション ポリシー パッケージを使用してアプリケーション名を変更しても、変更した名前はアプリケーションエクスペリエンスに表示されません。現在、アプリケーション ポリシー パッケージとアプリケーション エクスペリエンスは統合されていません。 （注） アプリケーションが NBAR の標準アプリケーションでない場合は、その HTTP ホスト名または SSL 共通名が表示されます（使用可能な場合）。これらのアプリケーションは、[Default] ビジネス関連性グループに割り当てられています。 アプリケーション名をクリックして、アプリケーションの 360 度ビューを表示することもできます。アプリケーションの健全性のモニター（180 ページ）を参照してください。 • [Health]：アプリケーションの正常性スコアが表示されます。 • [Business Relevance]：可能な値は、[Business Relevant]、[Business Irrelevant]、および [Default] です。 • [Usage Bytes]：このアプリケーションに転送されたバイト数。 • [Average Throughput]：クライアントとサーバー間のアプリケーショントラフィックのフローレート（Mbps 単位）。 • [Packet Loss（%）]：パケット損失の割合。 • [Network Latency]：ネットワークの遅延時間（ミリ秒単位）。Transmission Control Protocol（TCP）ベースのアプリケーションの場合。 • [Jitter]：ネットワーク上のデータパケット間の時間遅延の差異（ミリ秒単位）。Real-time Transport Protocol（RTP）ベースのアプリケーションの場合。

[Application] ダッシュレット	
アイテム	説明
⋮	テーブルに表示するデータをカスタマイズします。 1. ⋮ をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。

アプリケーションの健全性のモニター

この手順を使用して、特定のアプリケーションの詳細を表示します。

ステップ 1 [Health]メニューアイコン（≡）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

ステップ 3 [Application] テーブルで、アプリケーション名をクリックします。

[Application 360] ウィンドウが開き、アプリケーションの 360 度ビューが表示されます。

ステップ 4 左上隅にある時間範囲設定（🕓）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) [Start Date] と時刻、[End Date] と時刻を指定します。
c) [Apply] をクリックします。

ステップ 5 特定のロケーションのアプリケーション情報を表示するには、[Location] ドロップダウンリストからロケーションを選択します。

ステップ 6 [Filter] ドロップダウンリストから SSID を選択し、[Apply] をクリックして特定の SSID の情報を表示します。

ステップ 7 アプリケーションの正常性タイムラインスライダを使用して、より詳細な時間範囲のアプリケーションの正常性スコアやアプリケーションの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Health Score]：特定の時点の正常性スコアが表示されます。[Quality] 領域のメトリックの色分けは正常性スコアに対応しています。

[Quality]：[Quality] 情報領域には、遅延、ジッター、およびパケット損失に関する情報が表示されます。遅延については、クライアントとアプリケーションの間の遅延に関する次の情報が表示されます。

- LAN の遅延：クライアントとルータの間の遅延（ミリ秒）。
- WAN の遅延：ルータとサーバーの間の遅延（ミリ秒）。
- アプリケーションの遅延：サーバーとアプリケーションの間の遅延（ミリ秒）。

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、[Application 360] ウィンドウに表示されるアプリケーションデータのコンテキストが設定されます。

ステップ 8 タイムラインの下にある [Application Details] 領域で、次の情報を確認します。

Application Details	
アイテム	**説明**
[Health Score]	アプリケーションの正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、およびジッター）の加重平均に基づいて計算されます。 （注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。
[Time and Date] 範囲	[Application 360] ウィンドウに表示されているデータの時刻と日付の範囲が表示されます。
[Business Relevance [Traffic Class] **Category**	アプリケーションの次世代 Network-Based Application Recognition（NBAR）分類情報を表示します。
[Issues] タブ	クリックすると、問題のリストが表示されます。手順 8 を参照してください。
[Exporters] タブ	クリックすると、NetFow トラフィックを Cisco DNA Center に送信するデバイスのリストとその他の詳細情報が表示されます。手順 9 を参照してください。

ステップ 9 [Issues] をクリックして、次の情報を確認します。

問題
対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。 問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。 スライドインペインでは、次の操作を実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （215 ページ）を参照してください。

ステップ 10 [Exporters] をクリックして、次の情報を確認します。

エクスポータ	
アイテム	**説明**
[Device]	NetFlow トラフィックを Cisco DNA Center に送信しているデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アプライアンスなど）のリストが表示されます。
[Health Score]	直近の 5 分間の正常性スコア。正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、ジッターなど）に基づいて計算されます。 （注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよびCisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要なKPI をポーリングしません。
[Traffic Class]	該当する場合にアプリケーションのNBAR 分類情報が表示されます。

エクスポータ	
アイテム	説明
[Go to Device 360]	クリックすると、特定のデバイスの [Device 360] ウィンドウが開きます。

ステップ 11 メトリックチャートを表示するには、次の手順を実行します。

- ルータおよびアプライアンスの場合は、エクスポータの行をクリックします。その行の下に、使用状況、平均スループット、パケット損失、ジッター、および遅延のメトリックについてのチャートが表示されます。
- スイッチおよびワイヤレスコントローラの場合は、デバイス名をクリックします。スライドインペインが開き、使用状況および平均スループットのメトリックについてのチャートが表示されます。

  また、スライドインペインで [Device 360] をクリックして、特定のデバイスの [Device 360] ウィンドウを開くこともできます。

メトリック グラフ	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Thoughput]	クライアントとサーバーの間のアプリケーション トラフィックのレート（Mbps）。
[Packet Loss]	パケット損失のパーセンテージ（最大と平均）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Latency]	ネットワークの遅延時間（最大と平均）（ミリ秒単位）。次の遅延のチャートが提供されます。 • ネットワーク遅延 • クライアントネットワークの遅延 • サーバーネットワークの遅延 • アプリケーション ネットワークの遅延 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Jitter]	ネットワーク上のデータ パケット間の時間遅延（最大および平均）の差異（ミリ秒単位）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。

メトリック グラフ	
チャート	説明
[DSCP]	• [Observed]：アプリケーションの現在の DSCP 値。 • [Expected]：NBAR によって割り当てられたデフォルトの DSCP 値。 （注） このメトリックは、最適化APMについては提供されません。

ステップ 12 [Application Endpoint] のテーブルで、アプリケーションにアクセスしているクライアントのリストを確認します（メトリックチャートの後に表示されます）。

Cisco DNA Center で管理されるクライアントのみを表示する場合は、[Managed Clients] タブをクリックします。

このテーブルには、各クライアントの詳細が表示されます。これには、識別子（ユーザー ID、ホスト名、IPアドレス、MACアドレスのうち、この順序で使用可能なもの）、クライアント、クライアントの正常性、アプリケーションの正常性、使用状況、デバイスタイプ、MAC アドレス、VLAN ID などの情報が含まれます。

アクティブクライアントについては、[Identifier] 列をクリックして [Client 360] ウィンドウを開くことができます。

このテーブルには、クライアントが最大100個まで表示されます。追加のクライアントを表示するには、[Show More] をクリックします。

ステップ 13 （任意） テーブルに表示するデータをカスタマイズします。

a) をクリックします。
オプションのリストが表示されます。
b) 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。
c) [Apply] をクリックします。

ステップ 14 （任意） テーブルデータを CSV ファイルにエクスポートするには、[Export] をクリックします。

（注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。

アプリケーションの正常性スコア設定の設定

アプリケーションの正常性スコアを設定するには、次の手順を実行します。トラフィッククラスごとにKPIのしきい値を変更し、計算に含めるKPIを指定すると、アプリケーションの正常性スコアの計算をカスタマイズできます。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Manage]** > **[Health Score Settings]** の順に選択します。

ステップ 2 [Application Health] タブをクリックします。

ステップ 3 アプリケーションカテゴリのタブをクリックして、正常性スコアの計算設定をカスタマイズします。

このタブには、アプリケーションの正常性スコアの計算に影響する KPI が表示されます。

ステップ 4 [KPI Name] 列で、KPI 名のリンクをクリックします。

KPI のスライドインペインが表示されます。

ステップ 5 KPI の正常性スコアを次のように設定します。

a) [Poor]、[Fair]、および [Good] 正常性スコアの KPI しきい値をカスタマイズします。

b) [Weight]：有効な重みは 1 ー 10 です。重みが大きいほど、KPI がアプリケーションの正常性に及ぼす影響は大きくなります。

c) この KPI を正常性スコアの計算に含める場合は、[Include for health score] チェックボックスをオンにします。

d) デフォルトの KPI 設定を復元するには、[Reset to Default] をクリックします。

ステップ 6 [Apply] をクリックします。

アプリケーションのヘルス スコアと KPI メトリックスの理解

ここでは、アプリケーションのヘルス スコアと KPI メトリックの計算方法について説明します。

全体的なアプリケーション正常性スコア

アプリケーション正常性スコアは、正常なビジネス関連アプリケーションの数（正常性スコアが 8 ～ 10）をビジネス関連アプリケーションの総数で割ったパーセンテージです。このスコアは直近の 5 分間に対して計算されます。

例：90 %（正常性スコア）=90（正常性スコアが 8 ～ 10 のビジネス関連アプリケーション数）÷ 100（ビジネス関連アプリケーションの総数）

個別アプリケーションの正常性スコア

個別アプリケーションの正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、およびジッター）の加重平均に基づいて計算されます。

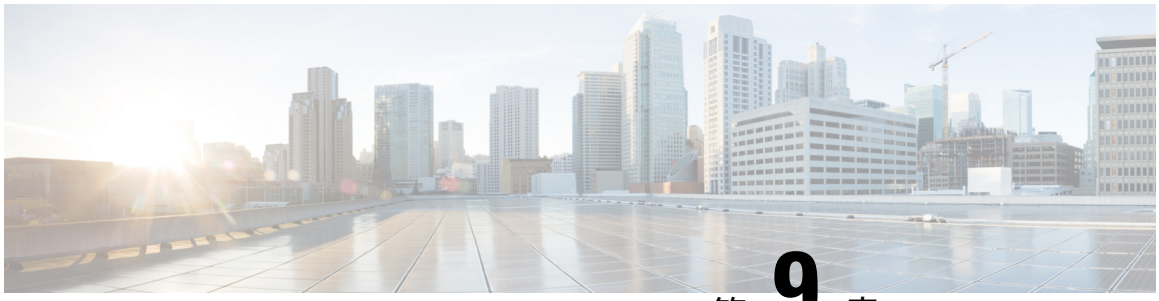
個別アプリケーションの正常性は1～10のスケールで測定され、10が最高スコアになります。個別アプリケーションの正常性スコアを計算するには、次の式を使用します。

個別アプリケーションの正常性スコア = (Latency_Weight * Latency_VoS_Score + Jitter_Weight * Jitter_VoS_Score + PacketLoss_Weight * PacketLoss_VoS_Score) ÷ (Latency_Weight + Jitter_Weight + PacketLoss_Weight)

（注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよびCisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要なKPIをポーリングしません。

個別アプリケーションの正常性スコアを計算するためのワークフローは次のとおりです。

1. KPI（ジッター、遅延、パケット損失）を取得します。
2. フローレコードのDSCP値に基づいて、アプリケーションのトラフィッククラスを決定します。
3. 各トラフィッククラスとKPIメトリックのCisco Validated Design（CVD）しきい値を使用して、KPI番号をサービススコア検証（VoSスコア）に変換します。
4. アプリケーションのトラフィッククラスと許容度レベルに基づいて、KPIの重み付けを行います。重み付けはRFC4594に基づきます。
5. アプリケーションの正常性スコアを計算します。これは、パケット損失、ネットワーク遅延、およびジッターの加重平均です。



第 9 章

ネットワークサービスの監視

AAA ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラによって報告されたすべての AAA サーバートランザクションを表示および監視します。

（注） **AAA 制約事項**

- AAA ネットワークサービスは、ワイヤレスクライアントおよびローカルモードをサポートします。
- AAA ネットワークサービスは、次をサポートしていません。
  - AireOS ワイヤレスコントローラ
  - フレックスモードまたはファブリックモード

始める前に

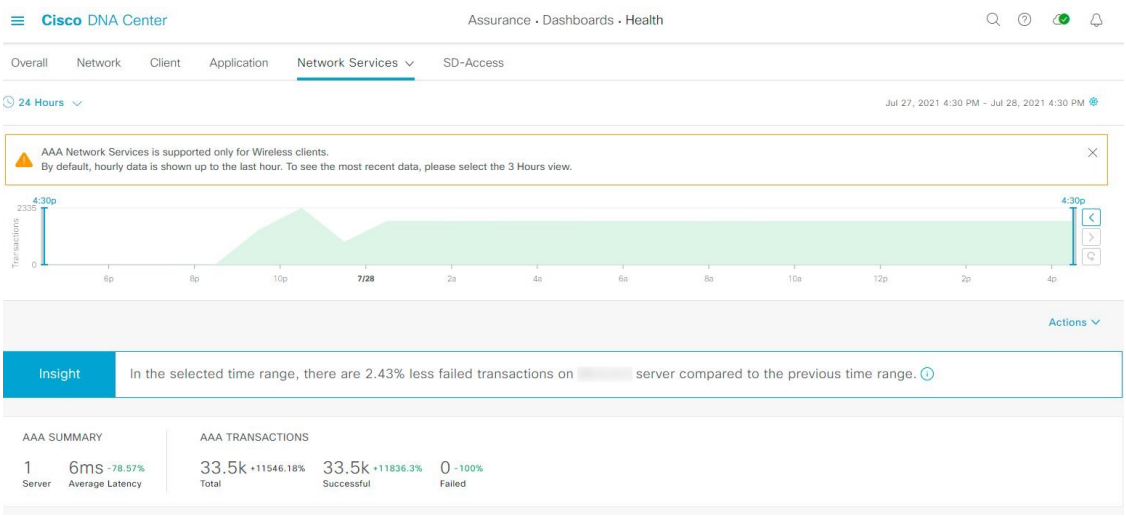
バージョン 17.6.1 以降の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラがインストールされており、ローカルモード AP で展開されていることを確認します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

ステップ 2 **[Network Services]** > **[AAA]**を選択します。

[AAA] ダッシュボードが表示されます。

図 *15 : [AAA]* ダッシュボード



ステップ 3 左上隅にある時間範囲設定（）をクリックして、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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 4 右上隅にある自動更新設定（）をクリックして、サポートされている アシュアランス ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 5 タイムラインスライダを使用して、一定期間における AAA サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには、次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の AAA サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 6 タイムラインスライダの下にある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- [Edit Dashboard] : ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ） およびカスタム ダッシュボードの作成 （313 ページ） を参照してください。

ステップ 7 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した AAA サーバートランザクションの割合を表示します。

ステップ 8 AAA の概要ダッシュレットを使用して、次の情報を確認できます。

AAA の概要	
アイテム	説明
AAA の概要	ネットワークの AAA サーバーの数と平均遅延（ミリ秒単位）を表示します。
AAA トランザクション	ネットワーク内の AAA トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合を表示します。

ステップ 9 次の機能には、AAA サーバーダッシュレットを使用します。

最も大きい遅延が発生した上位サイト
チャートには、AAA サーバーの遅延（ミリ秒単位）が最も大きい上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントにカーソルを合わせると、AAA サーバーの遅延が最も大きいサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

トランザクションエラーが発生した上位サイト
チャートには、AAA サーバーのトランザクションエラーが最も多い上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントまたはそれに対応する凡例にカーソルを合わせると、AAA サーバーのトランザクションエラーが最も多いサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

AAA サーバーの遅延
このチャートには、各 AAA サーバーにおける AAA 平均遅延が表示されます。[All]、[MAB]、または [EAP] に基づいて遅延をフィルタ処理できます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、AAA サーバーの遅延を表示できます。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

AAA サーバートランザクション
このチャートには、ワイヤレスコントローラによって報告された各 AAA サーバーの平均 AAA サーバートランザクション ステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、AAA サーバーのトランザクションを表示できます。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

ステップ 10 次の機能には、WLC による AAA サーバーダッシュレットを使用します。

WLC による AAA サーバーダッシュレット	
アイテム	**説明**
AAA サーバーテーブル	AAA サーバーの IP、WLC 名、WLC の場所、トランザクション、障害、平均遅延などを含むテーブル形式で AAA サーバー情報を表示します。[AAA Server IP] をクリックしてスライドインペインを開き、AAA サーバーの平均遅延およびトランザクションチャートを表示します。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、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 3. [Apply] をクリックします。

DHCP ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラによって報告されたすべての DHCP サーバートランザクションを表示および監視します。

（注） **DHCP の制限事項**

- DHCP ネットワークサービスは、ワイヤレスクライアントおよびローカルモードをサポートします。
- DHCP ネットワークサービスは、以下をサポートしていません。
  - SD-Access ファブリッククライアント
  - AireOS ワイヤレスコントローラ
  - フレックスモードまたはファブリックモード

始める前に

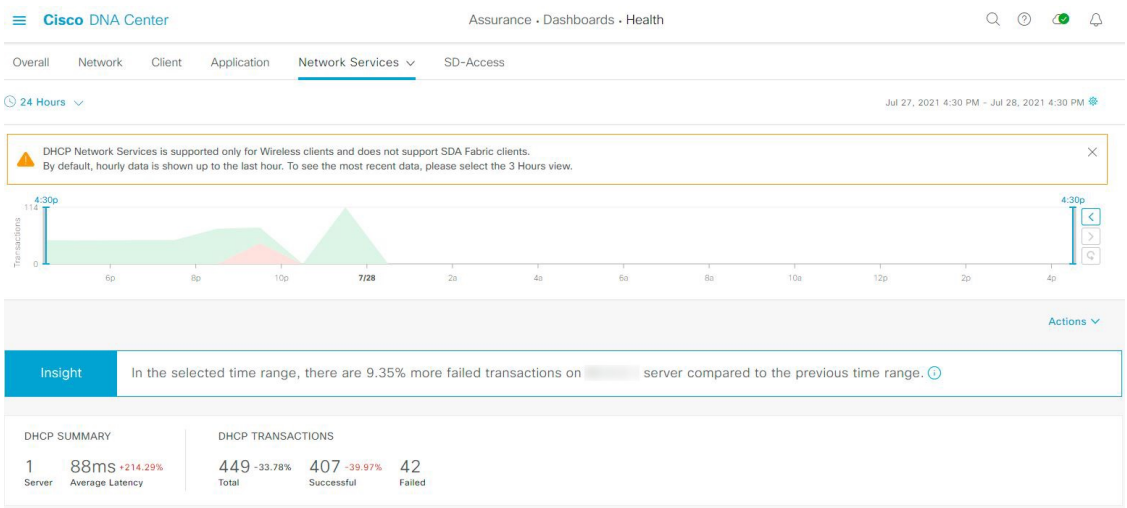
バージョン 17.6.1 以降の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラがインストールされていることを確認します。

ステップ 1 メニューアイコン（≡）をクリックして、**[Assurance]** > **[Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

ステップ 2 **[Network Services]** > **[DHCP]**を選択します。

[DHCP] ダッシュボードが表示されます。

図 *16 : [DHCP]* ダッシュボード



ステップ 3 左上隅にある時間範囲設定（🕓）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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 4 右上隅にある自動更新設定（⚙）をクリックして、サポートされている アシュアランス ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 5 タイムラインスライダを使用して、一定期間における DHCP サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには、次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の DHCP サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 6 タイムラインスライダの下にある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ） およびカスタム ダッシュボードの作成 （313 ページ） を参照してください。

ステップ 7 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した DHCP サーバートランザクションの割合を表示します。

ステップ 8 DHCP の概要ダッシュレットを使用して、次の情報を確認できます。

DHCP の概要	
アイテム	**説明**
DHCP Summary	ネットワークの DHCP サーバーの数と平均遅延（ミリ秒単位）が表示されます。
DHCP Transactions	ネットワーク内の DHCP トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合が表示されます。

ステップ 9 次の機能には、DHCP サーバーダッシュレットを使用します。

最も大きい遅延が発生した上位サイト
チャートには、DHCP サーバーの遅延（ミリ秒単位）が最も大きい上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントにカーソルを合わせると、DHCP サーバーの遅延が最も大きいサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

トランザクションエラーが発生した上位サイト
チャートには、DHCP サーバーのトランザクションエラーが最も多い上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントまたはそれに対応する凡例にカーソルを合わせると、DHCP サーバーのトランザクションエラーが最も多いサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

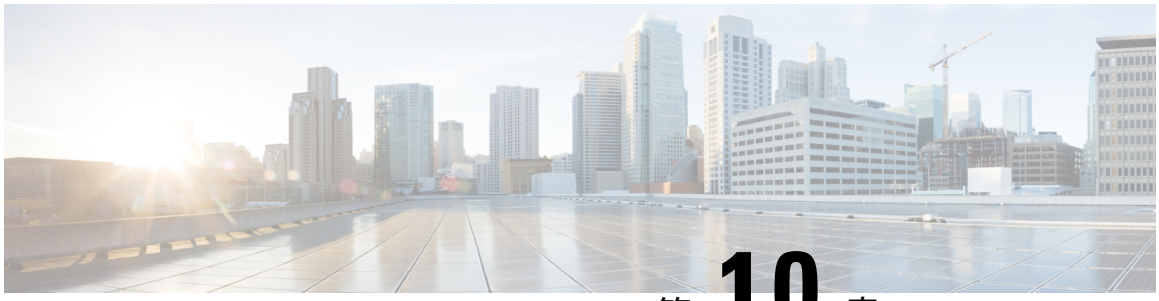
DHCP サーバーの遅延
このチャートには、各 DHCP サーバーにおける DHCP 平均遅延が表示されます。[All]、[Discover-offer]、または [Request-Ack] に基づいて遅延をフィルタ処理できます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、DHCP サーバーの遅延を表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

DHCP サーバートランザクション
このチャートには、ワイヤレスコントローラによって報告された各 DHCP サーバーの平均 DHCP サーバー トランザクション ステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、DHCP サーバーのトランザクションを表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

ステップ 10 次の機能には、WLC による DHCP サーバーダッシュレットを使用します。

WLC による DHCP サーバーダッシュレット	
アイテム	説明
DHCP サーバーテーブル	DHCP サーバーの IP、WLC 名、WLC の場所、トランザクション、障害、平均遅延などを含むテーブル形式で DHCP サーバー情報を表示します。[DHCP Server IP] をクリックしてスライドインペインを開き、サーバーの平均遅延およびトランザクションチャートを表示します。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

WLC による DHCP サーバーダッシュレット	
アイテム	説明
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、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。 3. [Apply] をクリックします。



第 10 章

SD-Accessの正常性のモニターとトラブルシューティング

SD-Access ファブリック

SD-Access ファブリックは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、新しいファブリックサイトを作成できます。つまり、サイトのテレメトリ設定を構成するときには、[Monitor wired clients] を有効にしておく必要があります。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[SD ACCESS]** > **[Fabric Sites]** の順に選択します。

ステップ 2 [Fabric Sites] タブで、[Add fabric site] をクリックします。

または、最初の 2 つの手順の代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** を選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let's Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 （オプション）ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、表示されたネットワーク階層からファブリックサイトを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウでファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 8 [作成（Create）] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」というメッセージが表示されます。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）
- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

1. メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
2. [Inventory] ウィンドウに、検出されたデバイスが表示されます。
3. ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
4. ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
5. 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで**[Inventory]** > **[Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 [SD ACCESS] の下でメニューアイコン（☰）をクリックして、**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 3 デバイスをクリックします。スライドインペインには、次の [Fabric] オプションが表示されます。

オプション	説明
エッジ	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
Border	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスを一体型ファブリックとして設定するには、[Control Plane]、[Border]、および [Edge] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane] と [Border] の両方を選択します。

ステップ 4 [Add] をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

SD-Access ファブリックの正常性の監視とトラブルシュート

この手順を使用して SD-Access ファブリックの概要を把握して、対処する必要がある潜在的な問題があるかどうかを判断します。

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。Cisco DNA Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

始める前に

wsiddiqi

アシュアランスを設定します。「基本的な設定のワークフロー （17 ページ）」を参照してください。

ファブリックサイトを監視およびトラブルシューティングするには、最初にファブリックサイトを構成する必要があります。ファブリックサイトの追加（119ページ）およびファブリックへのデバイスの追加 （120 ページ）を参照してください。

マルチサイト ファブリック サイトの詳細情報については、Cisco Digital Network Architecture Center ユーザー ガイドの「Provision Your Network」の章を参照してください。

（注） サブテンドノードと拡張ノードは、ファブリックの正常性の対象にはなりません。ファブリックのプロビジョニング中、これらのノードには、エッジ、ボーダー、コントロールプレーンなどのファブリックロールが割り当てられません。

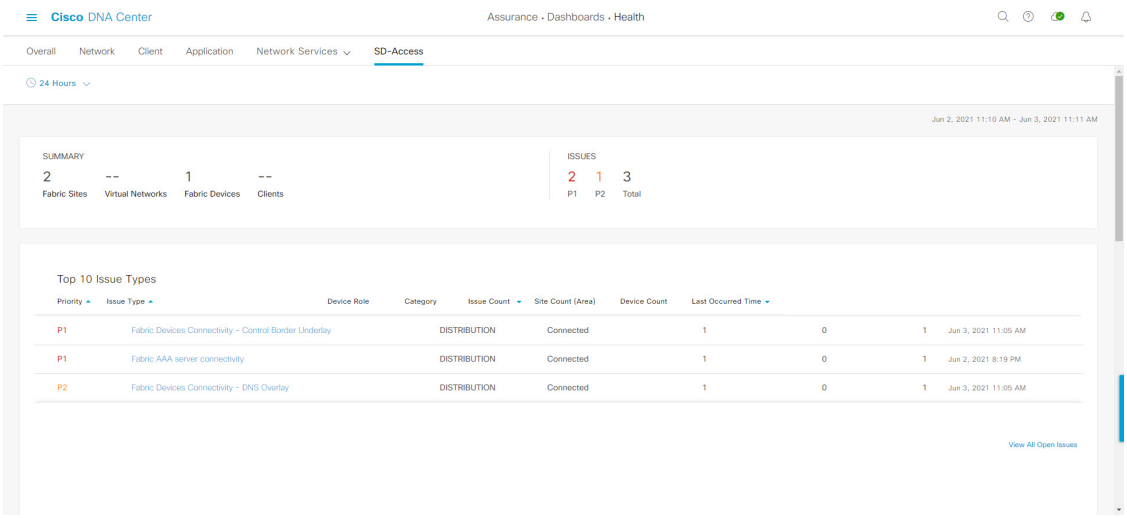
ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

図 *17 : [Network Health]* ダッシュボード



ステップ 3 上部のメニューバーにある時間範囲設定（）をクリックして、ダッシュボード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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

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

アイテム	説明
Summary	• [Fabric Sites]：ファブリックサイトの数。 • [Virtual Networks]：仮想ネットワークの数。 • [Fabric Endpoints]：ファブリックエンドポイントの数。 • [Endpoints]：エンドポイントの数。
問題	• [P1]：優先度 1 の問題の数。 • [P2]：優先度 2 の問題の数。 • [Total]：P1、P2、および P3 の問題の合計数。

ステップ 5 次の機能には、SD-Access の [Top 10 Issue Types] ダッシュレットを使用します。

表 *21 :*

[Top 10 Issues] ダッシュレット
対処する必要がある上位 10 件の問題を表示します（存在する場合）。問題は色分けされ、事前割り当てされた P1 から始まる優先度レベルで並び替えられます。 問題をクリックすると、スライドインペインが開き、問題のタイプに関する追加の詳細が表示されます。スライドインペインで問題のインスタンスをクリックします。必要に応じて、次の操作を実行できます。 • 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 • 問題のインスタンスを無視するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 [View All Issues] をクリックすると、[Open Issues] ウィンドウが開きます。

ステップ 6 [Fabric Sites] ダッシュレットを使用して、ネットワーク内のファブリックサイトに関する詳細情報を表示します。このダッシュレットには、次の機能があります。

[Fabric Sites] ダッシュレット	
アイテム	**説明**
ヘルス（**Health**）	次のオプションを使用して、クライアントの正常性を基にテーブルをフィルタリングします。 • **すべて** • [Inactive]：正常性スコアが 0 のファブリックサイト。 • [Poor]：正常性スコアが 1 ～ 3 のファブリックサイト。 • [Fair]：正常性スコアが 4 ～ 7 のファブリックサイト。 • [Good]：正常性スコアが 8 ～ 10 のファブリックサイト。 • [No Data]：データのないファブリックサイト。

[Fabric Sites] ダッシュレット	
アイテム	説明
[Fabric Site] テーブル	ファブリックサイトの詳細情報を表形式で表示します。デフォルトでは、[Fabric Site] テーブルには次の情報が表示されます。 • [Fabric Site]：ファブリックサイトの名前。 • [# of Fabric Devices]：ファブリックサイト内のファブリックデバイスの数。 • [Fabric Site Health]： • [Overall]： • [Fabric Site Connectivity]： • [Fabric Infrastructure]： ファブリックサイト名をクリックして、ファブリックサイトの 360 度ビューを表示することもできます。ファブリックサイトの正常性の監視 （201 ページ）を参照してください。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。
⚙	テーブルの表示をカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 3. [Apply] をクリックします。

ファブリックサイトの正常性の監視

この手順を使用して、特定のファブリックサイトの詳細を表示します。

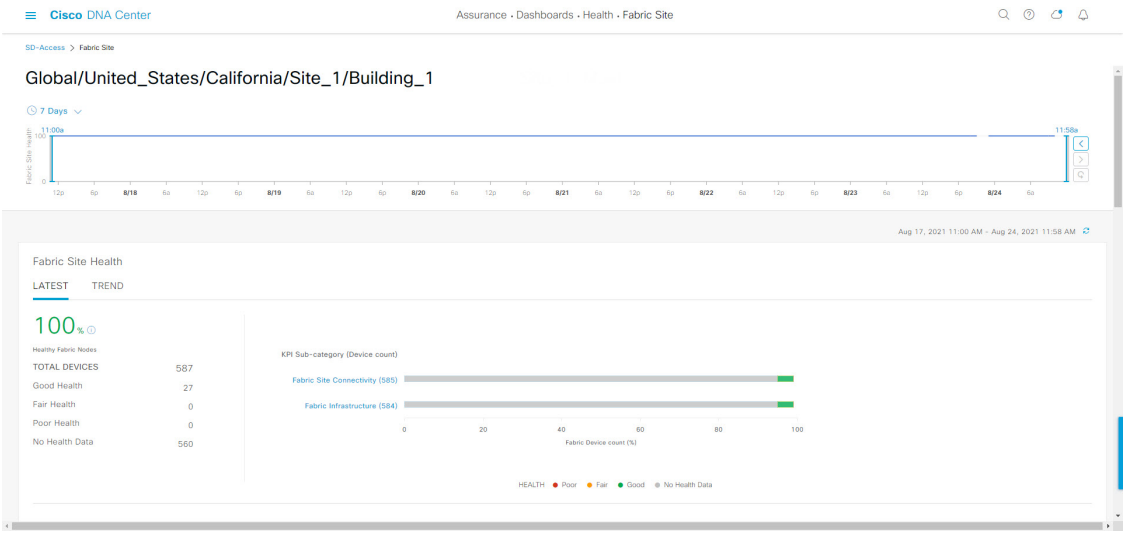
ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Fabric Site] テーブルで、ファブリックサイトの名前をクリックします。

ファブリックサイトの 360° ビューを提供する [Fabric Site 360] ウィンドウが表示されます。

図 *18 : Fabric Site 360*



ステップ 3 左上隅にある時間範囲設定（）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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 4 ファブリックサイトの正常性タイムラインスライダを使用して、より詳細な時間範囲のファブリックの正常性スコアやファブリックサイトの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Fabric Site Health]：正常性は、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスヘルスには含まれません。ファブリックサブカテゴリの正常性は、基礎となる KPI スコアの最小値です。

（注） KPI は正常性スコアに含まれません

[Fabric Site Connectivity]：コントロールプレーンに到達できません。

[Fabric Infrastructure]：

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、Fabric Site 360 ウィンドウに表示されるファブリックサイトデータのコンテキストが設定されます。

- [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。
- [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。

ステップ 5 タイムラインの下にある [Fabric Site Health] エリアで、次の情報を確認します。

ファブリックサイトの正常性	
アイテム	説明
Latest	デフォルトで表示されます。2つのペインがあります。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Health Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間のファブリックサイトの接続とインフラストラクチャを示します。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスのヘルス スコアと数が表示されます。 チャートに低いヘルス スコア（赤またはオレンジ）が示されている場合、その低いヘルス スコアに寄与した KPI がバーの隣に示されます。たとえば、ファブリック CP の到達可能性、マルチキャスト RP、AAA サーバーのステータスなどです。 グラフ内のハイパーリンクされたファブリックカテゴリをクリックしてサイドペインを開き、それぞれの KPI サブカテゴリを表示することもできます。 • [Fabric Site Connectivity]：コントロールプレーンの到達可能性。 • [Fabric Control Plane]：LISP セッションステータス。 • [Fabric Infrastructure]：INFRA VN の AAA サーバーステータスと Pub-Sub セッションステータス。
Trend	[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 です。 ●：正常性データなし。ヘルス スコアは 0 です。

ステップ 6 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題
対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。 問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。 スライドインペインでは、次の操作を実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （215 ページ）を参照してください。

ステップ 7 次の機能には、[Fabric Nodes] ダッシュレットを使用します。

[Networks Devices] ダッシュレット	
アイテム	**説明**
[Type]	オプション（[All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric WLC]、[Fabric AP]、[Extended Node]）を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
ファブリックサイトの正常性	次のオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。

[Networks Devices] ダッシュレット	
アイテム	説明
ファブリックノードテーブル	選択したサイトのすべてのファブリックノードのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、ファブリックサイト接続とファブリック インフラストラクチャの KPI メトリック正常性スコアの最小サブスコアです。 [Name]、[Issue Type Count]、および [Fabric Role] 列には、ファブリック名、問題数、およびファブリックロール（エッジ、ボーダー、マップサーバーなど）が表示されます。 [Device Fabric Site Health] の [Overall] 列で、正常性スコアの上にマウスカーソルを合わせます。全体の [Device Fabric Site Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。 カーソルを [Fabric Site Connectivity] および [Fabric Infrastructure] アイコンに合わせると、正常性スコアが表示されます。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。

トランジットおよびピアネットワークの正常性の監視

この手順を使用して、特定のトランジットネットワークの詳細を表示します。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

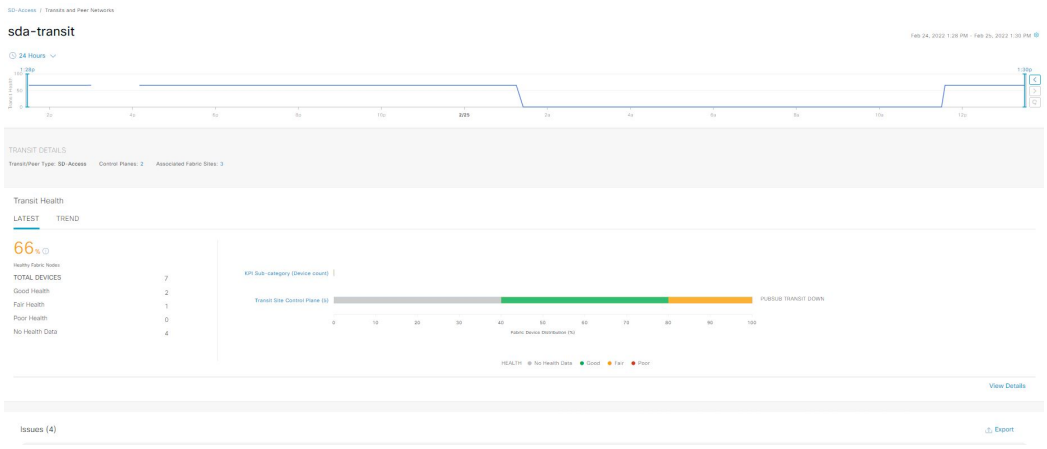
ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

ステップ 3 [Transit and Peer Network] テーブルで、トランジットの名前をクリックします。

ファブリックサイトの 360° ビューを提供する [Transit Site 360] ウィンドウが表示されます。

図 *19 :* トランジット *360*



ステップ 4 左上隅にある時間範囲設定（）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) ドロップダウンリストから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 5 正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Transit Network Health]：正常性は、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスの正常性は含まれません。ファブリックサブカテゴリの正常性は、基礎となる KPI スコアの最小値です。

[Transit Site Control Plane]：トランジットの LISP セッションや PubSub セッションなどの KPI サブカテゴリを一覧表示します。トランジット正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

- [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。
- [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。

ステップ 6 タイムラインの下にある [Transit Health] エリアで、次の情報を確認します。

トランジットの正常性	
アイテム	説明
Latest	デフォルトで表示されます。2つのペインがあります。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Health Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間のトランジット コントロール プレーンを示します。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。 チャート内のハイパーリンクされた [Transit Control Plane] をクリックしてサイドペインを開き、トランジットコントロールプレーンの次の KPI サブカテゴリを表示することもできます。 • [LISP session from Border to Transit Control Plane] • [PubSub session from Border to Transit Control Plane] チャートの色のセグメントにカーソルを合わせると、ファブリックノードの名前、問題数、ファブリックロール、ファブリックサイト、デバイスのトランジットの正常性などのファブリックノードの詳細を表形式で表示できます。
Trend	[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 です。 ●：正常性データなし。ヘルス スコアは 0 です。

ステップ 7 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題
対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。 問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。 スライドインペインでは、次の操作を実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （215 ページ）を参照してください。

ステップ 8 次の機能には、[Associated Fabric Sites] ダッシュレットを使用します。

[Associated Fabric Sites] ダッシュレット	
アイテム	説明
[Health]	次のオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。
[Associated Fabric Sites] テーブル	ファブリックテーブルに次の詳細を表示します。[Fabric Site]、[Health]、使用可能な [Connected Transit/ Peer Networks] の数、[Layer 3 Virtual Network]、および [Fabric Devices]。

[Associated Fabric Sites] ダッシュレット	
アイテム	説明
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。

ステップ 9 次の機能には、[Fabric Nodes] ダッシュレットを使用します。

[Fabric Nodes] ダッシュレット	
アイテム	説明
[Type]	オプション（[All]、[Transit Control Plane]、[Border]）を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
[Transit and Peer Network Health]	次のオプションを使用して、トランジットの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。

[Fabric Nodes] ダッシュレット	
アイテム	説明
ファブリックノードテーブル	選択したトランジットのすべてのファブリックノードのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、トランジット サイト コントロール プレーンの KPI メトリック正常性スコアの最小サブスコアです。 [Name]、[Issue Type Count]、[Fabric Role]、および [Fabric Site] 列には、ファブリック名、問題数、ファブリックロール、およびファブリックサイトが表示されます。 [Device Transit Health] の [Overall] 列で、正常性スコアの上にマウスカーソルを合わせます。全体の [Device Transit Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。 [Transit Site Control Plane] アイコンにカーソルを合わせると、正常性スコアが表示されます。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。

仮想ネットワークの正常性の監視

この手順を使用して、特定の仮想ネットワークの詳細を表示します。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

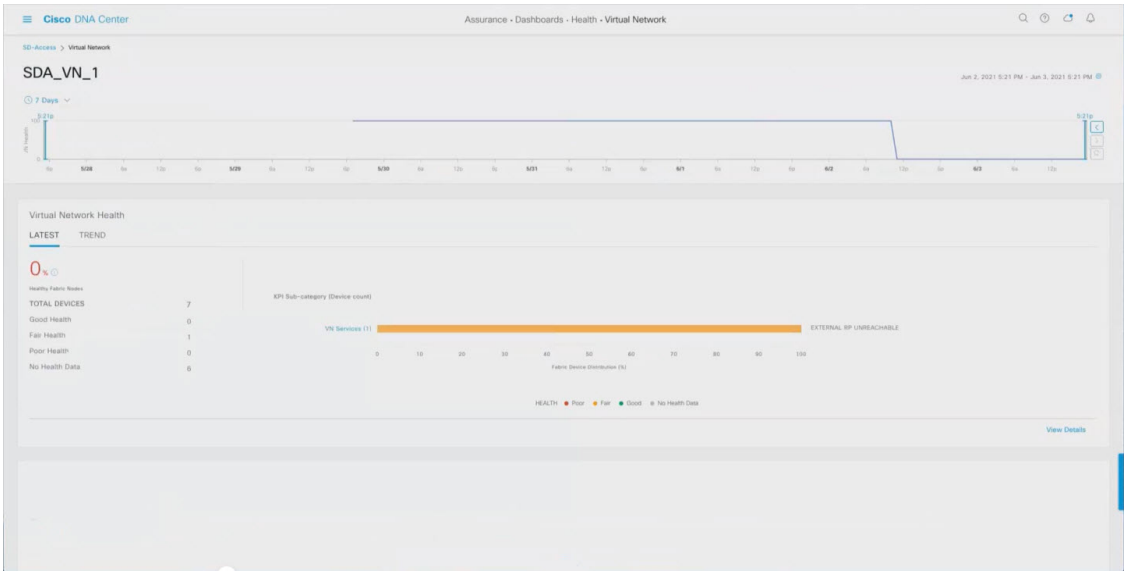
[SD-Access health] ダッシュボードが表示されます。

ステップ 3 下にスクロールし、[Virtual Network] をクリックします。

ステップ 4 [Virtual Network] テーブルで、仮想ネットワークの名前をクリックします。

仮想ネットワークの 360 度ビューを提供する [Virtual Network 360] ウィンドウが表示されます。

図 20 : Virtual Network 360



ステップ 5 左上隅にある時間範囲設定（）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) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 6 仮想ネットワークの正常性タイムラインスライダを使用して、より詳細な時間範囲の仮想ネットワークの正常性スコアや仮想ネットワークの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Virtual Network Health]：正常性スコアは、正常なマルチキャスト VN サービスの割合です。

VN 正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

（注） 現在、マルチキャスト VN サービスが、VN 正常性スコアに関係する唯一の KPI です。

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、360 ウィンドウに表示されるデータのコンテキストが設定されます。

- [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。
- [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。

ステップ 7 タイムラインの下にある [Virtual Network Health] エリアで、次の情報を確認します。

Virtual Network Health	
アイテム	**説明**
Latest	デフォルトで表示されます。2つのペインがあります。左側のペインには、仮想ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Healthy Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ファブリックデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts]：この色分けされたスナップショット ビュー チャートには、KPI サブカテゴリが表示されます。現在、KPI サブカテゴリは VN サービスのみです。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。 チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。 ハイパーリンクされたカテゴリをクリックして、詳細を示すサイドペインを開くこともできます。
Trend	[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 です。 ●：正常性データなし。ヘルス スコアは 0 です。

ステップ 8 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題
対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。 問題をクリックするとスライドインペインが開き、問題の説明、影響、および推奨されるアクションなど、対応する詳細情報が表示されます。 スライドインペインでは、次の操作を実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （215 ページ）を参照してください。

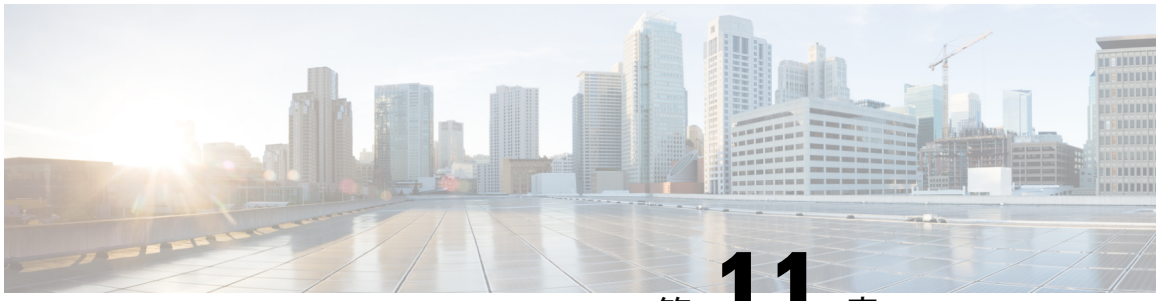
ステップ 9 次の機能には、[Virtual Network Devices] ダッシュレットを使用します。

[Virtual Network Devices] ダッシュレット	
アイテム	説明
[Type]	タイプに基づいてテーブルをフィルタ処理します。
[Virtual Network Health]	次のオプションを使用して、仮想ネットワークの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。

[Virtual Network Devices] ダッシュレット	
アイテム	説明
[Virtual Network Devices] テーブル	選択した項目のデバイス情報が表形式で表示されます。 （注） 全体的な正常性スコアは、仮想ネットワーク接続とインフラストラクチャの KPI メトリック正常性スコアの最小サブスコアです。 各種の正常性スコアとアイコンにカーソルを合わせると、追加情報が表示されます。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. をクリックします。 オプションのリストが表示されます。 2. 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。 3. [Apply] をクリックします。

仮想ネットワークの正常性スコア

現在、マルチキャスト VN サービスが、VN 正常性スコアに関係する唯一の KPI です。



第 11 章

問題の表示と管理

問題について

アシュアランス システムガイド付きとガイドなしの両方のトラブルシューティングを提供します。アシュアランスは多くの問題に対してシステムガイド付きアプローチを提供します。このアプローチでは、複数の重要業績評価指標（KPI）が関連付けられてます。また、テストやセンサーからの結果に基づき問題の根本原因が特定された後に、考えられる解決策が提供されます。データの監視ではなく、問題点を浮き彫りにすることに重点が置かれています。アシュアランスでは、非常に頻繁にレベル 3 サポートエンジニアの作業が実行されます。

Cisco DNA Center では、Cisco AI Network Analytics を使用してAI 駆動型の問題を表示およびトラブルシューティングできます。Cisco AI Network Analytics は、高度な人工知能（AI）や機械学習（ML）テクノロジーを基盤としたクラウドベースの学習プラットフォームを活用して、問題のインテリジェントな検出と分析を実現します。異常を検知すると、根本原因を特定してトラブルシューティングを容易にします。

Cisco AI Network Analytics 次のタイプのクラウドベースの AI 駆動型の問題を検出できます。

- **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な関連付け時間、過剰な関連付け障害回数、過剰な認証時間、過剰な認証障害回数、過剰なDHCP時間、過剰な DHCP 障害回数。
- **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーション アプリケーションのスループット、およびソーシャルアプリケーションのスループット。

（注） 現在、Cisco AI Network Analytics のユースケースは、AireOS コントローラが稼働するワイヤレス環境でのみサポートされています。

機械推論エンジンについて

機械推論エンジン（MRE）は、ネットワーク自動化エンジンであり、人工知能（AI）を使用して複雑なネットワーク運用ワークフローを自動化します。完全に自動化された推論エンジンに人間の知識と専門知識をカプセル化し、複雑な根本原因の分析、問題や脆弱性の検出、および手動または自動による是正処置の実行を支援します。MRE は、シスコのネットワーキング エキスパートによって構築された、クラウドホスト型のナレッジベースを実装しています。

MRE を使用して、有線クライアントの問題、レイヤ 2 ループの問題、および PoE の問題をトラブルシューティングできます。問題のリストについては、MREの問題（260ページ）を参照してください。

手順については、MREを使用した有線クライアントの問題のトラブルシュート（231ページ）、レイヤ2のループ問題に関与するインスタンスの詳細とPoEの問題（225ページ）、およびPoEの問題に関する問題インスタンスの詳細（228ページ）を参照してください。

レイヤ 2 のループの問題について

レイヤ 2 のループ問題は、1 つ以上の VLAN パスで転送ループが形成されたときに発生します。この場合、リンクとデバイスが最大キャパシティに達するまで、パケットは転送され、影響を受けるパスで無限に増幅されます。ブロードキャストストームが発生すると、レイヤ 2 ネットワーク全体は即時にシャットダウンします。MRE の次の機能を使用することで、レイヤ 2 のループ問題をトラブルシューティングできます。

- ループに関係すると考えられる VLAN とポートが表示されます。
- ループに関係しているデバイスが表示されます。

（注） レイヤ 2 ループのスケールに関する制約事項は、次のとおりです。

- VLAN 数は 10 です。
- VLAN ごとのデバイス数は 30 です。

重要 現在のところ、MRE では、管理対象外のネットワークデバイスや仮想マシンなどのエンティティが原因で発生したレイヤ2のループについては、根本原因の分析が実行されません。こうしたエンティティは、Cisco DNA Center で認識されるトポロジには含まれません。

未解決の問題を表示

次のカテゴリに分類される未解決の問題をすべて表示するには、次の手順を実行します。

- **しきい値ベースの問題**：アシュアランス によって検出された問題。
- **駆動型の問題**：Cisco AI Network Analytics によって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

  Cisco DNA Center で Cisco AI Network Analytics アプリケーションをインストールおよび設定している場合は、次のタイプのクラウドベース AI 駆動型に関する問題を確認できます。

  - **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な関連付け時間、過剰な関連付け障害回数、過剰な認証時間、過剰な認証障害回数、過剰な DHCP 時間、過剰な DHCP 障害回数。

（注） 接続の問題が表示されるようにするには、AP がサイトに適切に割り当てられていることを確認してください。

- **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーションアプリケーションのスループット、およびソーシャルアプリケーションのスループット。

（注） アプリケーション エクスペリエンスに関する問題を表示するには、ワイヤレスコントローラで Application Visibility and Control（AVC）が有効になっていることを確認してください。スループットの問題では、AVC データに基づいて基準化と異常検出を行います。

- **レイヤ 2 ループの問題**と **PoE の問題**：アシュアランスによって検出された、MRE ワークフローを使用してトラブルシューティングできる問題。機械推論エンジンについて （216 ページ）を参照してください。

始める前に

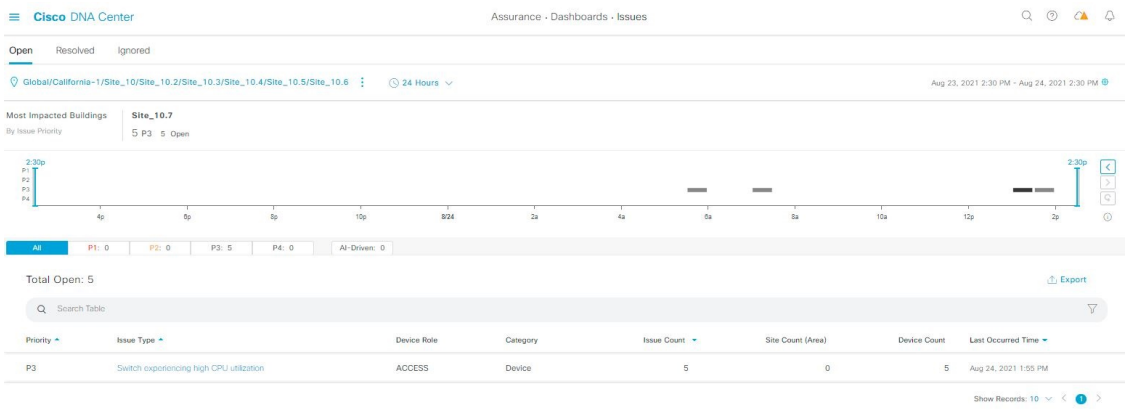
- 人工知能（AI）および機械学習（ML）テクノロジーを使用してインテリジェントな問題の検出と分析を行う AI 駆動型クラウドベースの問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認します。Cisco AI Network Analytics データ収集の設定 （84 ページ）を参照してください。
- syslog メッセージを表示するため、syslog が設定されていることを確認します。『Cisco Digital Network Architecture Center ユーザー ガイド』で「テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定（83 ページ）」を参照してください。

ステップ 1 次のいずれかを実行します。

- Cisco DNA Center ホームページの **アシュアランス [Summary]** > **[Critical Issues]**エリアで、[View Details] を選択します。
- メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboards]** > **[Issues]** の順に選択します。

[Open Issues] ダッシュボードが表示され、次の情報が示されます。

図 *21 : [Open Issues]* ダッシュボード



[Open Issues] ダッシュボード	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Open Issues] ダッシュボードに表示されます。
[Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
Most Impacted Areas	問題のプライオリティに基づいて最も影響を受けるエリアに関する情報が表示されます。ハイパーリンクされたロケーションをクリックすると、問題が発生した建物とフロアにドリルダウンします。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。 色は、問題のプライオリティを表します。 : P1 : P2 : P3 および P4 （注） 色の明度は重要性（そのプライオリティ レベルで発生した問題数の多寡）を示します。たとえば、薄い黄色は、濃い黄色よりも（未解決の）P2 問題が少ないことを示します。

[Open Issues] ダッシュボード	
アイテム	説明
Total Open	アクションを必要とする未解決の問題の合計数が表示されます。 [Total Open] の値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。

ステップ 2 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Open Issue] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル（事前割り当てされたもの）。
Issue Type	問題のタイプ。 （注） AI駆動型の問題の場合、問題のタイプの前に AI アイコンが表示されます。
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 3 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題タイプに関するすべての問題が次の情報とともに一覧表示されます。

[Issue Instance]（最初のスライドインペイン）	
アイテム	説明
Open Issues	その問題タイプで未解決の問題の数。
Area	問題の影響を受けるビルディングとフロアの数。
[Device]	問題の影響を受けるデバイスの数。
[Actions] ドロップダウン リスト	個別に問題を解決または無視することも、一度に大量の問題を解決または無視することもできます。問題の解決または無視 （238 ページ）を参照してください。

[Issue Instance]（最初のスライドインペイン）	
アイテム	説明
Issue	問題の説明。
Site	問題の影響を受けたサイト、ビルディング、またはフロア。
[Device]	問題の影響を受けたデバイス。デバイス名をクリックして、[Device 360] ウィンドウを開きます。
Device Type	問題の影響を受けたデバイスのタイプ。
Issue Count	この種類の問題が発生した回数。
Last Occurred Time	問題が発生した日付と時刻。
Last Updated Time	この問題の最終更新日時。
Updated By	この問題を更新したエンティティ名。

ステップ 4 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

（注） 推奨されるアクションには、その隣に [Run] ボタンが表示されます。[Run] をクリックすると、指定された CLI コマンドがデバイスで実行されます。

AI 駆動型の問題の場合、[Issue Instance Details] のスライドインペインに AI によって導出された固有の情報が表示されます。AI 駆動型の問題に関与するインスタンスの詳細 （221 ページ）を参照してください。

機械推論をサポートするレイヤ 2 ループの問題については、[Issue Instance Details] スライドインペインに特定の情報が表示されます。レイヤ 2 のループ問題に関与するインスタンスの詳細と PoE の問題 （225 ページ）を参照してください。

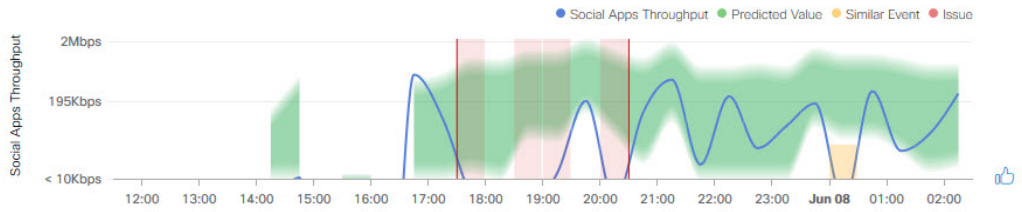
機械推論をサポートする PoE の問題については、[Issue Instance Details] スライドインペインに特定の情報が表示されます。PoE の問題に関する問題インスタンスの詳細 （228 ページ）を参照してください。

AI 駆動型の問題に関与するインスタンスの詳細

（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題を表示 （217 ページ） 」のステップ 4 を参照してください。

AI 駆動型の問題が発生すると、[Issue Instance Details]（2 番目のスライドインペイン）に次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Description	問題の説明。
[Status] ドロップダウンリスト	問題のステータスを変更できます。次の手順を実行します。 • 問題を解決するには、[Status] ドロップダウン メニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。
[Summary] エリア	問題の簡単な要約。ここには、影響を受ける無線、無線の場所、問題が発生した日時、問題の場所などの情報が表示されます。
[Impacted Summary for this Network]	問題によって影響を受けた場所と、影響を受けたクライアント数に関する情報が表示されます。
[Feedback] アイコン	 アイコンをクリックして、このページの情報が役に立ったかどうかについてコメントを入力し、[Submit] をクリックしてください。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Problem	問題の簡単な説明と、実際の KPI 値が予測した正常な動作からどの程度乖離しているかを視覚的に示すグラフが表示されます。 デフォルトでは、次の図に示すように、グラフは問題発生の前後 6 時間にズームインされます。 **図 *22 :* 問題のチャート**  AI 駆動型の問題のチャートでは、詳細がさまざまな色で表されます。 • **緑色の帯域**：機械学習に基づいて予測されたネットワークの正常な動作。 • **青色の実線**：実際の KPI 値。 • **垂直の赤色の線またはバー**：問題を示します。青色の線（実際の KPI 値）が緑色の帯域（予測される正常な動作）の外側になると、問題が発生します。 • **垂直の黄色のバー**：類似のイベントが発生したことを示します。 グラフの上にカーソルを移動すると、選択した時点での KPI 値、予測下限値、予測上限値などの同期情報が表示されます。
Impact	問題の影響を受ける接続済みクライアント、AP、デバイス、およびアプリケーションに関する情報が表示されます。 過剰なオンボーディング時間と失敗、過剰な DHCP、アソシエーション、または認証時間と失敗については、[Impacted Clients] タブと [Top 10 Impacted APs] タブが表示されます。 合計無線スループットおよびアプリケーション スループット（クラウド、コラボレーション、メディアおよびソーシャル）については、[Impacted Clients] タブ、[Device Breakout] タブ、[Applications TX / RX] タブが表示されます。 タブをクリックすると、チャートとチャートの下の表が更新されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	次の図に示すように、問題とその問題の原因として考えられるネットワーク関連の原因がチャートに表示されます。 図 *23 :* 根本原因の分析チャート  過剰なオンボーディング時間と失敗については、[Network Causes] タブ、[Failed Distribution] タブ、[Failed Percentage] タブ、[Failed Count] タブが表示されます。 過剰な DHCP、アソシエーション、または認証時間については、[Network Causes] タブ、[Top Impacted APs] タブ、[Top Impacted Times] タブが表示されます。 過剰な DHCP、アソシエーション、または認証の失敗については、[Network Causes] タブ、[Top Impacted APs] タブ、[Top Impacted Failures] タブが表示されます。 合計無線スループットおよびアプリケーション スループット（クラウド、コラボレーション、メディアおよびソーシャル）については、[Network Causes] タブが表示されます。 タブをクリックすると、下のチャートが更新されます。 追加された KPI のグラフを表示するには、[KPI] アイコンをクリックし、KPI を選択してから、[Apply] をクリックします。
Suggested Actions	この問題を解決するために実行できるアクションが表示されます。

レイヤ 2 のループ問題に関与するインスタンスの詳細と PoE の問題

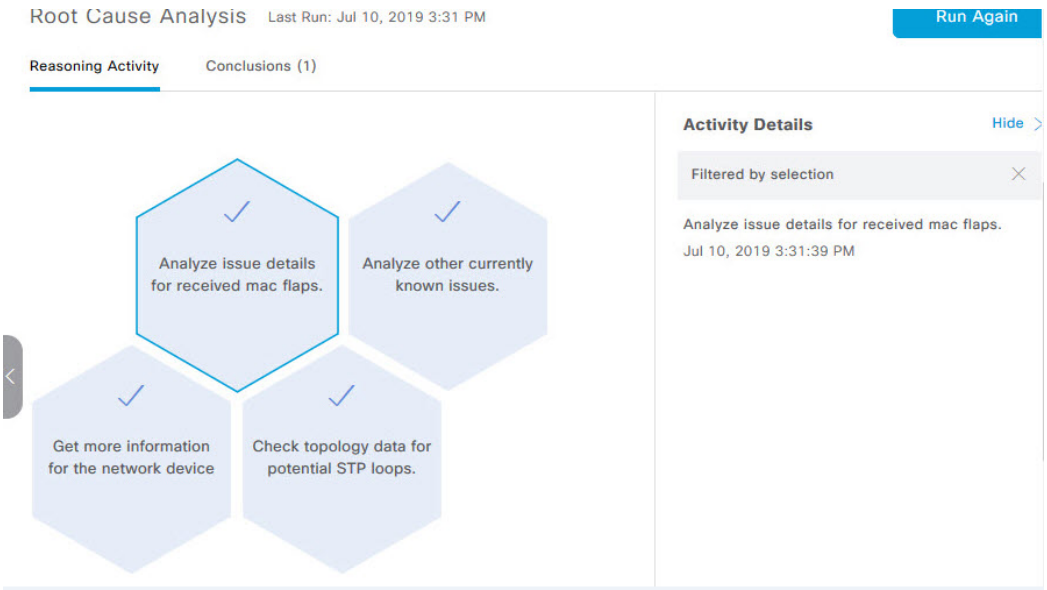
（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題を表示 （217 ページ） 」のステップ 4 を参照してください。

レイヤ 2 のループ問題と機械推論エンジンについては、「レイヤ 2 のループの問題について（216 ページ）」を参照してください。

機械推論をサポートするレイヤ 2 のループ問題については、[Issue Instance Details] スライドインペインに次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	**説明**
[Status] ドロップダウンリスト	問題のステータスを変更できます。次の手順を実行します。 • 問題を解決するには、[Status] ドロップダウン メニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。
Summary	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。 この領域では、レイヤ 2 のループ問題に関して、ループしている可能性のある VLAN やポートなどの初期アセスメントも提供されます。
[Problem Details]	（注） この領域は、レイヤ 2 のループ問題に対して表示されます。 問題についての簡単な説明と以下の項目が表示されます。 • [Relevant Events] ドロップダウンリスト：ループ中に発生したイベントが一覧表示されます。イベントをクリックすると、サイドペインに詳細情報が表示されます。 • [Potential Loop Details] ドロップダウンリスト：ループ情報（デバイス、ロール、ループ状態のポート、デュプレックスモード、ループに関与している VLAN など）が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 1. [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Run Machine Reasoning] ポップアップ ダイアログボックスが表示されます。 2. このポップアップ ダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 3. [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。このアクティビティは、根本原因分析の各ステップで使用されたコマンドを示します。 4.  アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力してください。 5. [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインにアクティビティの詳細が表示されます。 実行中の推論アクティビティをキャンセルするには、[Stop] をクリックします。 （注） チェックマークは、ステップが完了したことを示します。 図 *24 :* 推論アクティビティ 

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	6. MRE を再実行する場合は、[Run Again] をクリックします。
[Topology] アイコン	（注） このアイコンは、レイヤー 2 ループの問題に対して表示されます。 アイコンをクリックすると、ループが発生したネットワークセグメントのトポロジが表示されます。

PoE の問題に関する問題インスタンスの詳細

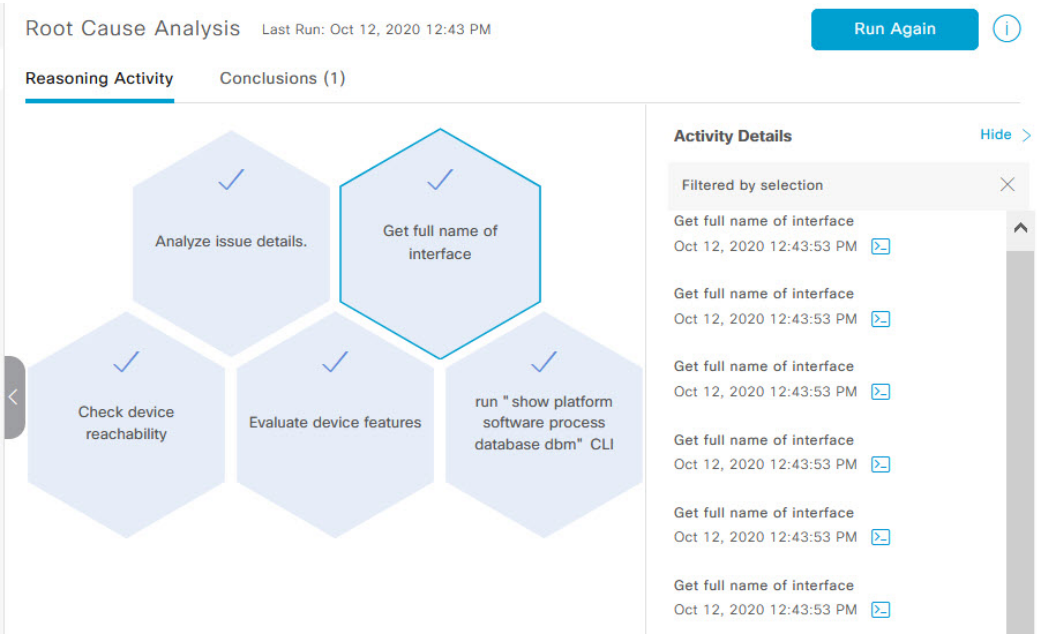
（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題を表示 （217 ページ） 」のステップ 4 を参照してください。

機械推論をサポートする PoE の問題については、[Issue Instance Details] スライドインペインに次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
[Status] ドロップダウンリスト	問題のステータスを変更できます。次の手順を実行します。 • 問題を解決するには、[Status] ドロップダウン メニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダを使用して、問題を無視する時間数を設定し、[Confirm] をクリックします。
Summary	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。
Problem Details	問題の簡単な説明と次の情報が提供されます。 • [Event Types] タブ：発生したイベントのタイプのタブが含まれます。イベントのタブをクリックすると、そのイベントタイプに関するエラーのリストが表示されます。 • [Errors]：各イベントタイプに関して発生したエラー。エラーは、クリックした [Event Types] タブに基づいて更新されます。 • [Detailed Information]：エラーをクリックすると、そのエラーに関する追加情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 **1.** [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。 **2.** このポップアップ ダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 **3.** [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。このアクティビティは、根本原因分析の各ステップで使用されたコマンドを示します。 **4.**  アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力してください。 **5.** [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインに [Activity Details] が表示されます。 実行中の推論アクティビティをキャンセルするには、[Stop] をクリックします。 （注） チェックマークは、ステップが完了したことを示します。 図 *25 :* 推論アクティビティ

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	 6. MRE を再実行する場合は、[Run Again] をクリックします。

MREを使用した有線クライアントの問題のトラブルシュート

アシュアランス によって検出された有線クライアントの問題を表示し、MRE ワークフローを使用してトラブルシュートするには、次の手順を使用します。MRE をサポートする有線クライアントの問題のリストについては、MRE の問題 （260 ページ）を参照してください。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。機械推論ナレッジベースの更新 （87 ページ）を参照してください。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

ステップ 3 [Wired Clients] サマリーエリアで、[View Details] をクリックしてスライドインペインを開きます。

ステップ 4 スライドインペインの [Wired Clients] チャートで、[Authentication] または [DHCP] をクリックします。

[Authentication] をクリックすると、チャートの下に [Top Authentication Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。認証に失敗したクライアントのリストを示すテーブルも表示されます。

[DHCP] をクリックすると、チャートの下に [Top DHCP Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。テーブルも表示されます。

ステップ 5 次のいずれかを実行します。

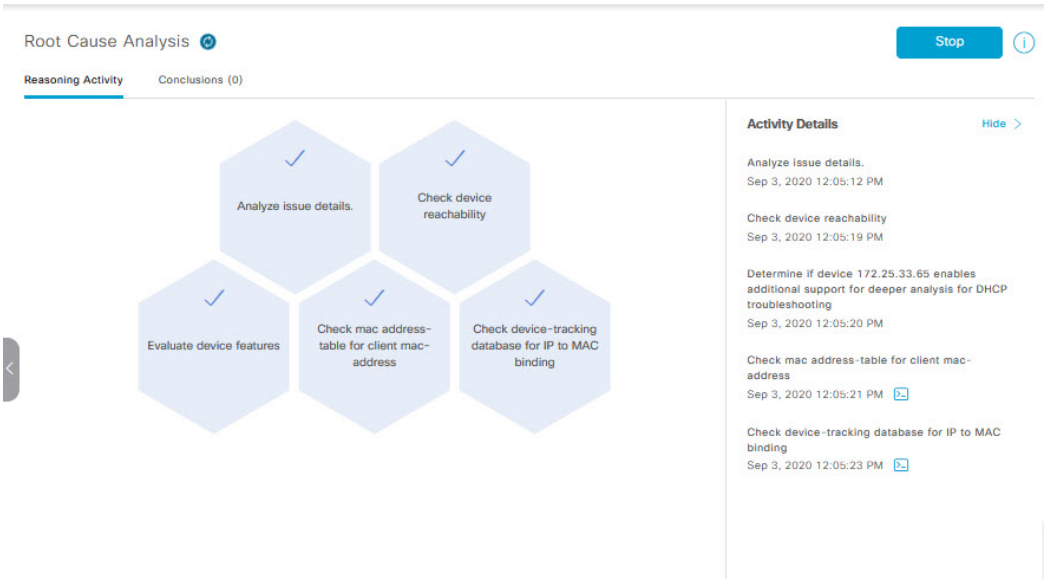
- SUPER-ADMIN-ROLE 権限を持つユーザーの場合は、検索ツールにクライアントの MAC アドレスを入力します。
- テーブルの [Identifier] 列で、ハイパーリンクされた識別子をクリックします。

クライアントの [Client 360] ウィンドウが表示されます。

ステップ 6 [Client 360] ウィンドウの [Issues] ダッシュレットで、認証または DHCP の問題をクリックします。

[Issue Details] ウィンドウに、次の情報が表示されます。

問題の詳細	
アイテム	**説明**
[Status] ドロップダウンリスト	問題の現在のステータスが表示されます。このステータスは変更できます。次の手順を実行します。 • 問題を解決するには、[Status] ドロップダウン メニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。
Summary	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。

問題の詳細	
アイテム	説明
Root Cause Analysis	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 **1.** [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。 **2.** このダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 **3.** [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。 **4.** 👍 👎 アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力し、[Submit] をクリックしてください。 **5.** [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインにアクティビティの詳細が表示されます。 実行中の推論アクティビティを停止するには、[Stop] をクリックします。 （注）　チェックマークは、ステップが完了したことを示します。 **図 *26 :* 推論アクティビティ**  **6.** MRE を再実行する場合は、[Run Again] をクリックします。

解決済みの問題の表示

次のカテゴリに分類される解決済みの問題をすべて表示するには、次の手順を実行します。

- しきい値ベースの問題：アシュアランス によって検出された問題。
- AI 駆動型の問題：Cisco AI Network Analytics によって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

始める前に

AI 駆動型の解決済みの問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認してください。Cisco AI Network Analytics データ収集の設定 （84 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboards]** > **[Issues]** の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 [Resolved] タブをクリックします。

[Resolved Issues] ウィンドウが表示されます。

ステップ 3 [Resolved Issues] ウィンドウには、次の情報が表示されます。

[Resolved Issues] ウィンドウ	
アイテム	**説明**
Global	• 上部のメニューバーで Global ⋮ をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある ⋮ をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の ⇥ をクリックすると、そのロケーションのデータのみが [Resolved Issues] ダッシュボードに表示されます。

[Resolved Issues] ウィンドウ	
アイテム	説明
[24 Hours] ドロップダウンリスト	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。
[Total Resolved]	解決済みの問題の合計数を示します。 [Total Resolved] 値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Resolved Issue] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル（事前割り当てされたもの）。
Issue Type	問題のタイプ。 （注） AI駆動型の問題の場合、問題のタイプの前に AI アイコンが表示されます。
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題タイプに関するすべての解決済み問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプ、問題を更新したエンティティ名などの情報が表示されます。

問題状況がなくなった場合、システムによる自動解決として処理され、[Updated By] 列には [System] と表示されます。自動問題解決 （240 ページ）を参照してください。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細（問題を解決したエンティティ名とタイムスタンプ）が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

無視された問題の表示

無視されたとしてマークされているすべての問題を表示するには、次の手順を実行します。無視された問題は、次のカテゴリに分類されます。

- しきい値ベースの問題：アシュアランス によって検出された問題。
- AI 駆動型の問題：Cisco AI Network Analytics によって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

始める前に

AI 駆動型の無視された問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認します。Cisco AI Network Analytics データ収集の設定 （84 ページ） を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboards]** > **[Issues]** の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 [Ignored] タブをクリックします。

[Ignored Issues] ウィンドウが表示されます。

ステップ 3 [Ignored Issues] ウィンドウには、次の情報が表示されます。

[Ignored Issues] ウィンドウ	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Ignored Issues] ダッシュボードに表示されます。
[24 Hours] ドロップダウンリスト	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。
Total Ignored	無視された問題の合計数が表示されます。 [Total Ignored] の値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Ignored Issues] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル（事前割り当てされたもの）。
Issue Type	問題のタイプ。 （注） AI駆動型の問題の場合、問題のタイプの前に AI アイコンが表示されます。

[Ignored Issues] ウィンドウの [Issue Type] 表	
アイテム	説明
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題のタイプのすべての無視された問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプなどの情報が表示されます。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

問題の解決または無視

次の手順により、問題の解決や無視を一括して、または個別に行うことができます。

ステップ 1 メニューアイコン（≡）をクリックして、**[Assurance]** > **[Dashboards]** > **[Issues]** の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 複数の問題の解決や無視を一括して行うには、次の操作を実行します。

a) [Open Issues] ダッシュボードの [Issue Type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] が開き、その問題タイプに関するすべての未解決問題が一覧表示されます。このスライドインペインでは、問題の解決や無視を一括して行えます。

b) 次のいずれかを実行します。

- 特定の問題を解決または無視するには、問題の隣にあるチェックボックスをオンにします。
- 問題タイプのブラウザウィンドウに表示される未解決の問題をすべて解決または無視するには、[issue] 列の隣にあるチェックボックスをオンにします。ブラウザウィンドウに表示されるすべての問題が選択されます。

- 未解決の問題数が 25 を超えている場合（例：100）、最初の 25 件の問題がブラウザウィンドウに表示されます。未解決の問題をすべて選択するには、次の手順を実行します。

  1. [Issue] 列の横にあるチェックボックスをオンにします。

     最初の 25 件の問題が選択され、[Actions] ドロップダウンリストの横に [Select all number open issues] タブが表示されます。

  2. [[Select all number open issues] をクリックすると、その問題タイプのすべての未解決問題（例：100 件すべての問題）が選択されます。

  3. （オプション）ブラウザウィンドウで次の 25 件の問題を表示するには、ページの下部にある [Show More] をクリックします。次の 25 件の問題がブラウザウィンドウに追加され、表示される問題の数が 50 件に増えます。ブラウザウィンドウで次の 25 件の問題を表示するには、[Show More] をもう一度クリックします。

c) 問題を解決するには、[Actions] ドロップダウンリストで [Resolve] を選択します。

   警告ダイアログボックスが表示されます。[Warning] ダイアログボックスで [Yes] をクリックして、アクションを続行します。

   問題が解決されると、[View resolved issues] タブが表示されます。[View All Issues] をクリックすると、[Resolved Issues] ウィンドウが開きます。

d) 問題を無視するには、[Actions] ドロップダウンリストで [Ignore] を選択します。

   スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。

   問題が無視されると、[View ignored issues] タブが表示されます。[View ignored issues] をクリックすると、[Ignored Issues] ウィンドウが開きます。

（注） 750 を超える問題を解決または無視しようとすると、アクションが完了するまでに 1 分ほどかかる可能性があることを知らせる警告メッセージが表示されます。

ステップ 3 問題を個別に解決または無視するには、次の手順を実行します。

a) [Issue Instances] スライドインペイン（最初のスライドイン ペイン）の [issue] 列で、問題をクリックします。
   2 番目のスライドインペイン [Issue Instance Details] が開き、問題に関する詳細が表示されます。この 2 番目のスライドインペインで、表示している問題を解決または無視できます。

b) 問題を解決するには、[Status] ドロップダウン メニューで [Resolve] を選択します。

c) 問題の報告を停止するには、次の手順を実行します。

   1. [Status] ドロップダウンリストから、[Ignore] を選択します。

   2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。

無線停止の問題のトリガー

無線停止の問題は、次のすべての条件がデフォルトのトリガー時間である 60 分間にわたって満たされるとトリガーされます。

（注） デフォルトのトリガー時間を変更するには、**アシュアランス**[Manage] > [Issue Settings] に移動します。問題の設定の管理 （241 ページ）を参照してください。

- AP 無線動作状態は [up] である。
- AP モードはローカルまたは Flex-Connect である。
- この無線でクライアント数が 0 である。
- RX データまたは管理フレーム数が増えていない。
- AP 無線チャンネルの使用率が 0 である。
- AP は**分離された** AP ではない。

自動問題解決

次のタイプの問題については、問題の状態が存在しなくなった場合、システムは自動的に問題を解決します。

- インターフェイスが停止した。
- ワイヤレスコントローラ/スイッチ/ルータが到達不能である。
- WLC からの AP の切断。
- 無線でのアクティビティなし。

（注） 次のいずれかの状態が解消した場合、システムによって自動的にこの問題が解決されます。

- この無線でクライアント数が 0 である。
- RX データまたは管理フレーム数が増えていない。
- AP 無線チャンネルの使用率が 0 である。

問題が解決されると、[Resolved Issues] > [Issue Instance] スライドインペインの [Updated By] カラムに、[System] と表示されます。「解決済みの問題の表示 （234 ページ） 」の**ステップ 3** を参照してください。

問題の設定の管理

次の手順に従って、問題の設定を管理します。トリガー可能な特定の問題を有効または無効にする、問題の優先順位を変更する、問題がトリガーされるしきい値を変更する、トリガーされたときに問題を外部通知に登録するといった操作を実行できます。

ステップ 1 メニューアイコン（≡）をクリックして、 **[Assurance]** > **[Manage]** > **[Issue Settings]** の順に選択します。

[Issue Settings] ウィンドウが表示されます。

ステップ 2 設定する問題のタイプを表示するには、[DEVICE TYPE] と [CATEGORY] フィルタを設定します。

AI 駆動型の問題を表示するには、[CATEGORY] フィルタの [AI-Driven] タブをクリックします。

ステップ 3 [Issue Name] 列の問題をクリックすると、次の設定を含むスライドインペインが開きます。

（注） いくつかの問題については、設定に加えられた変更は複数のデバイス タイプで共有されます。スライドインペインで、情報アイコン（ⓘ）にカーソルを合わせると、影響を受けるデバイス タイプが表示されます。

a) 問題がトリガー可能かどうかを有効または無効にするには、[Enabled] トグルをクリックします。

b) 問題の優先順位を設定するには、[Priority] ドロップダウンリストをクリックし、優先順位を選択します。次のオプションがあります。

- [P1]：ネットワーク運用に幅広い影響を与える可能性がある、早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
- [P3]：局所的または最小限の影響を与える軽微な問題。
- [P4]：ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。

c) （一部の問題のみ）[Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。

（注） 無線停止のトリガー条件については、無線停止の問題のトリガー （240 ページ） を参照してください。

トリガー条件の例：

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

アクセスポイントのメモリ使用率が 90% を超えた

d) （任意） 設定に変更がある場合は、[View Default Settings] の上にカーソルを置くと、デフォルトの問題が表示されます。問題の設定をすべてデフォルト値に復元するには、[Use Default] をクリックします。

e) [Apply] をクリックします。

ステップ 4 [Manage Subscriptions] をクリックすると、サポートされている問題がトリガーされたときに外部通知に登録できます。問題の通知の有効化 （242 ページ）を参照してください。

問題の通知の有効化

アシュアランスで特定の問題がトリガーされたときに外部通知を受信するには、次の手順を実行します。問題がトリガーされてステータスが変わると、アシュアランスは、REST または電子メール通知を生成できます。

ステップ 1 メニューアイコン（☰）をクリックして、 **[Assurance]** > **[Manage]** > **[Issue Settings]** の順に選択します。

[Issue Settings] ウィンドウが表示されます。

ステップ 2 [Manage Subscriptions] をクリックします。

[Events] ウィンドウが表示されます。

ステップ 3 登録するイベントのチェックボックスをオンにします。

（注） Cisco DNA Center プラットフォーム の [Event] の名前は、アシュアランス の [Issue Name] と同じです。

ステップ 4 [Subscribe] をクリックします。
[Subscribe] ダイアログボックスが表示されます。

ステップ 5 [Subscribe] ダイアログボックスで、サブスクリプションの詳細を入力します。

a) [Name] フィールドに、サブスクリプション名を入力します。

b) [Subscription Type] ドロップダウンリストをクリックして、通知タイプを選択します。REST または電子メール通知を受信できます。

通知タイプ	詳細
[REST]	問題/イベントがトリガーされたときに、REST 通知を受信します。次の設定を行います。 • [Select an existing endpoint] または [Create a new endpoint] のどちらかのオプションを選択して、そのエンドポイントを指定し、そのエンドポイントの後続のフィールドを設定します。 • **信頼できる証明書** • [HTTP Method]：[POST] または [PUT] を選択できます。 • [Headers]：[Header Key] フィールドと [Header Value] フィールドにヘッダーの詳細を入力します。
[EMAIL]	問題/イベントがトリガーされたときに電子メール通知を受信します。 **重要** 電子メール通知を受信するには、⚙ > **[System Settings]** > **[Email configuration]** ウィンドウで、電子メールサーバーが設定されていることを確認します。

c) [Subscribe] をクリックします。

問題/イベントのサブスクリプションが作成されます。問題/イベントがトリガーされると、ステータス変更の通知が送信されます。

次のタスク

Cisco DNA Center プラットフォーム で既存のイベントサブスクリプションを表示および管理できます。詳細については、『*Cisco DNA Center Platform User Guide*』の「*Working with Events*」を参照してください。

アシュアランス、Cisco AI Network Analytics、および MRE の問題

ルータの問題

アシュアランス で検出されるルータの問題を次の表に示します。

ルータの問題		
カテゴリ	**問題の名称**	**[Summary]**
接続性	BGP トンネル接続	自律システム（AS）番号が間違っているため、ピアとのボーダーゲートウェイ プロトコル（BGP）接続に失敗しました。
接続性	ネットワークデバイスを接続しているインターフェイスでダウン発生	ネットワークデバイスを接続しているインターフェイスがダウンしています。
接続性	レイヤ 2 のループ症状	ネットワークデバイスでホストMACアドレスのフラッピングが見られます。
接続性	ネットワークデバイスインターフェイスの接続 - BGP フラップ	ネイバーとのボーダー ゲートウェイ プロトコル（BGP）接続がフラッピングしています。
接続性	ネットワーク デバイス インターフェイスの接続 - EIGRP 隣接関係の障害	ネイバーとの Enhanced Interior Gateway Routing Protocol（EIGRP）隣接関係に障害が発生しました。
接続性	ネットワークデバイスインターフェイスの接続 - インターフェイスダウン	デバイス上のインターフェイスがダウンしています。
接続性	ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害	デバイスで Intermediate System Intermediate System（ISIS）の隣接関係に障害が発生しました。
接続性	ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害	ネイバーとの Open Shortest Path First（OSPF）隣接関係に障害が発生しました。
接続	WAN インターフェイスダウン	WAN ネットワークに接続しているインターフェイスがダウンしています。
接続されている状態	SGT のアクセスポリシーのインストールに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセスポリシーのインストールに失敗しました。
接続されている状態	ルータインターフェイスの入出力エラー率が高い	インターフェイスの入出力エラー率が高くなっています。
接続されている状態	ルータインターフェイスの入出力破棄率が高い	インターフェイスの入出力破棄率が高くなっています。
接続されている状態	ルータインターフェイスの入力/出力使用率が高い	インターフェイスの入出力使用率が高くなっています。

ルータの問題		
カテゴリ	**問題の名称**	**[Summary]**
接続されている状態	ルータ WAN インターフェイスの入出力破棄率が高い	WAN インターフェイスの入出力破棄率が高くなっています。
接続されている状態	ルータ WAN インターフェイスの入力/出力使用率が高い	WAN インターフェイスの入出力使用率が高くなっています。
接続されている状態	デバイスでSGTアクセスポリシーのダウンロードに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセス コントロール エントリ（ACE）のダウンロードに失敗しました。
接続されている状態	デバイスでSGTアクセスポリシーのインストールに失敗	セキュリティグループタグ（SGT）のアクセスポリシーのインストールに失敗しました。ロールベースのアクセスコントロールリスト（RBACL）でポリシールールエラーが見つかりました。
接続されている状態	ポリシーサーバーからSGTアクセスポリシーをダウンロードできない	セキュリティグループタグ（SGT）のアクセスポリシーのソースリストをダウンロードできませんでした。
接続されている状態	デバイスでSGTアクセスポリシーのアンインストールに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセスポリシーのアンインストールに失敗しました。
デバイス	DNA Centerとネットワークデバイスの時間差	Cisco DNA Center とデバイスの間に過剰なタイムラグがあります。
デバイス	syslogイベントに基づく問題 - 高温	高温に関連する syslog イベントの単一オカレンスによって作成された問題。
デバイス	ルータの高 CPU 使用率	デバイスで CPU 使用率が高くなっています。
デバイス	ルータの高メモリ使用率	デバイスでメモリ使用率が高くなっています。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスで高可用性（HA）スイッチオーバーが発生しました。
可用性	ルータ到達不能	ネットワークデバイスがコントローラから到達不能です。

コア層、ディストリビューション層、およびアクセス層に関する問題

アシュアランスによって検出されるコア層、ディストリビューション層、およびアクセス層の問題を次の表に示します。

コア層、ディストリビューション層、およびアクセス層に関する問題		
カテゴリ	**問題の名称**	**[Summary]**
接続性	BGP トンネル接続	自律システム（AS）番号が間違っているため、ピアとのBGP接続に失敗しました。
接続性	ネットワークデバイスを接続しているインターフェイスでダウン発生	ネットワークデバイスを接続しているインターフェイスがダウンしています。
接続性	レイヤ 2 のループ症状	ネットワークデバイスでホストMACアドレスのフラッピングが見られます。
接続性	ネットワークデバイスインターフェイスの接続 - BGP フラップ	ネイバーとの BGP 接続がフラッピングしています。
接続性	ネットワーク デバイス インターフェイスの接続 - EIGRP 隣接関係の障害	ネイバーとの EIGRP（Enhanced Interior Gateway Routing Protocol）隣接関係に障害が発生しました。
接続性	ネットワークデバイスインターフェイスの接続 - インターフェイスダウン	デバイス上のインターフェイスがダウンしています。
接続性	ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害	デバイスで Intermediate System Intermediate System（IS-IS）の隣接関係に障害が発生しました。
接続性	ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害	ネイバーとの Open Shortest Path First（OSPF）隣接関係に障害が発生しました。
接続	WAN インターフェイスダウン	WANネットワークに接続しているインターフェイスがダウンしています。
接続性	ネットワークデバイスでデュアルアクティブ検出リンクに障害発生	ネットワークデバイス *Switch Name* でデュアルアクティブ検出リンクに障害が発生しました。
接続性	ネットワークデバイスでStackWise Virtual リンクに障害発生	ネットワークデバイスの *Switch Name* で StackWise Virtual リンクに障害が発生しました。
接続	ネットワークデバイスでStackWise リンクに障害発生	ネットワークデバイス *Switch Name* で StackWise リンクに障害が発生しました。
接続されている状態	ファブリックデバイスの接続-ボーダーオーバーレイ	ファブリックエッジが仮想ネットワーク内のファブリックボーダーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続-ボーダーアンダーレイ	ファブリックエッジが物理ネットワーク内のファブリックボーダーへの接続を失いました。

コア層、ディストリビューション層、およびアクセス層に関する問題		
カテゴリ	**問題の名称**	**[Summary]**
接続されている状態	ファブリックデバイスの接続 - コントロールボーダーアンダーレイ	ファブリックノードは、物理ネットワーク内の同じ場所に配置されたファブリックボーダーとコントロールプレーンへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - コントロールアンダーレイ	ファブリックノードは、物理ネットワーク内のファブリック コントロール プレーン デバイスへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DHCP オーバーレイ	ファブリックノードが仮想ネットワーク内の DHCP サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DHCP アンダーレイ	ファブリックノードが物理ネットワーク内の DHCP サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DNS オーバーレイ	ファブリックノードが仮想ネットワーク内の DNS サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DNS アンダーレイ	ファブリックノードが物理ネットワーク内の DNS サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - 外部 URL	ユーザーがプロビジョニングした外部 URL にファブリックボーダーが到達できません。
接続されている状態	ファブリックデバイスの接続 - ISE サーバー	ファブリックエッジが物理ネットワーク内の ISE サーバーへの接続を失いました。
接続されている状態	SGT のアクセスポリシーのインストールに失敗	SGT の SGACL アクセスポリシーのインストールに失敗しました。
接続されている状態	スイッチインターフェイスの入出力エラー率が高い	スイッチインターフェイスの入出力エラー率が高くなっています。
接続されている状態	スイッチインターフェイスの入出力破棄率が高い	スイッチインターフェイスの入出力破棄率が高くなっています。
接続されている状態	スイッチインターフェイスの入出力使用率が高い	インターフェイスの入出力使用率が高くなっています。
接続されている状態	デバイスで SGT アクセスポリシーのダウンロードに失敗	SGT の SGACL ACE のダウンロードに失敗しました。
接続されている状態	デバイスで SGT アクセスポリシーのインストールに失敗	SGT のアクセスポリシーのインストールに失敗しました。RBACL でポリシー規則エラーが検出されました。
接続されている状態	ポリシーサーバーから SGT アクセスポリシーをダウンロードできない	SGT のアクセスポリシーのソースリストをダウンロードできませんでした。

コア層、ディストリビューション層、およびアクセス層に関する問題		
カテゴリ	**問題の名称**	**[Summary]**
接続されている状態	デバイスでSGTアクセスポリシーのアンインストールに失敗	SGT の SGACL アクセス ポリシーのアンインストールに失敗しました。
デバイス	デバイスリブートクラッシュ	ハードウェアまたはソフトウェアのクラッシュによりデバイスがリブートしました。
デバイス	デバイス時間のずれ Cisco DNA Center	Cisco DNA Center とデバイスの間に過剰なタイムラグがあります。
デバイス	ネットワークデバイスでインターフェイスのフラッピングが発生	ポートインターフェイスがスイッチでフラッピングしています。
デバイス	syslogイベントに基づく問題 - 高温	高温に関連する syslog イベントの単一オカレンスによって作成された問題。
デバイス	syslogイベントに基づく問題 - POE	電源に関連する syslog イベントの単一オカレンスによって作成された問題。
デバイス	PoE ポートがエラー状態	PoE ポートがエラーにより無効になっていることが syslog イベントで報告されました。
デバイス	PoE 受電デバイスに障害フラグあり	PoE ポートに接続された PoE 対応デバイスに障害フラグが設定されていることが syslog イベントで報告されました。
デバイス	PoE 受電デバイスへの電力供給拒否	PoE ポートに接続された PoE 対応デバイスへの電力供給が拒否されたことが syslog イベントで報告されました。
デバイス	スタックメンバーの削除	スタックメンバーが削除されました。
デバイス	スタックメンバーが互換性のないイメージを実行	スタックメンバーが互換性のないイメージを実行しています。
デバイス	スイッチの高 CPU 使用率	デバイスで CPU 使用率が高くなっています。
デバイス	スイッチの高メモリ使用率	デバイスでメモリ使用率が高くなっています。
デバイス	スイッチファンの障害	スイッチのファンに障害が発生しました。
デバイス	スイッチの電源障害	スイッチの電源に障害が発生しました。
デバイス	高 TCAM 使用率の問題	レイヤ 2、レイヤ 3、QoS、および SGACL での TCAM 枯渇の問題。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスでHAスイッチオーバーが発生しました。
可用性	スイッチ到達不能	デバイスが到達不能です。

コア層、ディストリビューション層、およびアクセス層に関する問題		
カテゴリ	**問題の名称**	**[Summary]**
使用率（Utilization）	マップキャッシュの上限に達した	マップキャッシュエントリがマップサーバーの上限を超えました。

コントローラの問題

アシュアランス によって検出されるコントローラの問題を次の表に示します。

コントローラの問題		
カテゴリ	**問題の名称**	**[Summary]**
接続性	ネットワークデバイスを接続しているインターフェイスでダウン発生	ネットワークデバイスを接続しているインターフェイスがダウンしています。
接続されている状態	ファブリック WLC と MapServer の接続性	ファブリック WLC がファブリック コントロール プレーン ノードへの接続を失いました。
デバイス	デバイス時間のずれ Cisco DNA Center	Cisco DNA Center とデバイスの間に過剰なタイムラグがあります。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスでHAスイッチオーバーが発生しました。
可用性	WLC モニター	ネットワークコントローラがWLCからデータを受信していません。
可用性	WLC 電源の障害	この WLC で電源に障害が発生しました。
可用性	WLC のリブートクラッシュ	WLC のリブートクラッシュが発生しました。
可用性	WLC 到達不能	デバイスが到達不能です。
使用率（Utilization）	WLC での AP ライセンス枯渇	WLC には現在、空いている AP ライセンスはありません。
使用率（Utilization）	WLC 高メモリ使用率	WLC のメモリ使用率が高くなっています。

アクセスポイントの問題

アシュアランス によって検出されるアクセスポイントの問題を次の表に示します。

アクセスポイントの問題		
カテゴリ	**問題の名称**	**[Summary]**
可用性	AP のカバレッジホール	AP にカバレッジ ホールがあります。
可用性	Cisco WLC からの AP の切断	AP が切断されています。
可用性	AP のフラッピング	AP でフラッピングが発生しています。この問題は、AP が 15 分以内に 2 回以上フラップすると発生します。
可用性	AP のリブートクラッシュ	ハードウェアまたはソフトウェアのクラッシュにより AP がリブートしました。
使用率（Utilization）	AP の高 CPU 使用率	AP で CPU 使用率が高くなっています。
使用率（Utilization）	AP の高メモリ使用率	AP のメモリ使用率が高くなっています。
使用率（Utilization）	無線の高使用率（2.4 GHz）	AP の 2.4 GHz 無線の使用率が高くなっています。
使用率（Utilization）	無線の高使用率（5 GHz）	AP の 5 GHz 無線の使用率が高くなっています。
使用率（Utilization）	無線でのアクティビティなし（2.4 GHz）	AP の 2.4 GHz 無線 x でアクティビティがありません。
使用率（Utilization）	無線でのアクティビティなし（5 GHz）	AP の 5 GHz 無線 x でアクティビティがありません。
AP 異常	AP 異常	AP で異常が発生しました。
可用性	フロアでの RF（2.4 GHz）の低下	この問題は、APのワイヤレスエクスペリエンスが低い場合に発生します。 無線周波数（RF）の低下の問題には次のようなものがあります。 • 単一の問題は、干渉またはノイズが、30分以内に特定のAP帯域のしきい値を超えた場合にトリガーされます。 • グローバルな問題は、少なくとも1つのAPの干渉またはノイズが、30 分以内にしきい値を超えた場合にトリガーされます。

アクセスポイントの問題		
カテゴリ	**問題の名称**	**[Summary]**
可用性	フロアでの RF（5 GHz）の低下	この問題は、APのワイヤレスエクスペリエンスが低い場合に発生します。 RF の低下の問題には次のようなものがあります。 • 単一の問題は、干渉またはノイズが、30分以内に特定のAP帯域のしきい値を超えた場合にトリガーされます。 • グローバルな問題は、少なくとも1つのAPの干渉またはノイズが、30 分以内にしきい値を超えた場合にトリガーされます。

有線クライアントの問題

アシュアランス によって検出される有線クライアントの問題を次の表に示します。

有線クライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IP アドレスを取得できませんでした。
オンボーディング	有線クライアント認証エラー - Dot1.x エラー	有線クライアント認証に失敗しました。Dot1.x を使用するユーザーデバイス認証のエラーです。 （注） この問題は、単独の有線クライアントにのみ適用されます。
オンボーディング	有線クライアント認証エラー - MAB エラー	有線クライアント認証に失敗しました。ユーザーデバイス認証が MAC 認証バイパスの問題により失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。

ワイヤレスクライアントの問題

アシュアランス によって検出されるワイヤレスクライアントの問題を次の表に示します。

（注） この問題は、単独のクライアントと複数のクライアントの両方に適用されます。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
オンボーディング	802.11r クライアントの低速ローミング	高速ローミングが可能なワイヤレスクライアントが、ローミング中に高速認証ではなくフル認証を実行しています。
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IP アドレスを取得できませんでした。
オンボーディング	ワイヤレスクライアントの除外 - クライアントがローミング前に除外される	ワイヤレスクライアントの除外 - クライアントがローミングの前に除外されました。
オンボーディング	ワイヤレスクライアントの除外 - IP 盗難の問題	ワイヤレスクライアントの除外 - IP 盗難の問題が発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーによるクライアントの拒否	ワイヤレス クライアントの接続失敗 - AAA サーバーによりクライアントが拒否されました。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウト	ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアント PMK が見つからない	ワイヤレスクライアントの接続失敗 - クライアント PMK が見つかりません。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウト	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証に失敗しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウト	ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - DHCP タイムアウト	ワイヤレスクライアントの接続失敗 - DHCP タイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスの取得失敗	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスを取得できませんでした。
オンボーディング	ワイヤレスクライアントの接続失敗 - 不正な PSK	ワイヤレスクライアントは接続に失敗し、除外されました。クライアントの PSK は設定された WLAN PSK と一致しませんでした。
オンボーディング	ワイヤレスクライアントの接続失敗 - セキュリティパラメータの不一致	ワイヤレス クライアントの接続失敗 - セキュリティパラメータが一致していません。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
オンボーディング	ワイヤレスクライアントの接続失敗 - WLC 設定エラー	ワイヤレスクライアントの接続失敗 - WLC 設定エラーが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - WLC 内部エラー	ワイヤレスクライアントの接続失敗 - WLC 内部エラーが発生しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - AAA サーバーによるクライアントの拒否	ワイヤレスクライアントのローミング失敗 - AAA サーバーによりクライアントが拒否されました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - AAA サーバーのタイムアウト	ワイヤレスクライアントのローミング失敗 - AAA サーバーでタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - クライアント PMK 未検出	ワイヤレスクライアントのローミング失敗 - クライアント PMK が見つかりません。
オンボーディング	ワイヤレスクライアントのローミング失敗 - クライアントのタイムアウト	ワイヤレスクライアントのローミング失敗 - クライアントのタイムアウトにより認証に失敗しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - セキュリティパラメータの不一致	ワイヤレスクライアントのローミング失敗 - セキュリティパラメータが一致していません。
オンボーディング	ワイヤレスクライアントのローミング失敗 - WLC 設定エラー	ワイヤレスクライアントのローミング失敗 - WLC 設定エラーが発生しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - WLC 内部エラー	ワイヤレスクライアントのローミング失敗 - WLC 内部エラーが発生しました。
オンボーディング	ワイヤレスクライアントの AP 間のローミング失敗 - 外部エラー	ワイヤレスクライアントの AP 間のローミング失敗 - 外部エラーが発生しました。
オンボーディング	ワイヤレスクライアントの AP 間のローミング失敗 - WLC 設定の不一致	ワイヤレスクライアントの AP 間のローミング失敗 - WLC 設定が一致しません。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - 認証タイムアウトによる過剰な時間	ワイヤレスクライアントの接続に時間がかかる - 認証タイムアウトにより過剰な時間がかかります。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害による過剰な時間	ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害により過剰な時間がかかります。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーによる過剰な時間	ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーによる過剰な時間がかかりました。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - WLC の障害による過剰な時間	ワイヤレスクライアントの接続に時間がかかる - WLC の障害により過剰な時間がかかりました。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - AAA サーバーまたはネットワークの遅延による過剰な認証時間	ワイヤレスクライアントの接続に時間がかかる - AAA サーバーまたはネットワークの遅延により過剰な認証時間がかかりました。
オンボーディング	ワイヤレスクライアントの除外 - IP 盗難の問題	ワイヤレスクライアントの除外 - IP 盗難の問題が発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーによるクライアントの拒否	ワイヤレスクライアントの接続失敗 - AAA サーバーによりクライアントが拒否されました。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウト	ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアント PMK 未検出	ワイヤレス クライアントの接続失敗 - クライアント PMK が見つかりません。
オンボーディング	ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウト	ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証失敗	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証に失敗しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトによる IP アドレス取得失敗	ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスを取得できませんでした。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
オンボーディング	ワイヤレスクライアントの接続失敗 - DHCPサーバーまたはクライアントのタイムアウトによるIPアドレスを取得失敗	ワイヤレスクライアントの接続失敗 - DHCP サーバーまたはクライアントのタイムアウトにより IP アドレスを取得できませんでした。
オンボーディング	ワイヤレスクライアントの接続失敗 - 不正な PSK	ワイヤレスクライアントは接続に失敗し、除外されました。クライアントの PSK は設定された WLAN PSK と一致しませんでした。
オンボーディング	ワイヤレスクライアントの接続失敗 - セキュリティパラメータの不一致	ワイヤレスクライアントの接続失敗 - 認証中にセキュリティパラメータが一致していません。
オンボーディング	ワイヤレスクライアントの接続失敗 - WLC 設定エラー	ワイヤレスクライアントの接続失敗 - WLC 設定エラーが発生しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - WLC のクライアント除外ポリシー	ワイヤレスクライアントのローミング失敗 - クライアントは WLC のクライアント除外ポリシーにより除外されました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - クライアントがローミングの前に除外される	ワイヤレスクライアントのローミング失敗 - クライアントがローミングの前に除外されました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - WLC 設定の不一致	ワイヤレスクライアントの AP 間のローミング失敗 - WLC 設定が一致しません。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害による過剰な時間	ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害により過剰な時間がかかりました。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラー	ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーにより過剰な時間がかかりました。
オンボーディング	ワイヤレスクライアントの接続に時間がかかる - WLC の障害	ワイヤレスクライアントの接続に時間がかかる - WLC の障害により過剰な時間がかかりました。
接続されている状態	デュアルバンド対応クライアントが 5 GHzより 2.4 GHzを優先	デュアルバンド対応クライアントは、より優れたエクスペリエンスを提供する 5 GHz 無線が利用できるにもかかわらず、一貫して 2.4 GHz 無線に接続しています。
接続されている状態	ワイヤレスクライアントの RF が弱い	ワイヤレスクライアントに、ローミングできる、信号の強いネイバー AP がないため、クライアントの RF 状態が低下しています。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**[Summary]**
接続されている状態	ワイヤレスクライアントのスティッキーな動作	ワイヤレスクライアントは、信号が弱いAPとのアソシエーションを維持しています。信号強度の高い利用可能なAPにローミングする必要があります

アプリケーションの問題

アシュアランス によって検出されるアプリケーションの問題を次の表に示します。

アプリケーションの問題		
カテゴリ	**問題の名称**	**[Summary]**
アプリケーション	アプリケーションエクスペリエンスの問題	アプリケーションエクスペリエンスに関するすべての問題。

センサーの問題

アシュアランス で検出されるセンサーの問題を次の表に示します。

同じフロアにある 2 つ以上のセンサーが 30 分間のテストに失敗した場合、センサーは失敗の根本原因に基づいて問題を報告することがあります。これらのセンサーの問題はすべてグローバルな問題です。つまり、すべてのフロアのセンサーの問題がエスカレーションされて、[Issues] ダッシュボードに表示されます。

センサーの問題		
カテゴリ	**問題の名称**	**[Summary]**
センサーテスト	センサー - 速度テスト HTTP エラー	クエリサーバーへのアクセス中、複数のセンサーが速度テスト HTTP エラーを報告しています。
センサーテスト	センサー - DHCPの障害	複数のセンサーが IPv4 アドレスを取得できませんでした。
センサーテスト	センサー - DNS 解決の失敗	複数のセンサーが DNS サーバーによるドメイン名の解決に失敗しました。
センサーテスト	センサー - オンボーディング時の関連付けの失敗	複数のセンサーがオンボーディング時の関連付けに失敗しました。
センサーテスト	センサー - オンボーディング時の認証の失敗	複数のセンサーがオンボーディング時の認証に失敗しました
センサーテスト	センサー - FTP テスト失敗	複数のセンサーが FTP サーバーに接続できないことを報告しています。

センサーの問題		
カテゴリ	**問題の名称**	**[Summary]**
センサーテスト	センサー - FTP 転送の失敗	複数のセンサーが FTP サーバーとのファイル転送に失敗したことを報告しています。
センサーテスト	センサー - FTP 到達不能	複数のセンサーが FTP サーバーに到達できないことを報告しています。
センサーテスト	センサー - IPerf の無効な設定エラー	無効な iPerf 設定を受信したため、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPerf サーバーがビジー状態	iPerfのビジー状態エラーが原因で、複数のセンサーが iPerfテストを実行できませんでした。
センサーテスト	センサー - IPerf テストネットワークエラー	iPerfのネットワークエラーが原因で、複数のセンサーが iPerfテストを実行できませんでした。
センサーテスト	センサー - IPerf 未定義のエラー	未定義エラーが原因で、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPSLA IP アドレスなし	複数のセンサーが Cisco DNA Center から IPSLA テスト IP アドレスを受信していないことを報告しています。
センサーテスト	センサー - IPSLA 応答なし	複数のセンサーが IPSLA テストで IPSLA 応答側からの応答がないことを報告しています。
センサーテスト	センサー - IPSLA ソケットエラー	複数のセンサーが IPSLA テストソケットエラーを報告しています。
センサーテスト	センサー - IPSLA テスト失敗	複数のセンサーが IPSLA テスト失敗を報告しています。
センサーテスト	センサー - IPSLA 非対応プローブタイプ	複数のセンサーが IPSLA テスト非対応プローブタイプを報告しています。
センサーテスト	センサー - メールサーバーのテスト失敗	複数のセンサーがメールサーバーに接続できなかったことを報告しています。
センサーテスト	センサー - メールサーバーに到達不能	複数のセンサーがメールサーバーに到達できないことを報告しています。
センサーテスト	センサー - NDT サーバーなし	複数のセンサーが速度テスト NDT サーバーが存在しないことを報告しています。
センサーテスト	センサー - オンボーディングの障害	センサーがワイヤレスネットワークに接続できませんでした。
センサーテスト	センサー - Outlook サーバーのテスト失敗	複数のセンサーが Outlook Web アクセスに接続できなかったことを報告しています。

センサーの問題		
カテゴリ	**問題の名称**	**[Summary]**
センサーテスト	センサー - Outlook サーバーに到達不能	複数のセンサーが Outlook Web アクセスホストに到達できないことを報告しています。
センサーテスト	センサー - クエリサーバーのタイムアウト	複数のセンサーが速度テスト対象クエリサーバーのタイムアウトを報告しています。
センサーテスト	センサー - RADIUS 認証の失敗	複数のセンサーが RADIUS サーバーでの認証に失敗したことを報告しています。
センサーテスト	センサー - 速度テスト失敗	複数のセンサーが速度テスト失敗を報告しています。
センサーテスト	センサー - 速度テストの一般的なエラー	複数のセンサーが速度テストの一般的な障害を報告しています。
センサーテスト	センサー - 速度テストのアップリンクタイムアウト	複数のセンサーが速度テストでのアップリンクテストのタイムアウトを報告しています。
センサーテスト	センサー - 速度テスト URL エラー	クエリサーバーへのアクセス中、複数のセンサーが速度テスト URL エラーを報告しています。
センサーテスト	センサー - 到達不能なホスト	複数のセンサーがホストへの ping の失敗を報告しています。ホストに到達できません。
センサーテスト	センサー - 到達不能な RADIUS	複数のセンサーが RADIUS サーバーに到達できないことを報告しています。
センサーテスト	センサー - Web 認証の失敗	複数のセンサーが、クライアントが Web 認証テストに失敗していることを報告しています。
センサーテスト	センサー - Web サーバーのテスト失敗	複数のセンサーが Web サーバーからページをロードできなかったことを報告しています。
センサーテスト	センサー - Web サーバーに到達不能	複数のセンサーが Web サーバーに到達できないことを報告しています。
センサーテスト	センサー - Web ソケットエラー	複数のセンサーがテスト中に速度テスト websocket エラーを報告しています。
センサーテスト	センサー - 速度テストのアップリンクプロキシエラー	複数のセンサーが速度テストのアップリンクテストでプロキシエラーを報告しています。

AI 駆動型の問題

Cisco AI Network Analytics によって検出される AI 駆動型の問題を次の表に示します。

AI 駆動型の問題		
カテゴリ	**問題の名称**	**[Summary]**
接続の問題		
オンボーディング	AI 過剰な接続時間 - 基準から大きく乖離	通常と比較して、ネットワークでのオンボーディング時間がかなり長くなっています。クライアントは、*SSID* に接続するのに通常より時間がかかっています。
オンボーディング	AI 過剰な接続障害回数 - 基準から大きく乖離	通常と比較して、ネットワークでのオンボーディング時間がかなり長くなっています。クライアントは、*SSID* に接続するのに通常より時間がかかっています。
オンボーディング	AI 過剰なワイヤレスクライアントの接続時間 - 基準を上回る合計時間	ワイヤレスクライアントが、*location* にある *SSID* への接続に時間がかかりました。
AAA	AI 過剰な関連付け時間 - 基準から大きく乖離	過剰な関連付け時間 - *SSID* での時間が少なくとも *value*% 増加しています。
AAA	AI 過剰な関連付け障害回数 - 基準から大きく乖離	過剰な関連付け障害回数 - *SSID* での障害回数が少なくとも *value*% 増加しています。
AAA	AI 過剰な認証時間 - 基準から大きく乖離	過剰な認証時間 - *SSID* での時間が少なくとも *value*% 増加しています。
AAA	AI 過剰な認証障害回数 - 基準から大きく乖離	過剰な認証障害回数 - *SSID* での障害回数が少なくとも *value*% 増加しています。
DHCP	AI IPアドレスの取得にかかる過剰な時間 - 基準から大きく乖離	IP アドレスを取得するための過剰な時間 - *server_IP*からの取得時間が少なくとも *value*% 増加しています。
DHCP	AI 過剰なIPアドレス取得失敗回数 - 基準から大きく乖離	過剰なIPアドレス取得失敗回数 - *server_IP* での障害回数が少なくとも *value*% 増加しています。
ネットワークの接続性に関する問題		
接続性	AI ネットワークデバイスでホストMACアドレスのフラッピングが発生	ネットワークでレイヤ 2 のループ症状が発生しています。
アプリケーションエクスペリエンスの問題		
スループット	AI すべてのアプリケーションの合計無線スループットの低下	ネットワーク内のAPで、すべてのアプリケーションの合計無線スループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。

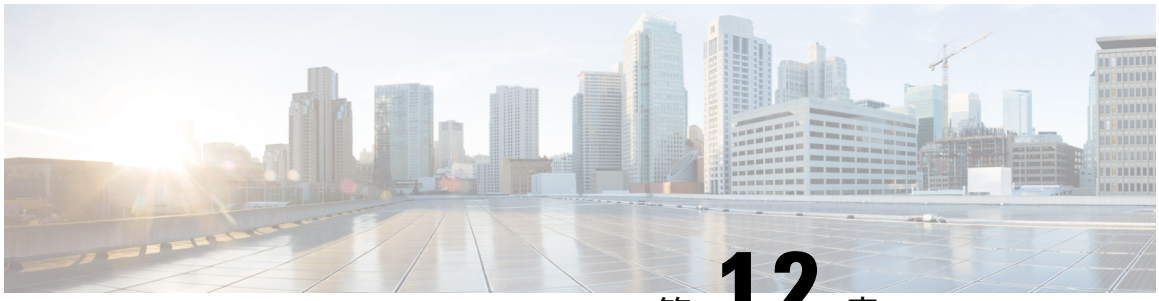
AI 駆動型の問題		
カテゴリ	**問題の名称**	**[Summary]**
スループット	AI クラウドアプリケーションの無線スループットの低下	ネットワーク内の AP で、クラウドアプリケーションのスループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。
スループット	AI ソーシャルアプリケーションの無線スループットの低下	ネットワーク内の AP で、ソーシャルアプリケーションのスループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。
スループット	AI メディアアプリケーションの無線スループットの低下	ネットワーク内の AP で、メディアアプリケーションのスループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。
スループット	AI Colab アプリケーションの無線スループットの低下	ネットワーク内の AP で Colab アプリケーションのスループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。

MRE の問題

次の表に、MRE ワークフローを使用してトラブルシュート可能な アシュアランス で検出される問題を示します。

MRE の問題		
カテゴリ	**問題の名称**	**[Summary]**
有線クライアントの問題		
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IPv4 アドレスを取得できませんでした。
オンボーディング	有線クライアント認証エラー - Dot1.x エラー	有線クライアント認証に失敗しました。Dot1.x を使用するユーザーデバイス認証のエラーです。 （注） この問題は、単独の有線クライアントにのみ適用されます。
オンボーディング	有線クライアント認証エラー - MAB エラー	有線クライアント認証に失敗しました。ユーザーデバイス認証が MAC 認証バイパスの問題により失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。
PoE の問題		

MRE の問題		
カテゴリ	問題の名称	[Summary]
デバイス	PoE 受電デバイスに障害フラグあり	PoE ポートに接続された PoE 対応デバイスに障害があると Syslog イベントにフラグが付きました。



第 12 章

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

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。

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（279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（264 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 （265 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 （279 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 （266 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シスコ 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。

a) [Network Assurance Configuration] 領域で、[Service Status] トグルを [Enabled] に設定します。
b) [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

デバイスに設定を割り当て、それをインベントリに追加してワイヤレスデバイスを要求すると、プロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

（注） あるデバイスについてデバイスの可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加された、またはサイトに割り当てられたときに、追加の設定がデバイスにプッシュされます。詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください。

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。ネットワーク階層について （45 ページ）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。
- 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 で説明されています。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 メニューアイコン（☰）をクリックして、**[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。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレス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 デバイス表の上にあるメニューバーで、**[Actions]** > **[Claim]** の順に選択します。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスクレデンシャルの定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスクレデンシャルを定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 （任意） 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP（アクセスポイント）または ME（Mobility Express）を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、ワイヤレス LAN コントローラやセンサーデバイスには表示されません。

ステップ 7 [サイトの選択（Select a Site）] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。アクセスポイントデバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[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。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 **[Next]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 9 （任意）テーブルに表示される列を変更するには、テーブル見出しの右端にある3つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意）[デバイス名（Device Name）] フィールドで、必要に応じてデバイス名を変更します。
c) アクセスポイントデバイスの場合、[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。
d) 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。[Management IP]、[Subnet Mask]、[Gateway]、[IP Interface Name]、また任意で [VLAN ID]。
e) 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。
f) 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） ソフトウェアリリース 1.3.1.2 よりも古い Cisco Aironet 1800s アクティブセンサの場合は、センサ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。

g) 変更した場合は、[保存（Save）] をクリックします。それ以外の場合は、[キャンセル（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。
h) **[アクション（Actions）]** 列の **[他のデバイスに...を適用（Apply … to Other Devices）]** をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 デバイスが Cisco Catalyst 9800-CL ワイヤレスコントローラの場合は、[Configuration] 列の [Image] の横にある [Assign] をクリックし、次の手順を実行します。

a) （オプション）[イメージ（Image）] 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。
b) **[保存（Save）]** をクリックします。

ステップ 12 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスに**[割り当て（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。

ステップ 13 **[Next]** をクリックします。
[概要（Summary）] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 14 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 [Day-0 Config] 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)] オプションボタンをクリックし、[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LAN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 15 [要求（Claim）] をクリックします。
確認のダイアログボックスが表示されます。

ステップ 16 **[はい（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。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUSおよびTACACS Cisco DNA Centerの AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

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。

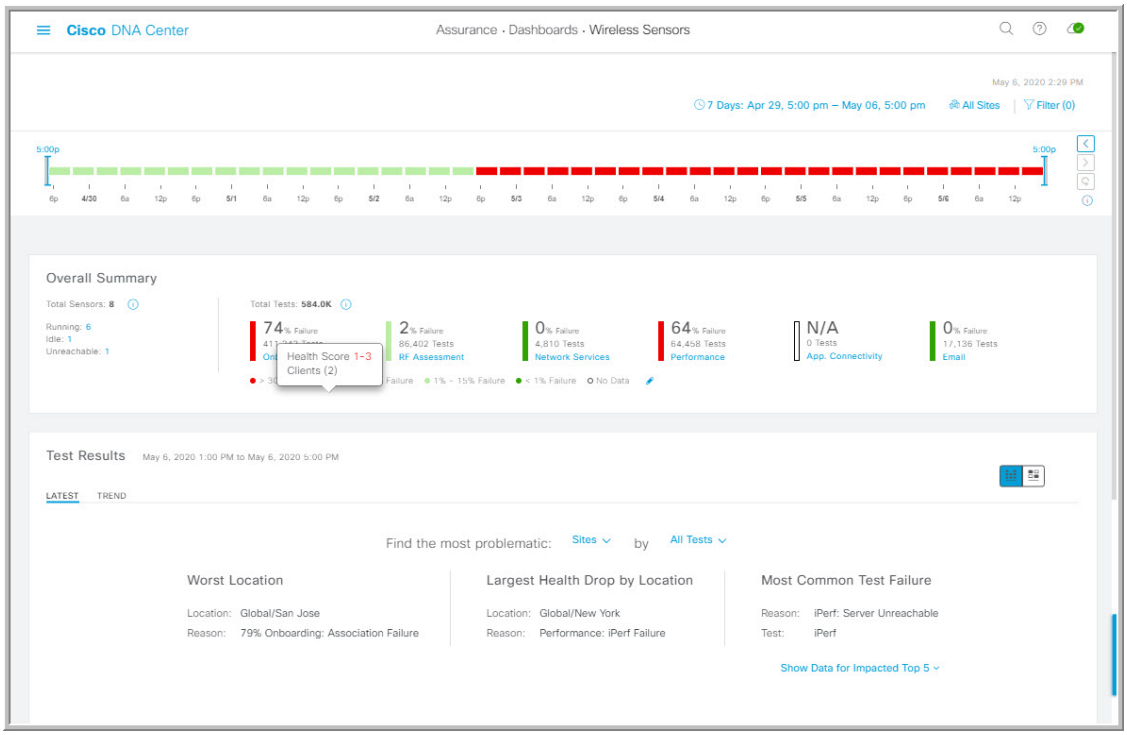
始める前に

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 （283 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboards]** > **[Wireless Sensors]** の順に選択します。

[Wireless Sensors] ダッシュボードが表示されます。

図 *27 : [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。 1. 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。 2. [Start Date] と時刻、[End Date] と時刻を指定します。 3. [Apply] をクリックします。
階層ロケーションの設定	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。 （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。

タイムラインエリア	
アイテム	説明
[Filter] アイコン	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。 フィルタを追加するには、次の手順を実行します。 **1.** [Filter] をクリックします。 **2.** 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。 **3.** 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。 **4.** [Apply] をクリックします。 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。 **1.** [Filter] アイコンをクリックします。 **2.** [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。

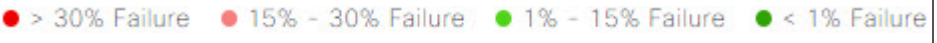
- 時間範囲が [3 Hours] の場合、各ブロックは 15 分を表します。
- 時間範囲が [24 Hours] の場合、各ブロックは 30 分を表します。
- 時間範囲が [7 Days] の場合、各ブロックは 4 時間を表します。

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 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	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。 • [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。 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。 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（275ページ）」を参照してください。

[Overall Health Summary] ダッシュレット	
アイテム	説明
全体テスト	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。 [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** 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。 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。 • 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。 （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。 • 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。 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。
 しきい値の編集	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。  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。 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	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。 • [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	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。 デフォルトでは、[Heatmap View] が表示されます。
 [Heatmap View]	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。 • [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。 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。 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。 • 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たます。

[Test Results] ダッシュレット	
アイテム	説明
[Card View]	カード形式でデータが表示され、高レベルのモニターリングと比較が可能です。 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。

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 メニューアイコン（☰）をクリックして、**[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

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。
• 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。
  • [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。

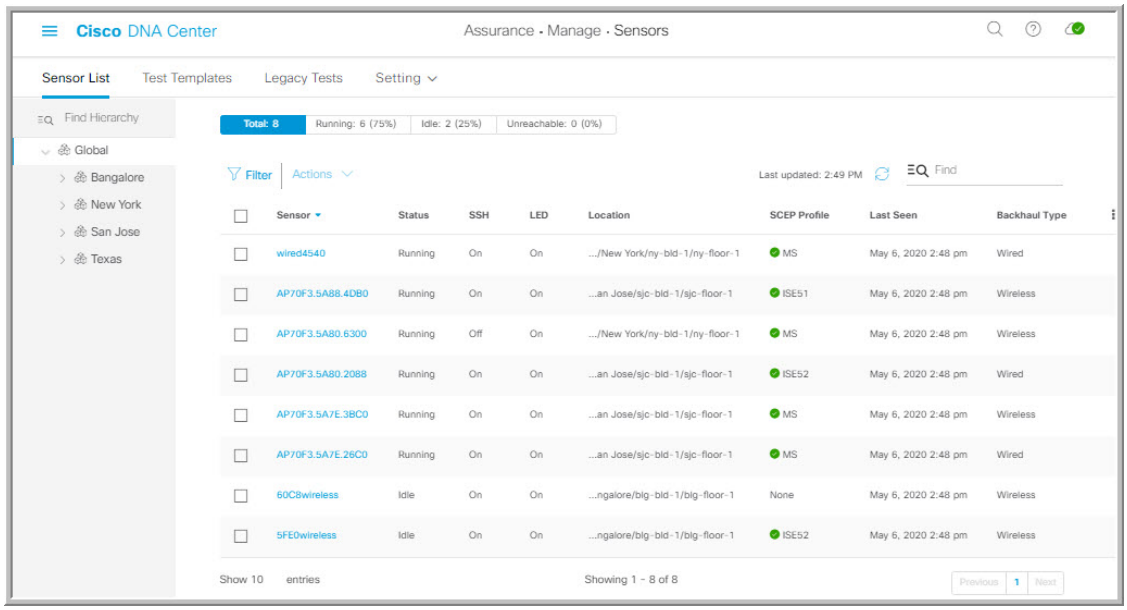
始める前に

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　メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[Sensors]** の順に選択します。

[Sensor List] ウィンドウが表示されます。

図 *28 : [Sensor List]* ウィンドウ



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す。

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。

a) をクリックします。
b) 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。
c) [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。

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。

c) [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。
d) [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。
e) [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。

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 （281 ページ） を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[Sensors]** の順に選択します。

結果：[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 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[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

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

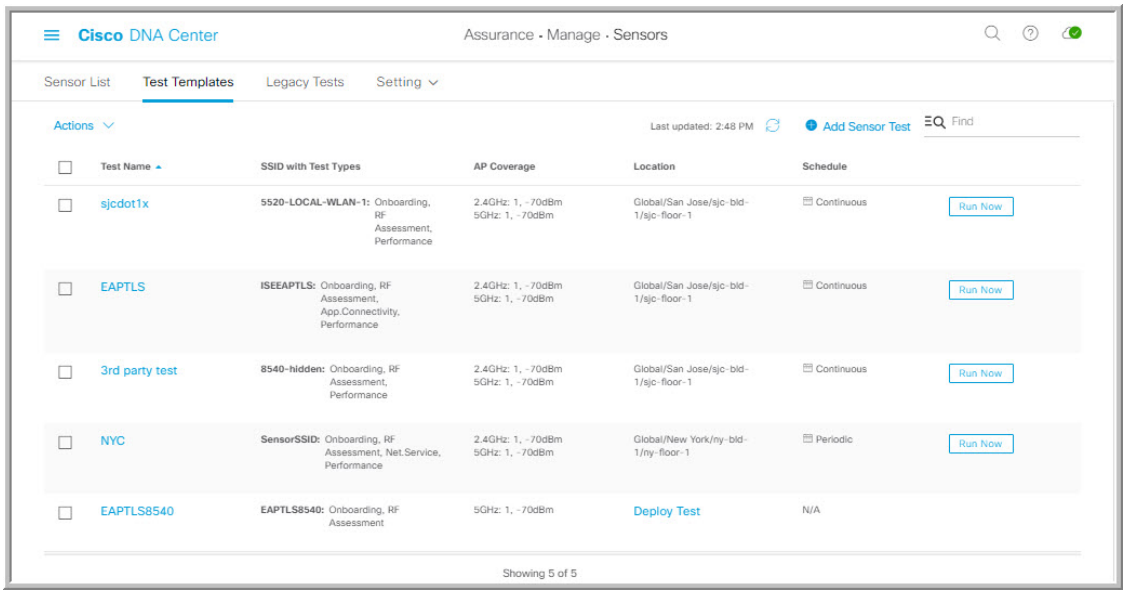
- Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[Inventory] で表示されるようにしてください。ワイヤレス Cisco Aironet 1800s アクティブ センサーのプロビジョニング（263 ページ）を参照してください。
- センサーテストテンプレートを再起動すると、そのテンプレート上のすべてのセンサーで同時にテストの実行が開始されるため、結果のグラフに周期的なパターンが現れることに注意してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[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 *29 : [Test Templates]* ウィンドウ



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 サプ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 NTD 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 Reachabilit]：（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 カバレージの選択**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

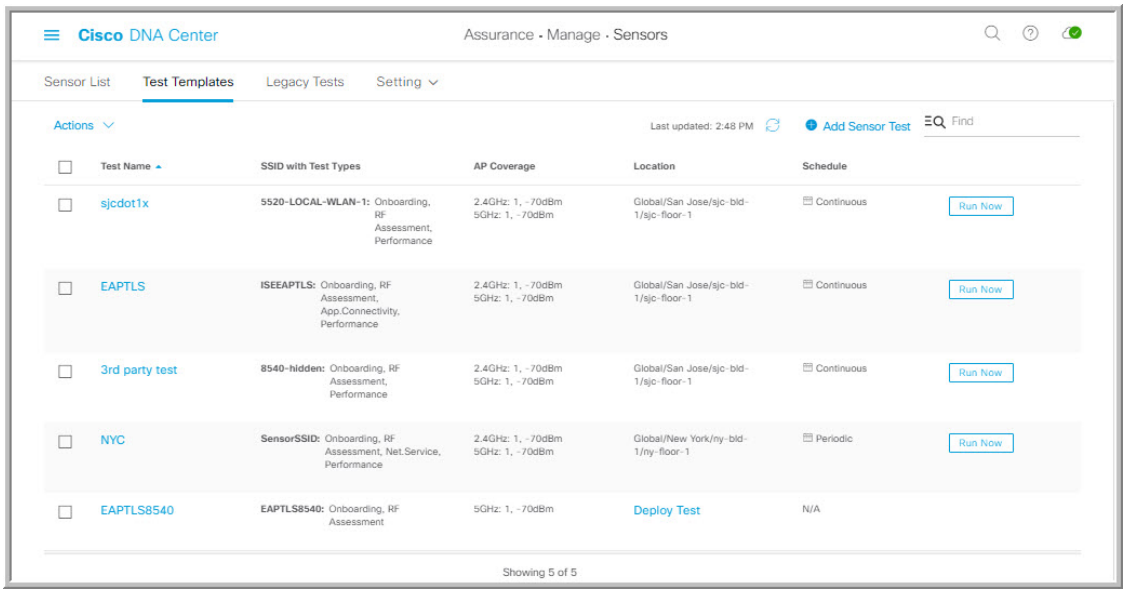
センサー主導テストのテンプレートを作成します。テンプレートを使用したセンサー主導テストの作成と実行 （283 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Manage]** > **[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 *30 : [Test Templates]* ウィンドウ



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。

a) 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。

b) **[Actions]** > **[Duplicate]** の順に選択します。

c) [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。

d) [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。

a) 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。

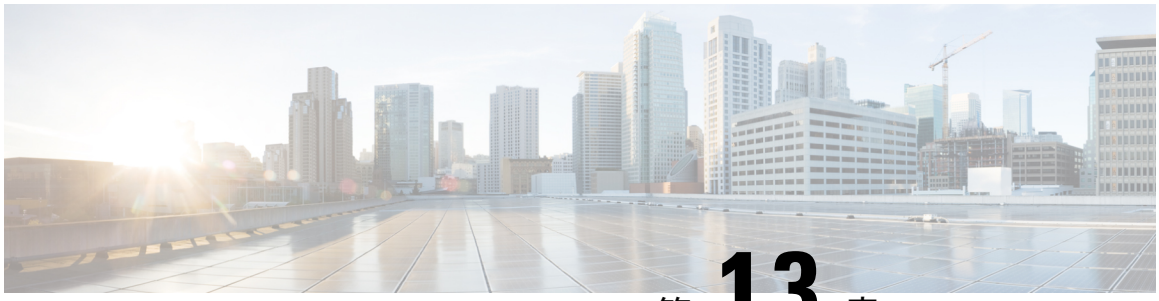
b) **[Actions]** > **[Delete]** の順に選択します。

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。



第 13 章

Wi-Fi 6 対応状況の監視

Wi-Fi 6 対応状況とその利点について

Wi-Fi 6 対応状況機能を使用すると、次のことを判断できます。

- Wi-Fi 6 対応クライアントの割合。
- Wi-Fi 6 対応の AP インフラストラクチャの割合。
- 上記の情報に基づいて、Wi-Fi 6 ネットワークのメリットを最大限に活用するためのアクションに関する推奨事項が提供されます。

このような推奨事項を提供するために、Cisco DNA Center は次のことを行います。

- ワイヤレスクライアントの Wi-Fi 機能を評価します。
- AP インベントリを収集して、Cisco DNA Center によって管理されている AP を特定し、AP の Wi-Fi 機能を評価します。
- ネットワーク内にあるワイヤレスコントローラのタイプと、ワイヤレスコントローラにインストールされているソフトウェアが Wi-Fi 6 に対応しているかを判別します。
- 無線 LAN の設定と、Wi-Fi 6 機能が無効になっているかを判断します。

Wi-Fi 6 ネットワークの対応状況とその利点について

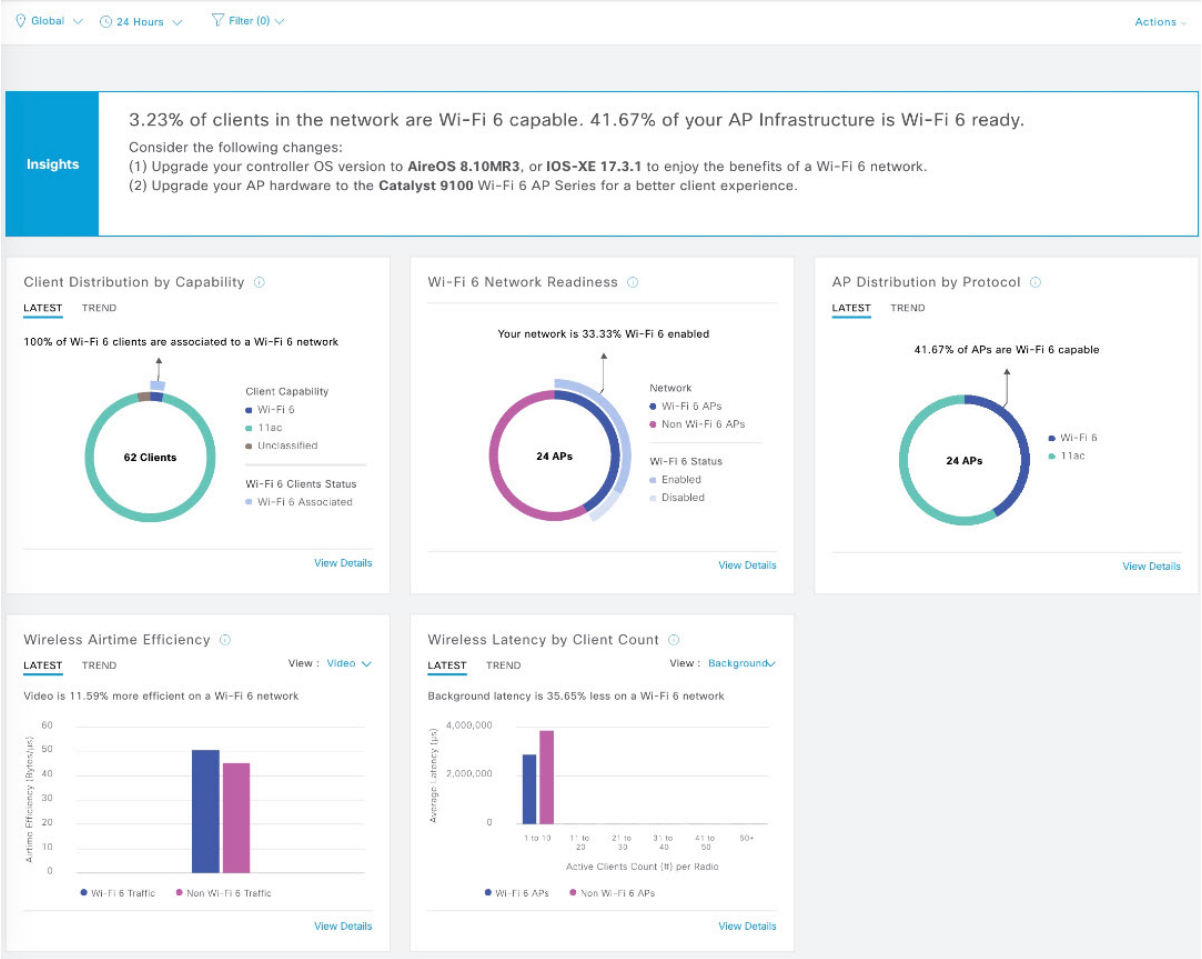
Wi-Fi 6 ネットワークの対応状況とその利点を確認するには、この手順を使用します。

始める前に

アシュアランスを設定します。「基本的な設定のワークフロー （17 ページ）」を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして、[Wi-Fi 6]**アシュアランス** > を選択します。

[Wi-Fi 6] ダッシュボードが表示されます。



ステップ 2 次の機能には、上部のメニューバーを使用します。

アイテム	説明
 [Location] ペイン	クリックすると、次のアイコンが表示されます。 •  ：[Hierarchical Site View] テーブルを表示するには、このトグルボタンをクリックします。サイト内のワイヤレスクライアントとワイヤレス ネットワーク デバイスの割合を示します。特定の建物の情報を表示するには、ドロップダウンリストから [Building View] を選択します。 •  ：このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、提示されるネットワーク サイトは問題の重大度に従って色分けされています。
 **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。 **1.** 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。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。
[Filter] アイコン	[SSID] および [Band] オプションが含まれます。ドロップダウンリストから SSID と帯域周波数の隣にあるチェックボックスをオンにして選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。
[Actions] ドロップダウン リスト	ドロップダウンリストから [Edit Dashboards] を選択すると、ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ）およびカスタム ダッシュボードの作成 （313 ページ）を参照してください。

ステップ 3 ネットワークに関する情報を取得するには、[Insights] 領域を使用します。次の情報を出力します。

- Wi-Fi6 対応クライアントの割合。
- Wi-Fi6 対応の AP インフラストラクチャの割合。
- 上記の情報に基づいて、Wi-Fi 6 ネットワークのメリットを最大限に活用するために実行できるアクションについての推奨事項が提供されます。

ステップ 4 [Client Distribution By Capability] ダッシュレットを使用して、クライアントのプロトコル機能を確認し、Wi-Fi 6 対応クライアントが Wi-Fi 6 ネットワークに参加しているかどうかを確認します。

クライアントが関連付けられている AP に基づいて、クライアントは Wi-Fi 6 機能で動作する場合もあれば、それより低い機能で動作することもあります。たとえば、11ac AP に関連付けられた Wi-Fi 6 クライアントは、11ac クライアントとして機能します。

[Client Distribution By Capability] ダッシュレット
このダッシュレットには、ワイヤレスネットワークに関連付けられているすべてのクライアントが表示されます。次の 2 つのタブがあります。 • [Latest]：デフォルトで表示されます。 円の**外側**のセグメントは、Wi-Fi 6 ネットワークに参加している（関連付けられている）Wi-Fi 6 対応クライアントの数を示します。 **内側**の円は、ネットワーク内のさまざまなクライアントのプロトコル機能を示します。ワイヤレスクライアントは、次のいずれかのプロトコルで機能します。 • **Wi-Fi 6**：802.11ax 対応クライアント。 • **11ac**：802.11ac Wave1 および Wave2 対応クライアント。 • **11n**：802.11n 対応クライアント。 • **11abg**：802.11a、b、または g 対応クライアント。 • [Unclassified]：次の理由で [Unclassified] に一覧表示されるクライアントがあります。 • ネットワーク遅延のため、クライアントデバイスの機能が報告されません。 • クライアントデバイスが接続されている AP またはワイヤレスコントローラに、正しいソフトウェアバージョンがインストールされていません。 チャートのいずれかの色にカーソルを重ねると、その色に関連付けられたクライアントの数が表示されます。 • [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、一定の時間範囲で Wi-Fi 6 プロトコルまたは非 Wi-Fi 6 プロトコルに関連付けられているクライアントの数を示します。 チャートにカーソルを重ねると、クライアントの合計数と指定された日時におけるクライアントのプロトコルが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 5 [Wi-Fi 6 Network Readiness] ダッシュレットを使用して、Wi-Fi 6 に対応し、Wi-Fi 6 モードで動作するように設定（有効化）されている AP の数を確認します。

[Wi-Fi 6 Network Readiness] ダッシュレット
このダッシュレットには、ネットワーク内の AP に関する 2 つのレベルの詳細情報が表示されます。 • 円の**外側**のセグメントは、Wi-Fi 6（11ax）が有効になっている Wi-Fi 6 AP の数と、Wi-Fi 6 が無効になっている Wi-Fi 6 AP の数を示します。 （注） AP の無線のうち 1 つのみで Wi-Fi 6 が有効になっている場合でも、その AP は Wi-Fi 6 モードで動作中と表示されます。 • **内側**の円は、Wi-Fi 6（11ax）AP の数と非 Wi-Fi 6（11ac、11n、および 11abg）AP の数を示します。 （注） Wi-Fi6 AP は、次の条件に従って Wi-Fi 6 モードで動作できます。 • Wi-Fi6 AP で 11ax 設定が有効になっている。 • ワイヤレスコントローラと AP が Wi-Fi 6（11ax）をサポートするソフトウェアバージョンを実行している。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色セグメントをクリックすると、[AP] タブと [WLC] タブが表示されます。[AP] タブと [WLC] タブをクリックすると、無線レベルと帯域レベルでの Wi-Fi 6 対応がそれぞれ表示されます。

ステップ 6 [AP Distribution by Protocol] ダッシュレットを使用して、ワイヤレスプロトコル（802.11ax、11ac、n、またはレガシー）をサポートするハードウェア機能を持つ AP の数を確認します。

[AP Distribution by Protocol] ダッシュレット
このダッシュレットには 2 つのタブがあります。 • [Latest]：デフォルトで表示されます。Wi-Fi 6（11ax）プロトコルをサポートする AP の数と、非 Wi-Fi 6（11ac、n、またはレガシー）プロトコルをサポートする AP の数を示します。 • [Wi-Fi 6]：802.11ax 対応 AP。 • [11ac]：802.11ac 対応 AP。 • [11n]：802.11n 対応 AP。 • [11abg]：802.11a、b、または g 対応 AP。 チャートのいずれかの色にカーソルを重ねると、その色に関連付けられた AP の数が表示されます。 • [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、一定の時間範囲でさまざまなプロトコル（Wi-Fi 6 または非 Wi-Fi 6）に関連付けられている AP の数を示します。 チャートにカーソルを重ねると、AP の合計数と指定された日時における AP のプロトコルが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

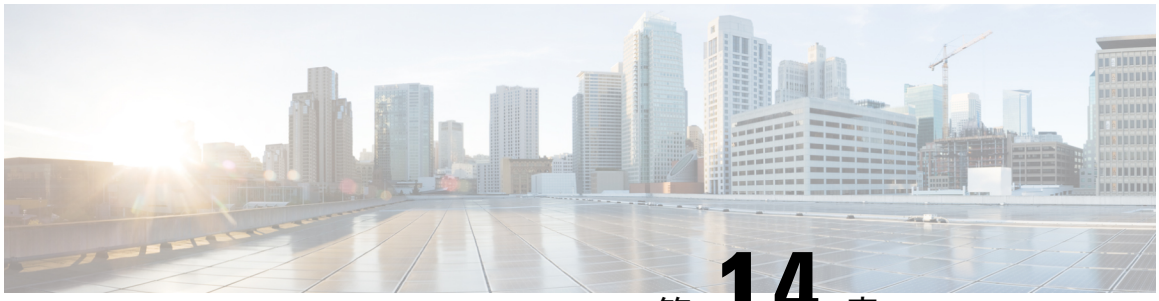
ステップ 7 [Wireless Airtime Efficiency] ダッシュレットを使用して、アクセスカテゴリ（音声、ビデオ、ベストエフォート、バックグラウンド）ごとに、Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均通信時間効率を比較します。

[Wireless Airtime Efficiency] ダッシュレット
[Voice]、[Video]、[Best Effort]、[Background]、および [All] のアクセスカテゴリに従って、ワイヤレス通信時間効率を表示できます。デフォルトは [Voice] です。 このダッシュレットには 2 つのタブがあります。 • [Latest]：デフォルトで表示されます。棒グラフでは、選択したアクセスカテゴリにおける Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均通信時間効率（1 ミリ秒あたりのバイト数）を比較できます。 AP の無線が、類似した RF 状態の他のネットワークよりも少ない通信時間（マイクロ秒）でより多くのトラフィック（クライアントに送信されるバイト数）を送信できる場合は、スペクトルが効率的に使用されています。効率的なネットワークでは、より多くのビデオまたは音声コールを処理できる可能性があります。 トラフィックは次のように分類されます。 • Wi-Fi 6 トラフィックは、Wi-Fi 6 の AP から Wi-Fi 6 として関連付けられているクライアントに送信されるトラフィックです。 • 非 Wi-Fi 6 トラフィックは以下を集約したものです。 • Wi-Fi 6 AP から非 Wi-Fi 6 対応クライアントへのトラフィック。 • 非 Wi-Fi 6 AP から非 Wi-Fi 6 対応クライアントへのトラフィック。 • 非 Wi-Fi 6 AP から Wi-Fi 6 対応クライアントへのトラフィック。 （注） Wi-Fi 6 対応クライアントは、非 Wi-Fi 6 AP に接続すると非 Wi-Fi 6 モードで動作します。 • [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、一定の時間範囲でさまざまなワイヤレス ネットワーク モード（Wi-Fi 6 または非 Wi-Fi 6）に関連付けられているクライアントの数を示します。 チャートにカーソルを重ねると、クライアントの合計数と指定された日時におけるクライアントのプロトコルが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 8 [Wireless Latency by Client Count] ダッシュレットを使用して、アクセスカテゴリ（音声、ビデオ、ベストエフォート、バックグラウンド）ごとに、Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均ワイヤレス遅延を比較します。

クライアント数が多い AP 無線は、通常、類似した RF 条件下のクライアント数が少ない無線と比べて遅延が多くなります。

[Wireless Latency by Client Count] ダッシュレット
[Voice]、[Video]、[Best Effort]、[Background] トラフィックのワイヤレス遅延を表示できます。デフォルトは [Voice] です。 このダッシュレットには 2 つのタブがあります。 • [Latest]：デフォルトで表示されます。同様の数の「アクティブな」クライアントに対応する Wi-Fi 6 無線と非 Wi-Fi 6 AP 無線間の平均ワイヤレス遅延を比較できます。ワイヤレス遅延は、パケットが AP からクライアントに正常に送信されるまでにかかる時間（マイクロ秒）で測定されます。 （注） アクティブクライアントには、Wi-Fi 6 AP に関連付けられ、特定のアクセスカテゴリのトラフィックをアクティブに送信しているクライアントが含まれます。 • [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。トレンドチャートには、すべてのアクセスカテゴリの平均ワイヤレス遅延が表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



第 14 章

Power over Ethernet の監視

PoE について

Cisco DNA Center Power over Ethernet（PoE）を使用してネットワーク内の PoE 対応デバイスをモニターできます。また、PoEを供給するスイッチの電源の概要がモニターされ、スイッチの電力バジェット、使用済み電力、残り電力、電力使用状況などの情報が提供されるため、スイッチの割り当て済み電力と電力負荷を表示できます。

PoE テレメトリの設定ワークフロー

アシュアランス で PoE テレメトリと分析を有効にするには、必要な設定タスクを実行する必要があります。基本的な設定ワークフローのタスクは次のとおりです。

1. PoE テレメトリに使用するネットワークデバイスで NETCONF を設定します。

   詳細については、「PoE テレメトリに使用するネットワークデバイスでの NETCONF の設定 （301 ページ）」を参照してください。

2. Cisco DNA Center でテレメトリ設定を更新します。

   詳細については、「PoE テレメトリのテレメトリ設定の更新 （303 ページ）」を参照してください。

設定ワークフロー

PoE テレメトリの設定ワークフローは、Cisco DNA Center のソフトウェアバージョンと設定、および PoE テレメトリをサポートするネットワークデバイスによって異なります。

Cisco DNA Center の新規インストールの場合は、次の表を参照してください。

Cisco DNA Center の新規インストール	
ネットワーク デバイス設定	必要な設定タスク
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Cisco DNA Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Cisco DNA Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が有効になっている。	1. Cisco DNA Center でテレメトリ設定を更新します。

以前のリリースから Cisco DNA Center にアップグレードする場合は、次の表を参照してください。

以前のリリースからのアップグレード	
ネットワーク デバイス設定	必要な設定タスク
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Cisco DNA Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が有効になっている。	1. Cisco DNA Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Cisco DNA Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が有効になっている。	1. Cisco DNA Center でテレメトリ設定を更新します。

PoEテレメトリをサポートするネットワークデバイスのインベントリに変更がある場合は、次の表を参照してください。

ネットワークデバイスのインベントリの変更	
ネットワークデバイスの変更	**必要な設定タスク**
インベントリからデバイスを削除して再度追加する。Cisco DNA Center	**1.** デバイスで NETCONF を有効にします。 **2.** Cisco DNA Center でテレメトリ設定を更新します。
インベントリに新しいデバイスを追加する。Cisco DNA Center	**1.** デバイスで NETCONF を有効にします。 **2.** Cisco DNA Center でテレメトリ設定を更新します。
インベントリの交換用デバイスを使用する。Cisco DNA Center	**1.** デバイスで NETCONF を有効にします。 **2.** Cisco DNA Center でテレメトリ設定を更新します。

PoE テレメトリに使用するネットワークデバイスでの NETCONF の設定

この手順では、PoE テレメトリに使用するネットワークデバイスで NETCONF を設定する方法を示します。PoE テレメトリを使用するには、サポートするネットワークデバイスで NETCONF が有効になっている必要があります。

始める前に

Cisco DNA Center とネットワークデバイスの設定によっては、PoE テレメトリを設定するためにこの手順を実行する必要がない場合もあります。詳細については、「PoE テレメトリの設定ワークフロー （299 ページ）」を参照してください。

ステップ 1 既存のネットワークデバイスの NETCONF ポートを設定します。

a) Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

b) NETCONF が有効になるように設定するネットワークデバイスのチェックボックスをオンにします。

c) **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

d) [Type] ドロップダウン リストから、[Network Device] を選択します。

e) [NETCONF] 領域を展開します。

f) [Port] フィールドに、「**830**」と入力します。

（注） NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。

g) [Update] をクリックします。

デバイスの NETCONF ポートが設定されます。

ステップ 2 [Template Editor] で NETCONF 設定のプロジェクトを作成します。

a) [Menu] アイコン（☰）をクリックし、**[Tools]** > **[Template Editor]** の順に選択します。

[Template Editor] ウィンドウが表示されます。

b) 左ペインで ⊕ アイコンをクリックし、[Create Project] を選択します。

c) [Name] フィールドに、プロジェクトの名前を入力します。

d) [Add] をクリックします。

プロジェクトが [Template Editor] の左ペインに追加されます。

ステップ 3 NETCONF 設定のプロジェクトでテンプレートを作成します。

a) 左ペインで、プロジェクトの右にある ⚙ アイコンにカーソルを合わせ、[Add Template] を選択します。

b) [Name] フィールドに、テンプレートの名前を入力します。

c) [Device Type（s）] フィールドで、[Edit] をクリックします。

d) スイッチとハブを追加するには、[Switches and Hubs] のチェックボックスをオンにしてテンプレートを適用します。

（注） スイッチの正確なモデルを指定する場合は、[Switches and Hubs] を展開し、特定のスイッチモデルのチェックボックスをオンにします。

e) [Back to Add New Template] をクリックします。

f) [Software Type] ドロップダウンリストをクリックし、[IOS-XE] を選択します。

g) [Add] をクリックします。

テンプレートが作成されて表示されます。

ステップ 4 テンプレートの内容を追加します。

a) テンプレートで次のように入力します。

```
netconf-yang
```

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

テンプレートの内容が保存されます。

c) [Actions] ドロップダウンリストから、[Commit] を選択します。

d) [Commit Note] テキストボックスに、メモを入力します。

e) [Commit] をクリックします。

ステップ 5 ネットワークプロファイルを作成してテンプレートを関連付けます。

a) [Menu] アイコン（☰）をクリックし、**[Design]** > **[Network Profile**） **]** の順に選択します。

[Network Profiles] ウィンドウが表示されます。

b) [+Add Profile] をクリックし、[Switching] を選択します。
c) [Profile Name] フィールドに、ネットワークプロファイルの名前を入力します。
d) [Day-N Templates] タブをクリックします。
e) [Add] をクリックします。
f) [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。
g) [Template] ドロップダウンリストから、手順 3 で作成したテンプレートを選択します。
h) [Save] をクリックします。

ネットワークプロファイルが作成され、[Network Profiles] ウィンドウに表示されます。

ステップ 6 ネットワークプロファイルのサイトを割り当てます。

a) [Sites] 列で、[Assign Site] をクリックします。
b) ネットワークデバイスが割り当てられているサイトのチェックボックスをオンにします。
c) [Save] をクリックします。

ステップ 7 NETCONF 設定をネットワークデバイスにプロビジョニングします。

a) [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

b) PoE テレメトリのネットワークデバイスのチェックボックスをオンにします。
c) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。
d) [Assign Site] ステップで、[Next] をクリックします。
e) [Advanced Configuration] ステップで、[Provision these templates even if they have been deploy before] チェックボックスをオンにします。
f) [Next] をクリックします。
g) [Summary] ステップで、[Deploy] をクリックします。
h) [Apply] をクリックします。

プロビジョニングが開始され、NETCONF 設定がネットワークデバイスにプッシュされます。

PoE テレメトリのテレメトリ設定の更新

この手順では、Cisco DNA Center でテレメトリ設定を更新する方法を示します。これは、NETCONF ポートを設定し、PoE テレメトリに使用するネットワークデバイスに NETCONF 設定をプッシュした後に必要な手順です。

始める前に

PoEテレメトリ用に設定するネットワークデバイスでNETCONFポートが確立され、NETCONFが適切に設定されていることを確認します。詳細については、「PoE テレメトリに使用するネットワークデバイスでの NETCONF の設定 （301 ページ）」を参照してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

ステップ 2 PoE テレメトリ用に設定されているネットワークデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Telemetry]** > **[Update Telemetry Settings]** の順に選択します。

ステップ 4 [Force Configuration Push] チェックボックスをオンにします。

（注） このオプションを選択すると、設定の変更がデバイスにプッシュされます。

ステップ 5 [Next] をクリックします。

ステップ 6 次のオプションボタンをクリックして、テレメトリ設定を更新するスケジュールを設定します。

- [Now]：テレメトリ設定をすぐに更新するには、このオプションを選択します。
- [Later]：テレメトリ設定を後で更新するようにタスクをスケジュールするには、このオプションを選択します。日付と時刻を指定します。

ステップ 7 [Apply] をクリックします。

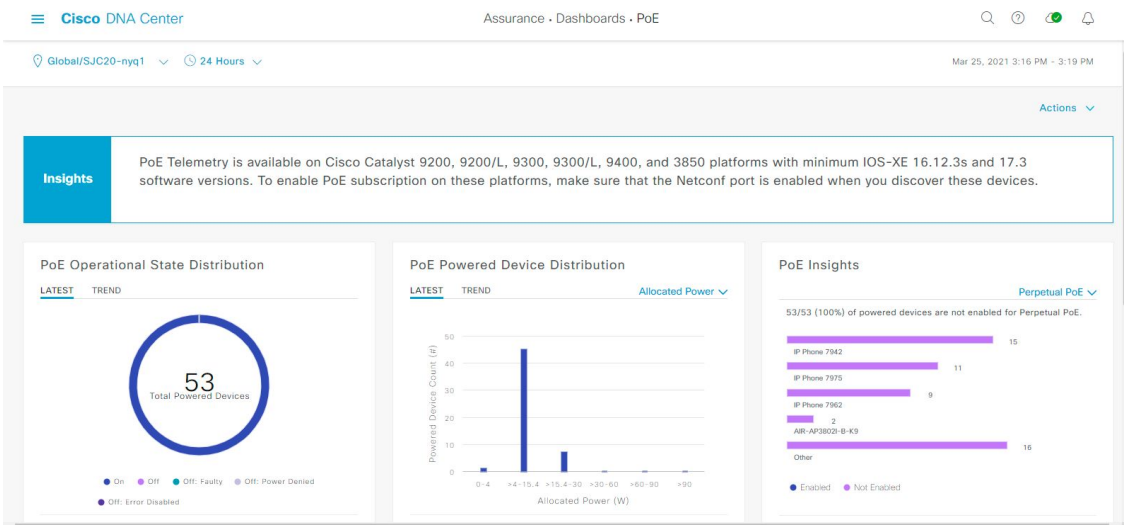
ネットワーク内の PoE 対応デバイスの監視

ネットワーク内のPoE対応デバイスのグローバルビューを取得するには、次の手順を使用します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[PoE]** の順に選択します。

[PoE] ダッシュボードが表示されます。

図 *31 : [PoE]* ダッシュボード



ステップ 2 上部のメニューバーにあるロケーションオプション（ Global ）をクリックして、ロケーションペインを表示します。

ロケーションペインには、次の機能があります。

ロケーションオプション	
アイテム	**説明**
トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。 ドロップダウンリストをクリックして、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。 [Apply to Page Location] 列で特定のサイトまたはビルディングの [Apply] をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [Building View]：リストをビルディングレベルで並べ替えます。 [Apply to Page Location] 列で特定のビルディングの [Apply] をクリックすると、そのビルディングのデータのみが [Network] ダッシュボードに表示されます。
トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、提示されるネットワークサイトは問題の重大度に従って色分けされています。

ロケーションオプション	
アイテム	説明
 [Topology]ツール	このアイコンをクリックすると、[Topology]ツールが開きます[Topology] ウィンドウには次のビューがあります。 • [Geographical View]：このトグルボタンをクリックすると、ネットワークが地理的マップで表示されます。  ロケーションにカーソルを合わせると、正常なデバイスの割合が表示されます。 •  [Topology View]：このトグルボタンをクリックすると、ネットワークにおけるコンポーネントの接続状況を示すトポロジが表示されます。 デバイスにカーソルを重ねると、デバイスロール、IP アドレス、ソフトウェアバージョンなどのデバイス情報が表示されます。デバイスの 360 度ビューを取得するには、[View Details 360] をクリックします。

ステップ 3 上部のメニューバーにある時間範囲設定（  ）をクリックして、ダッシュボード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) [Start Date] と時刻、[End Date] と時刻を指定します。
c) [Apply] をクリックします。

ステップ 4 上部のメニューバーにある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- [Export Dashboard]：PoE ダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （317 ページ） およびカスタム ダッシュボードの作成 （313 ページ） を参照してください。

ステップ 5 次の機能には、PoE ダッシュレットを使用します。

PoE AP 電力モード供給ダッシュレット

完全に電力が供給されている AP と部分的に電力が供給されている AP の分布が表示されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

PoE 動作状態の分布ダッシュレット

ネットワーク内の PoE 対応デバイスの数が表示されます。PoE で供給されているかどうかに基づいて、色分けされたチャートでデバイスの数が示されます。PoE で供給していないデバイスについては、その理由に応じてさらに分類されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

PoE 受電デバイスの分布ダッシュレット
現在 PoE を使用しているデバイスのうち、特定の基準に当てはまるデバイスの割合が表示されます。ドロップドロップリストを使用して、次の基準を指定します。 • 割り当て済み電力 • 受電デバイスクラス [Latest] タブには、10 分間のスナップショットビューが表示されます。 [Trend] タブには、次の情報が表示されます。 • 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。 • 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 （注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

電力負荷分散の分布ダッシュレット

PoE の電力負荷に基づくスイッチの割合が表示されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

PoE インサイトダッシュレット

現在 PoE を使用しているデバイスのうち、次の PoE テクノロジーをサポートするように設定されているデバイスや IEEE に準拠しているデバイスの割合が表示されます。

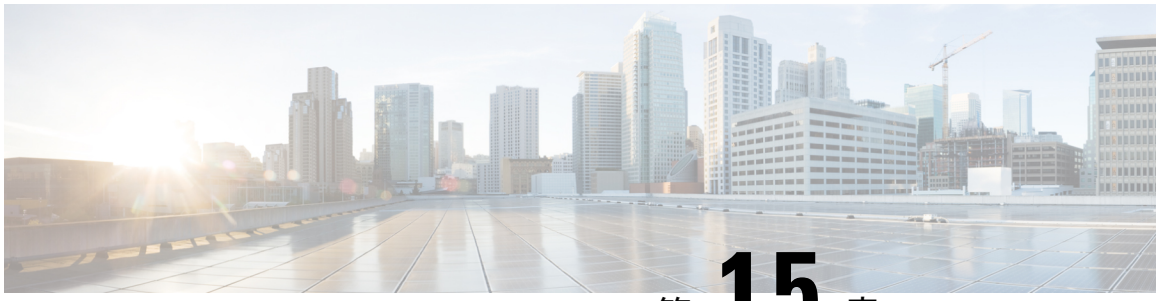
- **無停止型 POE**
- **高速 PoE**
- **IEEE 準拠**
- **UPOE+**

ドロップダウンリストを使用して、特性を選択します。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下のテーブルに表示されるデータを更新できます。

PoE 電力使用量ダッシュレット
現在 PoE を使用しているデバイスの合計電力使用量が表示されます。 [Latest] タブには、10 分間のスナップショットビューが表示されます。円グラフには、合計電力使用量の [Consumed Power] と [Remaining Power] がワット単位で表示されます。 [Trend] タブには、次の情報が表示されます。 • 時間範囲の設定で 24 時間を選択した場合、トレンドチャートには電力使用の 24 時間の範囲全体で 10 分のデータポイントが表示されます。 • 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、一定期間におけるデバイスの電力使用量の状況を表示できます。 水平バーとして表示されるデータを選択して、電力使用量、デバイスロール、および場所に基づいて進行中のテーブルをフィルタ処理できます。

PoE ポートの可用性ダッシュレット
PoE の電力負荷に基づいてポートの可用性が表示されます。 [Latest] タブには、10 分間のスナップショットビューが表示されます。 [Trend] タブには、次の情報が表示されます。 • 時間範囲の設定で 24 時間以下の時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 • 時間範囲の設定で 7 日間を選択した場合、トレンドチャートには、時間範囲全体に対して 12 時間のデータポイント（1 時間のデータから集約）が表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの1時間のデータポイントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



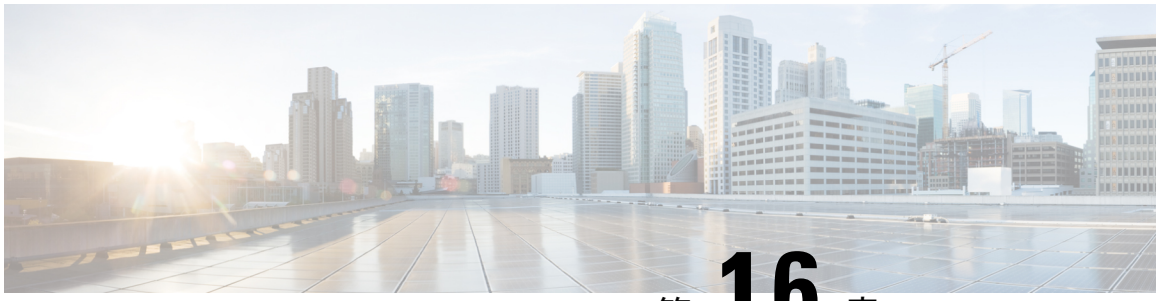
第 15 章

不正管理ダッシュボードの監視

ネットワークのセキュリティ脅威の管理

Cisco DNA Center の不正管理アプリケーションを使用すると、不正アクセスポイントからのネットワーク上の脅威をモニターできます。最も優先度の高い脅威を迅速に特定し、アシュアランス ダッシュボードからそうした脅威をモニターできます。

Cisco DNA Center の不正管理アプリケーションの詳細については、『Cisco DNA Center Rogue Management Application Quick Start Guide [英語]』を参照してください。



第 16 章

Manage Dashboards

ダッシュボードについて

ネットワーク監視用のカスタムダッシュボードを作成できます。ダッシュボードには、1 つまたは複数のダッシュレット（チャート、表、地理マップなどの情報）で構成されます。

カスタムダッシュボードは、それを作成したユーザーアカウントにのみ表示されます。作成者であるユーザー以外のユーザーには表示されません。

カスタム ダッシュボードの作成

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。

ステップ 2 [+ Create a Dashboard] をクリックします。

ステップ 3 **[Create a Dashboard]** ダイアログ ボックスで、ダッシュボードのタイトルを入力します。

ステップ 4 [Save] をクリックします。
空白のダッシュボードが表示されます。

ステップ 5 ダッシュボードでは、次の操作を実行できます。

a) [+ Add a Dashlet] をクリックして、このダッシュボードに内容を追加します。

b) ダッシュボードに追加するダッシュレットの横にあるチェックボックスをオンにします。

（注） ドロップダウンリストからカテゴリを選択するか、右側にある検索ボックスを使用して、ダッシュレットを検索します。

c) [Add] をクリックしてダッシュレットをダッシュボードに追加します。

ステップ 6 （任意）ダッシュレットをドラッグアンドドロップすると、ダッシュボード上でのダッシュレットの場所を変更できます。

ステップ 7 ダッシュボードからダッシュレットを削除するには、次の手順を実行します。

a) ダッシュレットの右上隅にあるゴミ箱アイコンをクリックします。

b) ダイアログボックスで、[Delete] をクリックします。

ステップ 8 [Save] をクリックしてダッシュボードを保存します。

テンプレートからのダッシュボードの作成

テンプレートからダッシュボードを作成すると、範囲を使用してダッシュボードデータをフィルタ処理できます。範囲は、場所、デバイスタイプ、およびその他のオプションでデバイスをフィルタ処理します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、すべての定義されたダッシュボードとテンプレートを（下に）リスト表示します。

ステップ 2 [Templates] エリアで、ダッシュボードテンプレートをクリックします。

ステップ 3 **[Create a Dashboard]** ダイアログ ボックスで、ダッシュボードのタイトルを入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 既存の範囲を使用する場合は、既存の範囲を選択して [Select Scope] をクリックします。

既存の範囲を選択した場合は、手順 ステップ 15 に進みます。新しい範囲を作成する場合は次の手順を続けます。

ステップ 6 新しい範囲を作成する場合は、[Create New Scope] をクリックします。
最初のステップ [Create New Scope] が表示されます。

ステップ 7 範囲名を入力し、[Next] をクリックします。範囲名にスペースを入力すると、スペースは下線に変換されます。
2 番目のステップ [Select Location（s）] が表示されます。

ステップ 8 範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含まれる 1 つ以上の場所を選択します。

（注） 場所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。

ステップ 9 [Next] をクリックします。

3 番目のステップ [Select Filters] が表示されます。

ステップ 10 [Client Health] テンプレートを使用している場合は、次のフィルタを使用できます。

- [Client Type]：範囲の隣にあるチェックボックスをオンまたはオフにして有線またはワイヤレスを選択し、これらのタイプのデバイスを範囲に含めます。
- [SSID]：範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に SSID を含めます。検索フィールドに入力して SSID をフィルタリングします。このフィルタはワイヤレスデバイスにのみ適用されます。
- [Host Name]：範囲に含めるホスト名を入力します。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- [Device Type]：デバイスの OS の種類（iOS、Android など）を入力して範囲に含めます。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- [MAC Address]：範囲に含める MAC アドレスを入力します。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- [IP Address]：範囲に含める IP アドレスを入力します。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。

ステップ 11 [Network Health] テンプレートを使用している場合は、次のフィルタを使用できます。

- [Network Device Type]：範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含まれる 1 つ以上のデバイスタイプを選択します。検索フィールドに入力してデバイスをフィルタリングします。
- [Network OS]：範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含めるネットワークの OS バージョンを選択します。検索フィールドに入力してバージョンをフィルタリングします。
- [IP Address]：範囲に含める IP アドレスを入力します。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- [Host Name]：範囲に含めるホスト名を入力します。パーセント記号（%）をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。

ステップ 12 [Next] をクリックします。
4 番目のステップの [Preview] が表示されます。

ステップ 13 選択したフィルタに基づいて更新されるクライアントのダイナミックリストを有効または無効にするには、[Dynamic list] トグルをクリックします。

ステップ 14 [Save] をクリックして範囲を保存します。
確認のダイアログが表示されます。

ステップ 15 （任意） ダッシュレットをドラッグアンドドロップすると、ダッシュボード上でのダッシュレットの場所を変更できます。

ステップ 16 ダッシュボードからダッシュレットを削除するには、次の手順を実行します。

a) ダッシュレットの右上隅にあるゴミ箱アイコンをクリックします。
b) ダイアログボックスで、[Delete] をクリックします。

ステップ 17 [Save] をクリックしてダッシュボードを保存します。

（注）　新しい範囲の場合は、ダッシュボードにデータが表示されるまで最大 15 分かかります。

ダッシュボードの表示

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。**[Dashboard Library]** ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

（注）　ダッシュボードを [Date Modified] で並べ替えると、ダッシュボードに変更が加えられていない場合でも、ダッシュボードを最後に開いた日時で並べ替えられます。

ステップ 2 お気に入りとしてマークされているダッシュボードを表示するには、[Favorite Dashboards] タブをクリックします。

ステップ 3 表示するダッシュボードをクリックします。

ステップ 4 ダッシュボードのコントロールで、[Show] または [Hide] をクリックし、必要に応じてマップを表示または非表示にします。

ステップ 5 （任意）フィルタから適切な値を選択して、期間、サイト、またはドメイン別にダッシュボードデータをフィルタ処理します。

ダッシュボードの編集または削除

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。**[Dashboard Library]** ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 編集または削除するダッシュボードをクリックします。

ステップ 3 次のいずれかを実行します。

- 変更するには、[Actions] メニューで [Edit Dashboard] を選択します。ダッシュレットを追加または削除し、ダッシュレットをダッシュボード内の別の位置にドラッグできます。設定が終了したら、[Save] をクリックします。
- ダッシュボードを削除するには、[Actions] メニューで [Delete Dashboard] を選択します。確認ダイアログで [Delete] をクリックします。

ダッシュボードの複製

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 ダッシュボードの複製アイコン（スターアイコンの隣）をクリックします。

ステップ 3 [Duplicate a Dashboard] ダイアログボックスで、ダッシュボードコピーのタイトルを入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 コピーしたこのダッシュボードは、ダッシュレットを追加、削除、または再配置することで変更できます。

ステップ 6 [Save] をクリックしてダッシュボードを保存します。
確認のダイアログが表示されます。

ステップ 7 [OK] をクリックします。

ダッシュボードをお気に入りにする

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Dashboard Library]** の順に選択します。

[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 ダッシュレット名の横にある ☆ をクリックすると、お気に入りとして登録されます。

（注） [Favorite Dashboards] タブをクリックすると、お気に入りにしたダッシュボードにアクセスできます。

ダッシュレットの位置の変更

アシュアランスのダッシュボード（デフォルト）で、ダッシュレットの位置を変更できます。

ステップ 1 次のいずれかを実行します。

- Cisco DNA Center GUI で **[Menu]** アイコン（☰）をクリックし、**アシュアランス** > **[Health]** を選択します。

[Overall Health] ダッシュボードが表示されます。

- Cisco DNA Center GUI で **[Menu]** アイコン（☰）をクリックし、**アシュアランス** > **[Health]** > **[Network Health]** タブを選択します。

  [ネットワークの健全性（Network Health）] ダッシュボードが表示されます。

- Cisco DNA Center GUI で **[Menu]** アイコン（☰）をクリックし、**アシュアランス** > **[Health]** > **[Client Health]** タブを選択します。

  [クライアントの健全性（Client Health）] ダッシュボードが表示されます。

- Cisco DNA Center GUI で **[Menu]** アイコン（☰）をクリックし、**アシュアランス** > **[Health]** > **[Application Health]** タブを選択します。

  [Application Health] ダッシュボードが表示されます。

ステップ 2 [Actions] ドロップダウンリスト（右上端）をクリックし、[Edit Dashboard] を選択します。
ダッシュボードが更新され、編集可能になります。

ステップ 3 移動するダッシュレットをクリックしてダッシュボードの別の位置にドラッグします。

ステップ 4 [Save] をクリックします。

第 17 章

ネットワークのトレンドを観察し洞察を得る

ネットワークのトレンドとインサイトについて

Cisco AI Network Analytics 機械学習アルゴリズムと AI テクノロジーを使用して、次の情報を提供します。

- **トレンドとインサイト**：グローバルパターン（トレンド）と乖離度を調べて、システム生成のインサイトを提供します。
- **比較分析**には、次の機能があります。
  - **AI 駆動型 AP 比較**：ヒートマップ内の特定の月について、ネットワーク内のすべての AP を比較してトレンドを把握し、洞察を得ます。
  - **AI 駆動型のピア比較**：選択した主要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。
  - **AI 駆動型のネットワークの比較**：選択した KPI 全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリ、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する

Cisco AI Network Analytics は、機械学習アルゴリズムを使用して、潜在的にクライアント エクスペリエンスが低いワイヤレス AP を特定します。AP は長期間にわたって継続的に分析され、最適ではないクライアントエクスペリエンスを提供していると疑われる AP は、根本的な原因と提案される改善点によってグループ化されます。修正可能な根本的な問題を診断するために使用できる一連の無線およびネットワーク機能で構成されるインサイトが生成されます。インサイトには次の主要なコンポーネントがあります。

- さまざまなクライアント エクスペリエンス KPI によってパフォーマンスの低い AP を検出します。
- 根本原因分析（RCA）の基礎として、重要であり、顧客によって実行可能な、不十分なクライアント エクスペリエンスまたは優れたクライアント エクスペリエンスを持つ AP を区別できる適切な機能を見つけます。

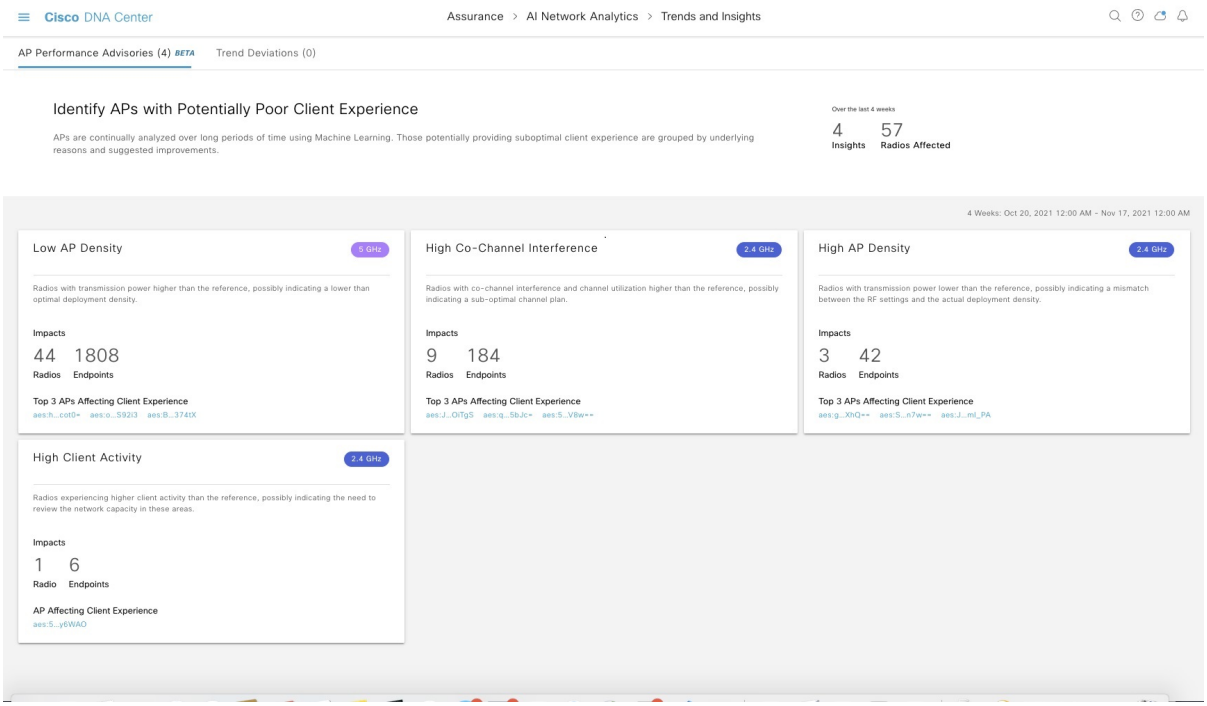
AP は、2.4 GHz と 5 GHz の別々の周波数帯域で分析されます。SNR、RSSI、リンク速度、パケット再試行、パケット障害など、さまざまな KPI の統計分析を使用して、不十分なクライアント エクスペリエンスが検出されます。

この手順を使用して、 AP パフォーマンスアドバイザリを表示し、4 週間のデータの分析に基づいてクライアント エクスペリエンスが低い最もアクティブな AP を強調表示します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Trends and Insights]** > **[AP Performance Advisories]** の順に選択します。

ステップ 2 [AP Performance Advisories] タブをクリックすると、一般的な根本原因分析カテゴリと影響を受ける無線に関するさまざまなタイプのインサイトの概要が表示されます。

図 *32* : アクセス ポイント パフォーマンス アドバイザリ



一般的な根本原因分析で発生する可能性のあるインサイトを以下に示します。

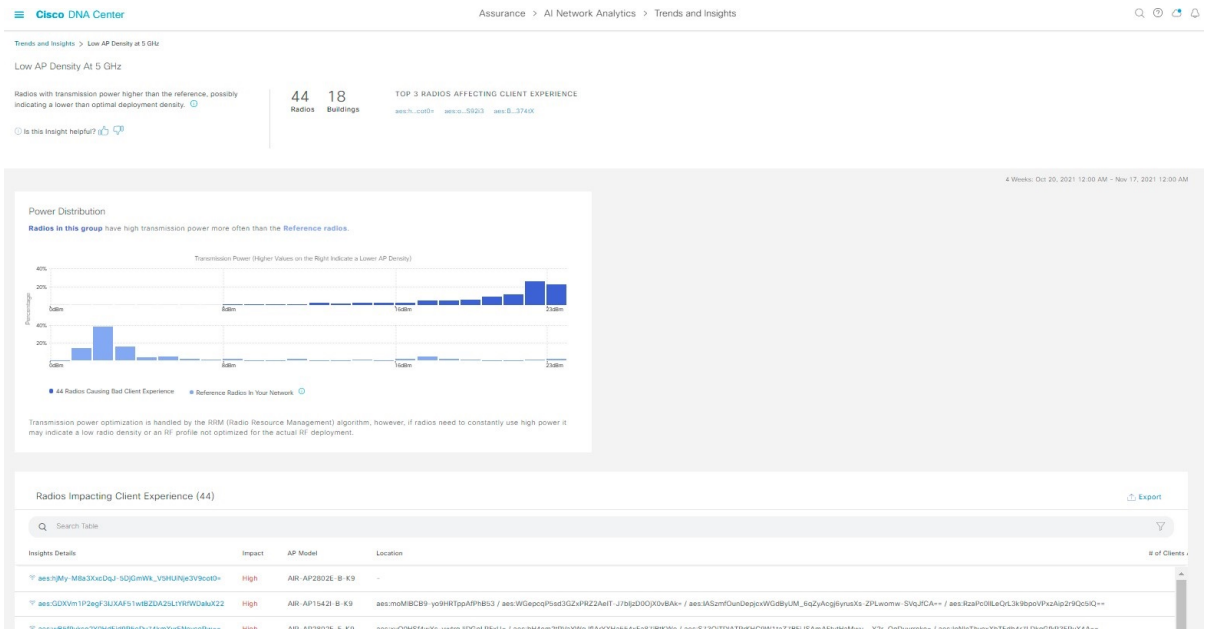
- 外部 RF 負荷
- クライアントアクティビティが多い外部 RF 負荷
- 頻繁なチャネル変更
- 高 RF 負荷
- 高いチャネル使用率
- 高いクライアントアクティビティ
- 高いクライアントの負荷
- 高い AP 展開密度
- 低い AP 展開密度
- 低い AP 展開密度および外部干渉
- 低い AP 展開密度および高負荷

ステップ 3 [AP Performance Advisories] ダッシュボードを使用して、次のインサイトの概要を確認します。

[Network Overview] ウィンドウ	
アイテム	説明
インサイトサマリー	特定の周波数帯に関するインサイト（低 AP 密度、高クライアントアクティビティなど）の名前と問題定義を表示します。
影響	インサイトごとに影響を受ける [Radios] と [Endpoints] の数を表示します。
クライアントエクスペリエンスに影響する上位 3 つの AP	特定の周波数帯で影響を受ける上位 3 つの AP を表示します。これらは、手順 5 に示す詳細ページへのハイパーリンクです。

ステップ 4 次の情報について各インサイトダッシュレットをクリックすると、一般的な根本原因分析と、このカテゴリのすべての無線に対する推奨アクションが表示されます。

図 *33*：影響を受ける無線のインサイト サマリー ダッシュボード



インサイトダッシュボード	
アイテム	説明
[Summary]	4 週間にわたって分析された無線の総数、建物の数、影響を受けた上位 3 つの AP を表示します。
[KPI] チャート	すべての無線での KPI の分布を示す RCA カテゴリに応じて、複数の KPI チャートを表示します。チャートを使用して、この一般的な RCA を使用した無線のパフォーマンスを、クライアントエクスペリエンスの問題が検出されていない参照の無線と比較対照できます。

インサイトダッシュボード	
アイテム	**説明**
[Radios Impacting Client Experience] テーブル	インサイトの詳細、影響（低、中、または重大）、AP モデル、場所、影響を受けるクライアントの数、およびクライアントエクスペリエンスに影響を与える KPI が含まれます。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。

ステップ 5 [Radios Impacting Client Experience] テーブルで、ハイパーリンクされた AP をクリックして、特定の AP に関する次の詳細なインサイトサマリーを表示します。

図 *34* : アクセスポイントのインサイトサマリー

インサイトダッシュボード	
アイテム	**説明**
上部バー	AP モデル、場所、影響を受けるクライアント、および [Assurance Device] ウィンドウにハイパーリンクされた追加の AP の詳細などの情報を表示します。また、クライアントエクスペリエンスを向上させるために、特定された根本原因と異常な KPI に固有の推奨アクションも提供します。

インサイトダッシュボード	
アイテム	説明
[Client Experience KPIs]	• ヒストグラムは、クライアントエクスペリエンスに影響を与えるさまざまなKPIの分布を示し、個々のAPと顧客のネットワーク全体の参照AP（クライアント エクスペリエンスの問題が観察されていない AP）を比較しやすくします。 • デフォルトでは、異常が検出されたKPIのみが表示されます。SNR、RSSI、リンク速度、パケットの再試行、パケットの失敗など、KPI の分布を表示する KPI の数を増やすことができます。 • カーソルをヒストグラムの bin 値の上に置くと、AP の参照セットと比較して、選択した AP で観測された発生率の追加の詳細を表示できます。
[Radio Specific Root-Cause Context]	• ヒストグラムは、無線に影響を与えるさまざまな根本原因分析KPIの分布を示します。デフォルトでは、異常が検出された KPI のみが表示されます。 • SNR、RSSI、リンク速度、パケットの再試行、パケットの失敗など、RCA KPI の分布を表示する KPI の数を増やすことができます。 • カーソルをヒストグラムの bin 値の上に置くと、無線の参照セットと比較して、選択した無線で観測された発生率の追加の詳細を表示できます。

ネットワークトレンドの表示とインサイトの取得

トレンドは、一定期間にわたって観察されたネットワーク内の動作の長期的な進化です。次のトレンドは、ネットワークのパフォーマンス（蜂群グラフで表現）に関するインサイトを提供します。以下のタイプのインサイトがあります。

- [Intra-Site]：Cisco AI Network Analytics は、単一のサイトまたはビルを検索し、そのビル内だけの外れ値デバイスを強調表示します。この場合、蜂群グラフ内のエンティティは無線であり、円で表されます。
- [Inter-Site]：Cisco AI Network Analytics は、グローバルネットワークを調べ、選択した KPI に関して外れ値となっているビルを特定します。この場合、蜂群グラフ内のエンティティはビルであり、多角形で表されます。

ネットワークのトレンドを表示するには、次の手順を実行します。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **ネットワークインサイト**

[Network Insights] ウィンドウに、[Capacity]、[Coverage]、[Throughput] のフィルタが表示されます。テーブルのデータを更新するには、該当するフィルタをクリックします。デフォルトでは、[Capacity] フィルタが選択されています。

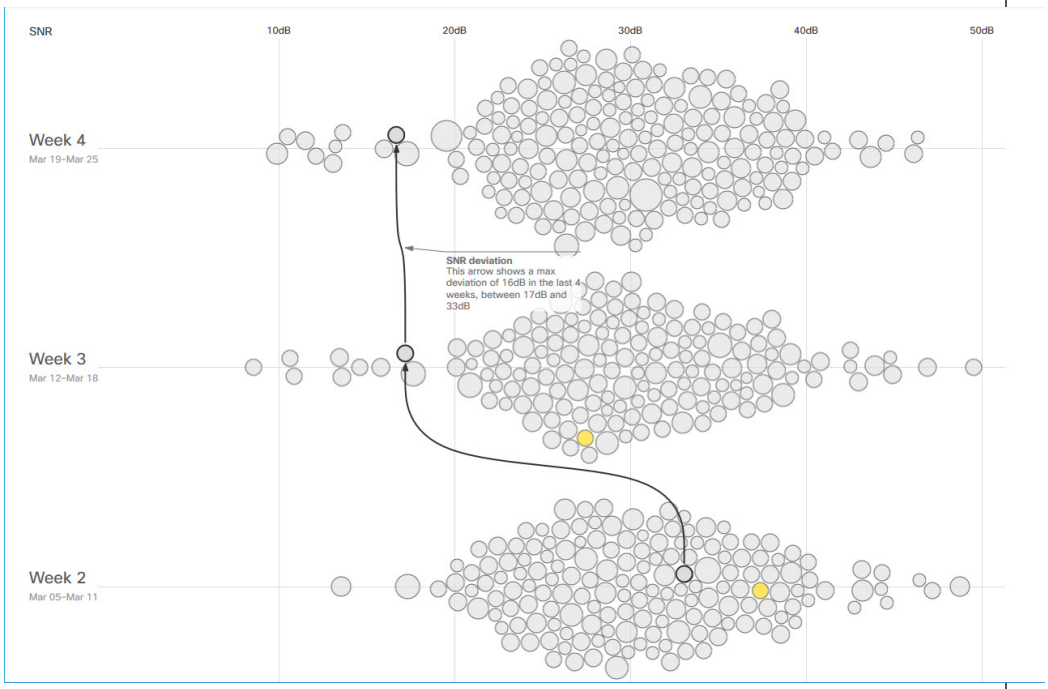
（注） フィルタは動的です。フィルタに使用可能なインサイトがない場合、そのフィルタは表示されません。

インサイトテーブル	
アイテム	**説明**
Occurrence	このトレンドが観測された期間（[May 27 - June 03 2019] など）。
Insight	特定の期間に観測されたすべての AI 駆動型のインサイトのリスト。
カテゴリ	インサイトが観測されたカテゴリ。インサイトの KPI は次のカテゴリにグループ化されます。 • [Capacity]：無線クライアント数、チャネル変更数 • [Coverage]：干渉、平均クライアント SNR、平均クライアント RSSI、トラフィック、使用率 • [Throughput]：総無線スループット
Frequency band	インサイトが観測された AP で使用されていた帯域周波数。値は [2.4 GHz]、[5 GHz]、またはその両方の周波数帯です。
KPI	特定のインサイトに関する重要業績評価指標（KPI）。
⋮ アイコン	インサイトテーブルに表示する列をカスタマイズできます。⋮ アイコンをクリックし、表示しない列のチェックボックスをオフにして、[Apply] をクリックします。

ステップ 2 [insights] 列でインサイトをクリックするとスライドインペインが開き、次の情報が表示されます。

[Insight Details] スライドインペイン	
アイテム	**説明**
Cisco AI	インサイトの計算方法に関する情報が表示されます。 人工知能の概要については、こちらを参照してください。
Insight Summary	蜂群グラフで確認されるトレンドに関する簡単なサマリー。このサマリーには、サイトまたは AP の名前、クライアント数、無線帯域周波数、および乖離が観測された時間帯などの情報が表示されます。
Weekly Client Load	週あたりのクライアント負荷。

[Insight Details] スライドインペイン	
アイテム	説明
トラブルシューティング	重大な問題になる前にトレンドのトラブルシューティングと修正を実施するためのリンクがあります。 • [Network Heatmap] をクリックすると、ヒートマップが開き、蜂群グラフで強調表示されている AP またはビルディングに関する情報が提供されます。トレンドが観測された特定の月のヒートマップが表示されます。 • [Intra-Site]：ヒートマップが起動し、特定の AP が優先順位に従って強調表示されたリストが表示されます。 • [Inter-Site]：ヒートマップが起動し、ビルディング（サイト）内の AP のフィルタ処理されたビューが表示されます。 • AP の名前をクリックすると、その AP の [Device 360] ページが開きます。
問題数	問題数のグラデーション。

[Insight Details] スライドインペイン	
アイテム	説明
チャート（Chart）	蜂群グラフには、次の図に示すように、ネットワーク内のクライアントデバイスのパフォーマンスが 4 週間分表示されます。チャートの一番下が第 1 週、一番上が第 4 週を表します。一定期間にわたってネットワークの動作が体系的に乖離している場合、その傾向はチャート内の矢印によって表示されます。 **図 *35 :* 蜂群チャート**  （注） • 蜂群チャート内の各円は、以下を表します。 • **サイト内**：円は無線を表します。 • **サイト間**：多角形はビルを表します。 • 円のサイズは、AP 内のクライアントの数を表します。小さな円には少数のクライアントが、大きな円には多数のクライアントが含まれます。

ステップ 3 チャート内の円の上にカーソルを置くと、AP の名前と MAC アドレス、帯域周波数、AP グループ、AP の場所、問題の数、クライアント数、および KPI 値などの情報が表示されます。

（注） グローバルサイトでは、チャート内の円の上にカーソルを置くと、トレンドが観測されたビルやクライアント数に関する情報が表示されます。

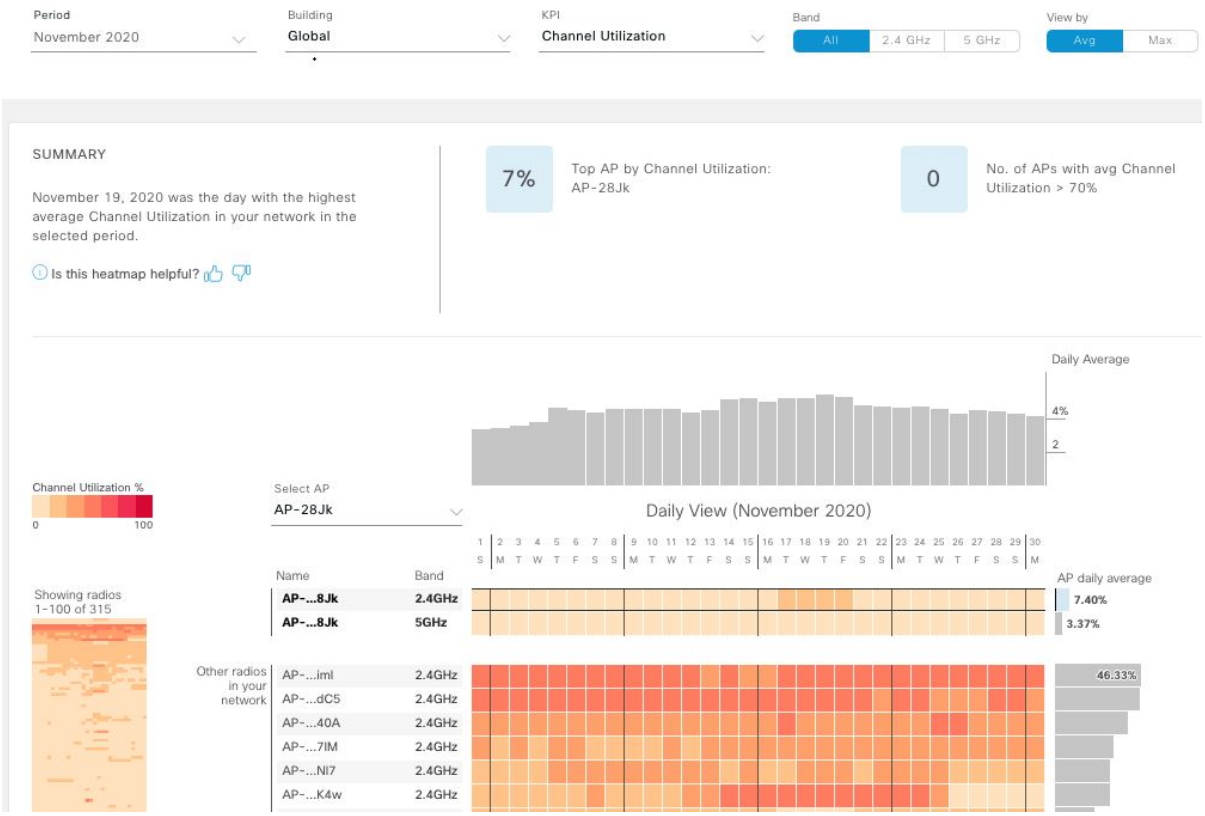
ネットワークヒートマップ内アクセスポイントの比較

ネットワークヒートマップを使用して、特定の月に関してネットワーク内のすべての AP を視覚的に比較し、トレンドを把握し、インサイトを取得します。異なる KPI と帯域周波数で AP を比較することを選択できます。取得したインサイトにより、最も輻輳が多い KPI、最も輻輳のある AP、および それらの AP のうち使用中の AP に関する情報が得られます。この情報により、トレンドが観察されたサイトまたはビルにさらにドリルダウンすることができます。AP または AP のグループを特定したら、それらの AP の動作履歴（1 日、1 週間、および月全体）を判断できます。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Network Heatmap]** の順に選択します。

[Network Heatmap] ウィンドウに次の情報が表示されます。

図 *36 : [Network Heatmap]* ウィンドウ



[Network Heatmap] ウィンドウ	
アイテム	説明
[Period]	ドロップダウンリストから選択した月の情報がヒートマップに表示されます。

[Network Heatmap] ウィンドウ	
アイテム	説明
[Building]	グローバルネットワーク全体またはドロップダウンリストから選択した特定のサイトとビルディングの情報がヒートマップに表示されます。デフォルトは [Global] です。
[KPI] ドロップダウンリスト	ドロップダウンリストから選択したKPIのヒートマップに情報を表示します。デフォルトは [Client Count] です。
[Band]	選択した帯域周波数のヒートマップに情報を表示します。[All]、[2.4 GHz]、[5 GHz] のいずれかを選択できます。デフォルトは [All] です。
[View By]	選択したオプションに基づいてヒートマップの情報を表示できます。 [View By] のリストに表示されるオプションは、選択した KPI に応じて異なります。 KPI に応じて、[Avg]、[Min]、または [Max] を並べ替えのオプションとして選択できる場合、[Avg] または [Max] を選択できる場合のほか、いずれのオプションも提供されない場合もあります。
[Summary] 領域	ヒートマップ分析から得られたインサイトの概要が表示されます。次のタイプの情報が表示されます。 • 最もビジーだった日。 • 無線あたりのクライアント数がゼロの AP の数。 • 無線あたりのクライアント数が 50 を超える AP の数。
[Feedback] アイコン	 アイコンをクリックして、このページの情報が役に立ったかどうかについてコメントを入力し、[Submit] をクリックしてください。
KPI のグラデーション	このエリアには、[KPI] ドロップダウンリストから選択した KPI に応じて、KPI のパフォーマンスに関する情報が色のグラデーションで表示されます。濃い色のブロックは、有意な KPI スコアを示します。たとえば、低い RSSI スコアは、高い RSSI スコアよりも有意になります。クライアント数が多いスコアは、クライアント数の少ないスコアよりも有意になります。
[Search AP] ドロップダウンリスト	AP を検索および選択できます。次の手順を実行します。 **1.** [Search AP] ドロップダウンリストをクリックし、検索フィルタにAP名を入力します。 検索した AP がドロップダウンリストで強調表示されます。 **2.** 強調表示された AP をクリックして選択します。 AP の個々の無線が、ヒートマップに個別に表示されます。

[Network Heatmap] ウィンドウ	
アイテム	説明
[Network Daily Avg]、[Network Daily Min]、または [Network Daily Max] グラフ	選択した [View By] オプションに応じて、該当するグラフが表示されます。 • [Avg] を選択した場合、日単位の平均値が表示され、最も高い平均値がグラフ内で強調表示されます。 • [Min] または [Max] を選択した場合、日単位の最小値または最大値が表示され、それらの値がグラフ内でそれぞれ強調表示されます。 グラフのバーにカーソルを合わせると、それぞれの日の KPI 値が表示されます。
[Showing Radios] ヒートマップ	ヒートマップの圧縮ビューが表示されます。 デフォルトでは、この領域には、最初の 100 個の無線のヒートマップが表示されます。追加の無線のヒートマップデータを表示するには、圧縮されたヒートマップの下部までスクロールして、ドロップダウンリストから適切なオプションを選択します。
[AP Heatmap] エリア	次が含まれます。 • [Radios in Your Network]：AP の名前とクライアントによって使用された帯域周波数が表示されます。AP の横にあるアイコンをクリックすると、その AP の [Device 360] ページが開きます。 この領域には、[Band] のオプションから選択した帯域周波数に応じて、対応する帯域の AP が一覧表示されます。 • [AP Heatmap]：AP の動作履歴（1 時間、1 日、1 週間、および月全体）を確認できます。ブロック内の色の明度は、その有意性を示します。濃い色のブロックは、薄い色のブロックよりも有意性が高くなります。ヒートマップの各行が 1 つの AP を表します。 [Heatmap] 内のカラーブロックにカーソルを合わせると、AP に関する情報（名前と MAC アドレス、帯域周波数、場所、日次平均 KPI スコアなど）が表示されます。 • [AP Daily Average] または [AP Daily Max]：この領域には、[Sort By] オプションで選択した内容に応じて、各 AP のその月の平均 KPI スコアまたは最大 KPI スコアが表示されます。スコアが最も高い AP がリストの一番上に表示されます。 [AP Daily Average] または [AP Daily Max] 領域にカーソルを合わせると、AP のその月の平均 KPI または最大 KPI の値を確認できます。

[Network Heatmap] ウィンドウ	
アイテム	説明
Export	CSV ファイルにヒートマップデータをエクスポートするには、[Export] をクリックします。 ヒートマップに適用されている AP とフィルタは、エクスポート対象のデータに適用されます。エクスポートは、日単位のビューでのみ有効になり、時間単位のビューでは有効になりません。

ステップ 2 追加の無線のヒートマップデータを表示するには、ウィンドウの下部までスクロールして、ドロップダウンリストから適切なオプションを選択します。

KPI 値をネットワーク内のピアと比較

選択した重要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。

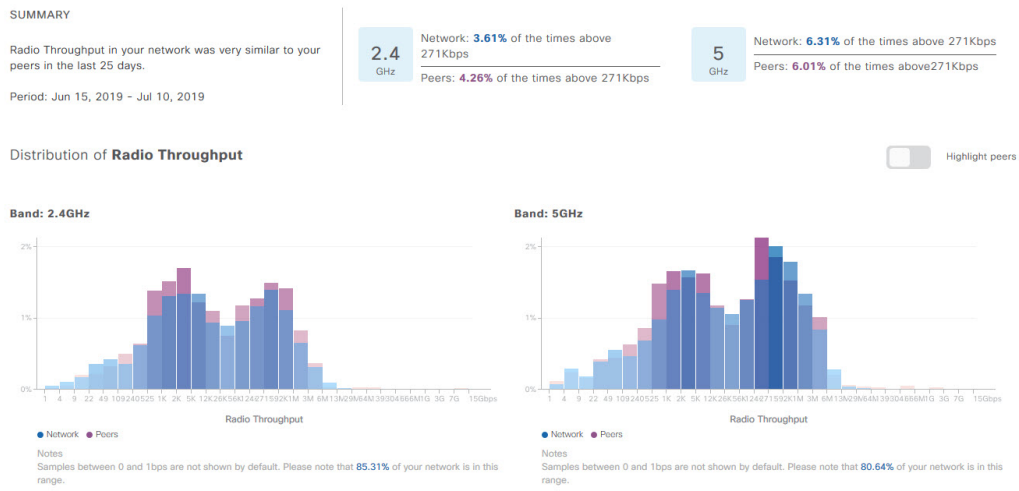
（注） 比較に使用されるピアネットワークは、同様の規模のネットワークです。

ピアの比較では、計算のために、オンボーディングの日付から数ヵ月のデータが使用されます。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Peer Comparison]** の順に選択します。

[Peer Comparison] ウィンドウが開き、次の情報が表示されます。

[Peer Comparison] ウィンドウ	
アイテム	説明
[KPI] ドロップダウンリスト	ドロップダウンリストから KPI を選択します。[Radio Throughput]、[Cloud Apps Throughput]、[Radio Resets]、[Packet Failure Rate]、[Interference]、[RSSI] のいずれかを選択できます。デフォルトは [Radio Throughput] です。
Show	自ネットワークとピアネットワークの間の KPI 値を比較する曜日を選択します。デフォルトは [All] です。
要約	AIネットワーク分析は、棒グラフを分析し、結果に関する簡単なサマリーを表示します。 • [2.4 GHz]：2.4 GHz 帯域周波数のネットワーク値とピア値のサマリー。 • [5 GHz]：5 GHz 帯域周波数のネットワーク値とピア値のサマリー。

[Peer Comparison] ウィンドウ	
アイテム	説明
[Highlight Peers] トグルボタン	自ネットワークとピアネットワークのグラフを切り替えることができます。
ピア比較棒グラフ	デフォルトでは、次の図に示すように、[Band 2.4 GHz] および [Band 5 GHz] グラフのネットワークの KPI 値が強調表示されます。 ピアネットワークの KPI 値を強調表示するには、[Highlight Peers] ボタンをクリックします。 **図 *37*: ピア比較棒グラフ**  グラフの色は、以下を表します。 • **青**：自ネットワーク。 • **ピンク**：ピアネットワーク。

ステップ 2 特定の日について、自ネットワークとピアネットワークの KPI 値を表示するには、[Show] エリアで該当する日を選択します。

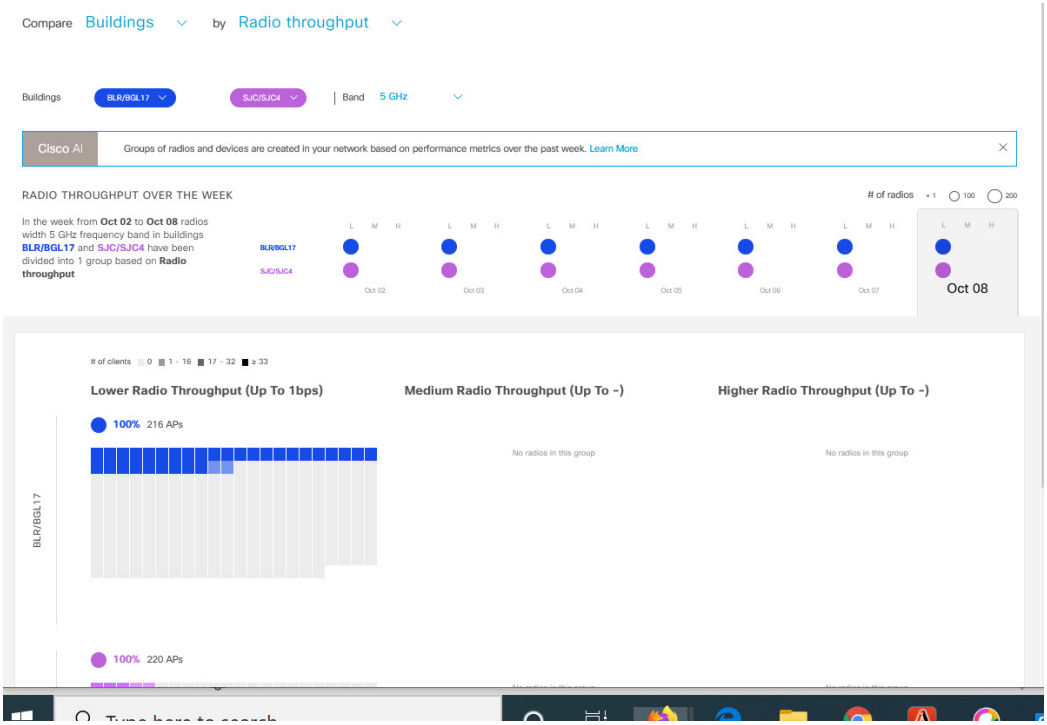
建物、AP モデルファミリ、およびワイヤレス エンドポイント タイプの比較

この手順を使用して、選択した重要業績評価指標（KPI）全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリ、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

ステップ 1 メニューアイコン（☰）をクリックして、**アシュアランス** > **[Network Object Comparison]** の順に選択します。

[Network Object Comparison] ウィンドウが開き、次の情報が表示されます。

図 *38 : [Network Object Comparison]* ウィンドウ



[Network Object Comparison] ウィンドウ	
アイテム	**説明**
[Compare] ドロップダウンリスト	比較するネットワーク内のオブジェクトを選択します。オプションは、[Buildings]（サイト）、[AP Model Families]、または [Wireless Endpoints]（Android デバイス、Android 携帯、IOS タブレット、IOS 携帯、Linux ワークステーションなど）です。

[Network Object Comparison] ウィンドウ	
アイテム	説明
[By KPI] ドロップダウンリスト	ネットワーク内のオブジェクトを比較するために使用する KPI を選択します。 [Buildings] の場合、オプションは次のとおりです。 • [Radio Throughput] • [Channel Utilization] • [Average Client RSSI] • [Average Client SNR] • [Average Onboarding Time] • [Average Authorization Time] • [Average DHCP Time] • [Cloud Throughput] • [Media Throughput] • [Social Throughput] • [Interference] [AP Model Families] の場合、オプションは次のとおりです。 • [Radio Throughput] • [Interference] • [Media Apps Throughput] • [Average Client RSSI] • [Channel Utilization] • [Average Client SNR] • [Cloud Throughput] • [Social Throughput] [Wireless Endpoints] の場合、オプションは次のとおりです。 • [Average AAA Time] • [Average Onboarding Time] • [Average DHCP Time]

[Network Object Comparison] ウィンドウ	
アイテム	説明
[Buildings] [AP Model Families] または [Wireless Endpoints] ドロップダウンリスト	KPI 値を比較する最初のネットワークオブジェクト（建物、AP モデルファミリ、またはワイヤレスエンドポイント）を選択します。最初のネットワークオブジェクトは青色で表示されます。 KPI 値を最初のネットワークオブジェクトと比較する 2 番目のネットワークオブジェクトを選択します。2 番目のネットワークオブジェクトはピンク/紫色で表示されます。
[Band]	帯域周波数を選択します。[Band 2.4 GHz] または [Band 5 GHz] を選択できます。
[Summary/Timeline]	各ネットワークオブジェクトの曜日ごとの平均KPIパフォーマンスが表示されます。
[Client Count] のグラデーション または [Device Count] のグラデーション	[Radio Throughput] や [Average Client RSSI] などの KPI については、この領域に各サイトの無線ごとのクライアント数が示されます。 [Onboarding Time] などの KPI については、この領域に各サイトのデバイス数が示されます。 ブロックの色の濃さでクライアント数またはデバイス数が示されます。濃い色のブロックには、薄い色のブロックよりも多くのクライアントやデバイスが存在します。
[AP Clusters] または [Device Type Clusters]	この領域には、各ネットワークオブジェクトに 1 つずつ、2 つのクラスタのセットが表示されます。この領域では、2 つのネットワークオブジェクトのパフォーマンスを視覚的に比較できます。次の情報を出力します。 • KPI のパフォーマンス（パーセンテージ）。 • ネットワーク内のオブジェクトの各サイトでのクラスタ化方法。 • KPI 値が低、中、高のネットワーク内のオブジェクト。 [Onboarding Time] や [Authorization Time] などの KPI については、この領域に次のような情報が表示されます。 • クライアントが各サイトでオンボーディングするデバイスのタイプ。たとえば、Windows ワークステーション、OS X ワークステーション、Linux ワークステーション、Android 電話機、IOS デバイスなどです。 • 各デバイスタイプの数。 • KPI の時間が低、中、高のデバイスの数。

ステップ 2 クラスタ内の色付きブロックにカーソルを合わせると、日付、AP が存在する建物、AP のモデル番号、無線プロトコル、無線クライアント数など、APに関する情報が表示されます。濃い色のブロックには、薄い色のブロックよりも多くのクライアントが存在します。

ベースラインを使用したネットワークパフォーマンスの表示と監視

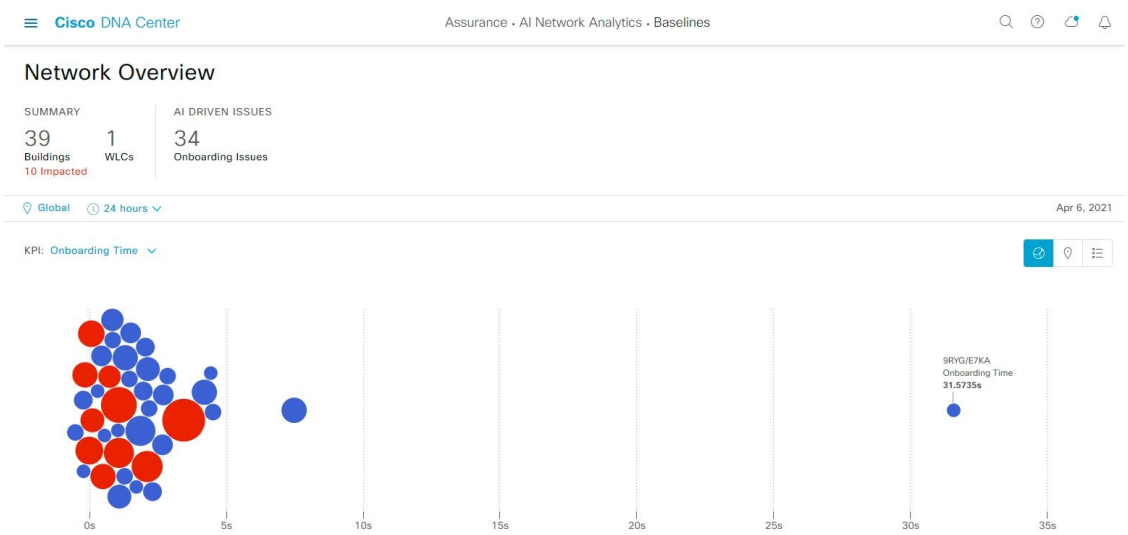
Cisco AI Network Analytics は最先端の機械学習技術を使用して、特定のネットワークとサイトに関するベースラインを定義します。Cisco AI Network Analytics は、この情報に基づいて特定の時点における各ネットワークとサイトの正常な動作を定義し、最も重要な問題を特定できます。

機械学習アルゴリズムから派生したベースラインを使用してネットワークパフォーマンスを調査および監視するには、次の手順を実行します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Baselines]** の順に選択します。

[Baselines] ダッシュボードが表示されます。

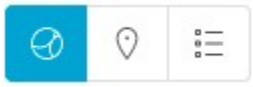
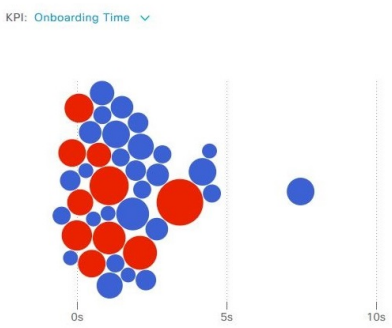
図 *39 : [Baselines]* ダッシュボード



ステップ 2 [Network Overview] ウィンドウを使用して、次の情報が表示されます。

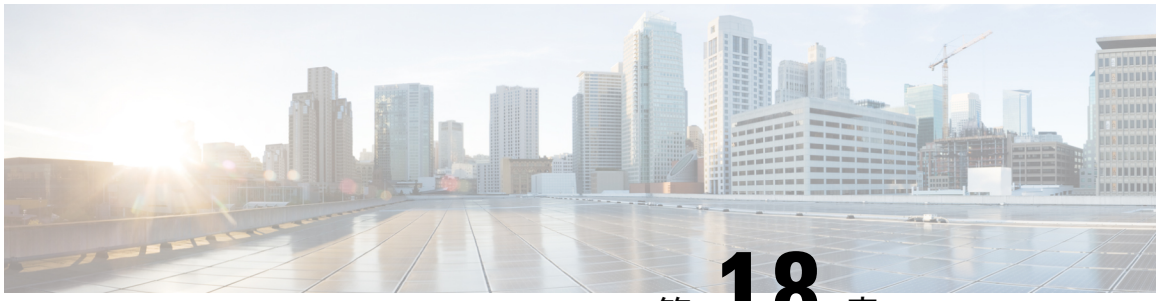
[Network Overview] ウィンドウ	
アイテム	**説明**
[Summary]	ネットワーク内の建物の総数、問題の影響を受けた建物の総数、および WLC の総数が表示されます。
[AI Driven Issues]	特定のネットワーク環境の予測ベースラインからの乖離度に基づいてトリガーされ、Cisco AI Network Analytics によって検出された問題が表示されます。

[Network Overview] ウィンドウ	
アイテム	説明
 [Location] ドロップダウンリスト	ロケーションアイコンをクリックしてペインのスライドを開き、サイトまたは建物を選択します。ダッシュボード上の情報が、選択に応じて更新されます。
 [Time Range] 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。 • ドロップダウンメニューで、範囲の長さ（[24 Hours]、またはカスタム範囲）を選択します。 • 開始日と終了日を指定します。 • [Apply] をクリックします。
[KPI] ドロップダウンリスト	ドロップダウンリストから KPI を選択します。オプションは、[Onboarding Time]、[Onboarding Failures]、[DHCP Time]、[Authentication Time]、および [Association Failures] です。デフォルトは [Onboarding Time] です。
 [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、ネットワークの地理的ロケーションに基づいたマップビューに表示されます。
 [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。

[Network Overview] ウィンドウ	
アイテム	説明
 [Beeswarm Chart]	このトグルボタンをクリックすると、選択したKPIに関するネットワークのクライアントデバイスのパフォーマンスに関するインサイトを提供する蜂群チャートが表示されます。  この場合、蜂群チャート内のエンティティは建物であり、円で表されます。 蜂群チャート内の各円は、以下を表します。 • 青色：円は建物を表します。チャート内の円の上にカーソルを合わせると、ロケーション、KPI、SSID、WLC、クライアント数などの情報が表示されます。 • 赤色：円は問題の影響を受けた建物を表します。チャート内の円にカーソルを合わせると、ロケーション、KPI値、SSID、WLC、クライアント数、AIに起因する問題などの情報が表示されます。 • 円のサイズは、接続されているクライアントの数を表します。小さな円には少数のクライアントが、大きな円には多数のクライアントが含まれます。

ステップ3 蜂群チャートから円をクリックして、次の情報の建物ビューを表示します。

建物ビュー
サイトまたは建物の特定の情報が表示されます。それぞれのドロップダウンリストからKPI、SSID、およびWLCを選択して、データを表示できます。 より詳細な時間範囲を指定するには、タイムラインスライダを使用します。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。 タイムラインスライダの下に色分けされたチャートが表示され、指定された期間内に選択された重要業績評価指標（KPI）の予測ベースラインからの乖離度に基づいてトリガーされた、ネットワークのパフォーマンスの問題を判断します。チャートの上にカーソルを合わせると、選択した時点での期間、予測上限範囲と予測下限範囲を示す、同期化されたツールチップが表示されます。 カラーコードは次のことを表します。 • 赤色はAIに起因する問題を表します。 • 青色は平均KPI期間を表します。 • 緑色は予測KPIを表します。 [View Details]をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。この内容は、KPIチャートから選択したKPIによって異なります。スライドインペインに、平均KPI期間（[Onboarding Time]、[DHCP Time]、[Onboarding Failures]、[Authentication Time]など）と固有のクライアントの色分けされたチャートが表示されます。 サンキーグラフは、フロアとデバイスタイプ（クライアントデバイス）間の主要なフローを強調するために表示されます。チャートの下にあるテーブルに、AP名、オンボーディング、失敗したオンボーディング、失敗したオンボーディングの割合、クライアント数などのデータがテーブルに表示されます。 （注） テーブルに表示されるクライアント数は、30分間に観測された個々のクライアント数の測定値における選択された時間間隔の平均です。



第 18 章

インテリジェントキャプチャの管理

インテリジェントキャプチャについて

Cisco DNA Center では、デバイスやクライアントの正常性に関するすべての情報は、通常シスコ ワイヤレス コントローラから入手できます。インテリジェントキャプチャ機能は Cisco DNA Center とアクセスポイント（AP）間の直接通信リンクをサポートしているため、各 AP は Cisco DNA Center と直接通信できます。Cisco DNA Center はこのチャネルを使用して、パケットキャプチャデータ、AP とクライアントの統計情報、およびスペクトルデータを受信できます。インテリジェントキャプチャ機能は、Cisco DNA Center と AP 間の直接通信リンクを利用することで、ワイヤレスコントローラからはアクセスできないデータに AP からアクセスできるようにします。

（注）
- インテリジェントキャプチャは、ローカルモードまたは FlexConnect モードの AP でのみサポートされます。
- インテリジェントキャプチャは、SDA 展開ではサポートされていません。

インテリジェントキャプチャ対応デバイス

インテリジェントキャプチャをサポートするシスコ ワイヤレス コントローラを次の表に示します。

サポート対象の Cisco Catalyst ワイヤレスコントローラ	
デバイス	サポート対象の最小ソフトウェアバージョン
Cisco 3504 ワイヤレス コントローラ	AireOS 8.8.125.0
Cisco 5520 ワイヤレス コントローラ	AireOS 8.8.125.0
Cisco 8540 ワイヤレス コントローラ	AireOS 8.8.125.0

インテリジェントキャプチャをサポートする Cisco Catalyst ワイヤレスコントローラを次の表に示します。

サポート対象の Cisco Catalyst ワイヤレスコントローラ	
デバイス	サポート対象の最小ソフトウェアバージョン
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	IOS-XE Gibraltar 16.12.1.s

インテリジェントキャプチャをサポートする Cisco AP を次の表に示します。

サポート対象の Cisco AP		
デバイス	サポート対象 AireOS ソフトウェアの最小バージョン	サポート対象 IOS-XE ソフトウェアの最小バージョン
Aironet 1540 AP[3]	8.10.105.0	16.12.1.s
Aironet 1560 AP	8.10.105.0	16.12.1 s
Aironet 1815 AP [1]	8.10.105.0	16.12.1 s
Aironet 1830 AP [1]	8.10.105.0	16.12.1 s
Aironet 1840 AP [1]	8.10.105.0	16.12.1 s
Aironet 1850 AP [1]	8.10.105.0	16.12.1 s
Aironet 2800 シリーズ AP	8.8.125.0 または 8.10	16.12.1s
Aironet 3800 シリーズ AP	8.8.125.0 または 8.10	16.12.1s
Aironet 4800シリーズ AP [4]	8.8.125.0 または 8.10	16.12.1s
Catalyst 9105 AP[1]	8.10 MR3	17.3.1
Catalyst 9115 AP [1]	8.10.105.0	16.12.1 s

サポート対象の Cisco AP		
デバイス	サポート対象 AireOS ソフトウェアの最小バージョン	サポート対象 IOS-XE ソフトウェアの最小バージョン
Catalyst 9120 AP	8.10.105.0 8.10.112.0（スペクトル解析向け）	16.12.1s 17.2.1（スペクトル解析向け）
Catalyst 9130 AP [2]	8.10 MR3	17.3.1
Catalyst IW6300 Heavy Duty シリーズ AP	8.10.105.0	17.1.1s
Catalyst ESW6300 組み込みサービス AP	8.10.105.0	17.1.1s

[3] スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、Catalyst 9105 AP、および Catalyst 9115 AP ではサポートされていません。

[4] データパケットキャプチャは、Aironet 4800 AP および Catalyst 9130 AP のみでサポートされます。

インテリジェントキャプチャのベストプラクティス

インテリジェントキャプチャ機能を Cisco DNA Center で確実に最適化するためのベストプラクティスを以下で紹介します。

- 新しいワイヤレス コントローラ デバイスを Cisco DNA Center に追加したら、インテリジェントキャプチャのグローバル設定を無効にしてから、設定を再度有効にします。これで、新しいワイヤレスコントローラにインテリジェントキャプチャが設定されます。
- Cisco DNA Center からワイヤレス コントローラ デバイスを削除する前に、すべてのインテリジェントキャプチャ設定を無効にします。
- 管理対象のワイヤレスコントローラのアップグレードや Cisco DNA Center の再イメージ化の前に、すべてのインテリジェントキャプチャ設定を無効にします。アップグレード完了後に設定を再度有効にします。

クライアントデバイス向けのライブおよびスケジュール済みキャプチャセッション

クライアントデバイス向けキャプチャセッションについて

クライアントデバイスに対して、次の種類のキャプチャセッションを実行できます。

- **ライブキャプチャセッション**：ライブキャプチャセッションは即時に開始できます。特定のクライアントに対して最大3時間実行可能です。「クライアントデバイスのライブキャプチャセッションの有効化 （346 ページ）」を参照してください。
- **スケジュール済みキャプチャセッション**：スケジュール済みキャプチャセッションは、将来の任意の時刻にスケジュールし、最大8時間実行可能です。「クライアントデバイス向けキャプチャセッションのスケジュールと管理 （352 ページ）」を参照してください。

（注） スケジュール済みキャプチャセッションとライブキャプチャセッションは同じデータを収集するため、現行のスケジュール済みキャプチャセッションは、ライブキャプチャセッションと同等です。

ライブおよびスケジュール済みキャプチャセッションでは、オンボーディングイベント（2 秒間隔）および RF 統計情報チャート（5 秒のサンプル）のデータを収集できます。このデータは、**[Client 360]** > **[Intelligent Capture]** ウィンドウに表示されます。

クライアント キャプチャ セッションの制限事項

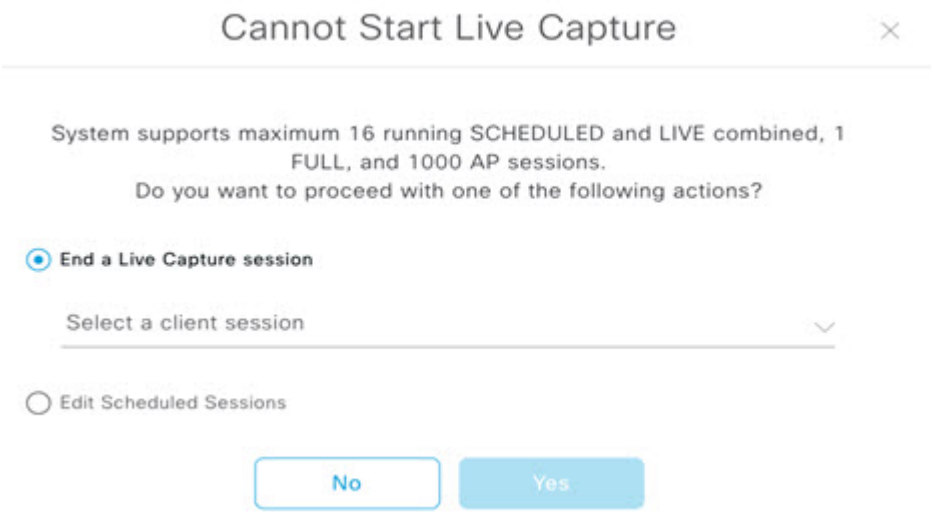
クライアント キャプチャ セッションの制限事項は次のとおりです。

- キャプチャセッション（ライブおよびスケジュール済み）には合計 16 個のタイムスロットが割り当てられています。セッション内の各クライアントは1つのタイムスロットを使用します。

  ライブキャプチャセッションの最大数は 16 であるため、16 のライブキャプチャセッションが同時に実行されている場合は、スケジュール済みキャプチャセッションに使用できるスロットはありません。

  同時に実行可能なスケジュール済みキャプチャセッションは、最大 12 です。このため、常に 4 個（16 - 12）のスロットがライブキャプチャセッション用に確保されています。

  たとえば、17個目のライブキャプチャセッションを開始しようとすると、この最大値を超えるため、次のエラーメッセージが表示されます。エラーメッセージのダイアログボックスで [Yes] をクリックし、次に終了するライブキャプチャセッションを選択します。



（注） 16個のタイムスロット制限は、ワイヤレスコントローラによって適用されます。

キャプチャセッションが Cisco DNA Center で設定されている場合、Cisco DNA Center が認識していないライブキャプチャセッションやスケジュール済みのキャプチャセッションはすべて削除されます（ワイヤレスコントローラで直接設定された部分的なパケット キャプチャ セッションなど）。

- オンボーディングイベント期間中は、オンボーディングイベントに関連した最大 100 パケットのキャプチャが可能です。
- Cisco DNA Center に格納するすべてのスケジュール済みオンボーディング パケット ファイルの合計サイズには、3.5 GB の制限があります。制限を超えると、合計サイズが 3.5 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

クライアント統計情報について

グローバル設定のライブおよびスケジュール済みキャプチャセッションを使用すると、サポート対象の AP でクライアント統計情報を 5 秒間隔で収集できます。

クライアント統計情報は、クライアントが接続されている AP で AP 統計が有効になっている場合にも 30 秒間隔で収集されます。

収集されたクライアント統計情報は、[Client 360] > [Intelligent Capture] ウィンドウの 4 つの RF 統計情報チャートに表示されます。

クライアントデバイスのライブキャプチャセッションの有効化

以下の手順により、特定のクライアントデバイスに対してライブキャプチャセッションを有効にし、オンボーディングイベントと RF 統計情報のデータパケットを表示できます。

ステップ 1 [Health]メニューアイコン（≡）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

[クライアントの健全性（Client Health）] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- **[クライアントデバイス（Client Devices）]** 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索（Search）] フィールド（右上端）に次のいずれかを入力します。ユーザ ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレス。

クライアント デバイスの 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンがクライアント名の横に表示される場合は、クライアントまたはアクセスポイントがインテリジェント キャプチャ データを送信できない Cisco DNA Center （370 ページ） で詳細を確認してください。

図 *40* : クライアントの *[Intelligent Capture]* ウィンドウ

ステップ 5 タイムラインスライダは、次の機能に使用できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。ライブキャプチャの結果については、オンボーディングイベントの折れ線グラフが表示されます。緑色はオンボーディングイベント、赤色は異常イベントを示します。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注） タイムラインには、最長で過去 2 週間のデータを表示できます。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

ステップ 6 ライブキャプチャセッションを実行するには、次の手順を実行します。

a) ライブキャプチャセッションを開始するには、右上隅にある [Start Live Capture] をクリックします。

ライブキャプチャセッション中、[Onboarding Events] と [RF Statistics] ダッシュレットのデータパケットが収集されます。

b) ライブキャプチャセッションを停止するには、[Stop Capturing] ボタンをクリックします。

（注） ライブキャプチャセッションは3時間実行されます。3時間が経過すると、セッションを延長するためのダイアログボックスが表示されます。

c) 実行中のライブキャプチャセッションは、クライアントの [Intelligent Capture Settings] ウィンドウで確認できます。

ステップ7 ネットワーク接続の確立に関連付けられているイベントを表示するには、[Onboarding Events ダッシュレットを使用します。

[Onboarding Events] ダッシュレット	
アイテム	**説明**
[All]および Anomaly PCAP フィルタ	オンボーディングイベントをフィルタ処理できます。次のオプションがあります。 • [All]：すべてのイベントを表示します。これはデフォルトです。 • Anomaly PCAP：異常イベントのみをフィルタ処理します。 （注） クライアントがネットワークに参加する際に問題が発生した場合は、特定のイベントの横に「PCAP」という語が赤色で表示されます。 クライアントが問題なくネットワークに参加できる場合は、特定のイベントの横に「PCAP」という語が灰色で表示されます。
Export PCAP	指定されたイベントの範囲のパケットをダウンロードできます。 1. [Export PCAP] をクリックします。 2. PCAP に含める最初と最後のイベントを指定します。 3. ダウンロードを開始するには、[Download PCAP] ボタンをクリックします。 （注） ヒューリスティックを使用してイベントに属するパケットを判断するため、最初のイベントの1分前と最後のイベントの1分後のパケットがダウンロードに含まれます。これにより、すべての関連するパケットがダウンロードされたPCAPに含まれるようになります。 各エクスポートに含まれるのは、最もタイムスタンプが古いものから2000パケットまでに制限されます。

[Onboarding Events] ダッシュレット	
アイテム	説明
オンボーディング、不完全、および異常イベントのリスト	オンボーディング、不完全、および異常イベントのリストを時系列順に表示します。イベントは、以下を示すために色分けされています。 ● : 正常なオンボーディングイベント。 ● : 不完全なイベント。 ● : 異常イベント。 （注） アイコン付きのイベントは、このイベントのデータパケットがダウンロードまたは分析のためにキャプチャされていることを示します。 親イベントグループをクリックすると、グループを展開して、そのグループの個々のイベントを表示できます。

[Onboarding Events] ダッシュレット	
アイテム	説明
Event Details	イベントグループまたは個々のイベントをクリックすると、次のセクションでさらに詳細情報を表示できます。 [Client Location]：イベント中のクライアントの場所のマップとクライアントの移動のマップが表示されます。 [Auto Packet Analyzer]：このセクションは、ライブキャプチャ、スケジュールされたキャプチャ、または異常キャプチャセッションがイベントのパケットをキャプチャした場合に表示されます。イベントの横に表示される アイコンは、イベントによってパケットがキャプチャされたことを示します。 [Auto Packet Analyzer] セクションには、次の情報を含むグラフが表示されます。 • イベントを囲むパケット（最大 100 個）は、次の 2 つのグループに分けられます。グレーのセクションは、オンボーディングセッション開始前のパケットを示します。白のセクションは、オンボーディングセッション内のパケットを示します。 認証解除パケットと予期しないパケットのパターンは赤色の三角形で表されます。これらは、クライアントのオンボーディングエクスペリエンスを低下させる可能性のある重要な意味を持つパケットです。 [Download Packets] をクリックすると詳細分析のためにパケットをダウンロードできます。 • パケット（クライアントまたは AP からのパケット） • オンボードパケットのステージ識別子 • パケット間ギャップ（ms） • パケットごとの RSSI（dBm） • 関連付けられている AP [RF Statistics]：イベントを囲む 10 分間隔の RF 統計データを使用したグラフが表示されます。 RF 統計データは、RSSI および SNR 測定値（デシベル単位）、Rx 平均データレートと Rx 最終データレート、Tx パケットと Rx パケット、および Tx パケットの再試行で構成されます。 （注） [Anomaly Capture] が有効になっている場合、ライブまたはスケジュールされたキャプチャが実行されていない場合でも、異常イベントのパケットはキャプチャされます。

ステップ 8 [Client Location] ダッシュレットでは、フロアマップを表示して次の情報を確認できます。

- フロア上のクライアントと AP の場所。
- 色の強度でカバレッジの強度を表すヒートマップ。
- フロアマップ上のクライアントのリアルタイムロケーション。クライアントが別の場所に移動すると、その移動が表示されます。
- RF 統計情報 RSSI、SNR、データレート、スループット、およびパケットドロップレートを使用して接続が色分け表示されたクライアント証跡トラッキング。

  マップ上の色は、クライアントの正常性を示します。

  ●：良い ●：平均 ●：悪い
- 選択したオンボーディングイベントの時間を含む 1 分間のクライアントのトラッキング。
- マップの下のリプレイおよび停止/開始のコントロールを使用すると表示をコントロールできます。

（注） クライアントロケーション機能を使用するには、CMX が Cisco DNA Center と統合されている必要があります。詳細については、「ワイヤレスマップ向け Cisco CMX の統合 （379 ページ）」の章を参照してください。

ステップ 9 [RF Statistics] ダッシュレットでは、RF 情報の詳細を確認できます。

クライアントの AP クライアント統計情報は、4 つのチャートに表示さます。クライアント統計情報について （345 ページ）を参照してください。データは色分けされていて、次の情報が含まれています。

- RSSI および SNR の測定値（デシベル単位）。
- Rx 平均データレート（直近の 5 秒間）および Rx 最新データレート。
- Tx パケットおよび Rx パケット。
- Tx パケットの再試行。

チャートでは、次の操作を実行できます。

- チャートにカーソルを重ねると、特定の時点の統計を表示できます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルト表示に変更するには、  アイコンをクリックします。

ステップ 10 クライアントデバイスのデータパケットキャプチャを実行するには、「クライアントデバイスのデータパケットキャプチャの実行 （356 ページ）」を参照してください。

クライアントデバイス向けキャプチャセッションのスケジュールと管理

スケジュール済みのキャプチャセッションを停止、編集、削除するには、次の手順を実行します。

クライアントキャプチャセッションは、次のデータを収集します。

- オンボーディングイベントのデータパケットおよび**[Client 360]** > **[Intelligent Capture]** ウィンドウに表示される [RF Statistics] チャートデータ（5 秒のサンプル）。クライアントデバイスのライブキャプチャセッションの有効化 （346 ページ） を参照してください。
- **[Device 360]** > **[Intelligent Capture]** ウィンドウに表示されるチャートおよび表のデータ。RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理 （364 ページ） を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 クライアント キャプチャ セッションをスケジュールするには、[+ Schedule Client Capture] をクリックします。

[Schedule Client Capture] スライドインペインで、次の設定を行います。

a) [Start Time] エリアで、キャプチャセッションを開始するタイミングを指定します。[Run Now]、[Run Later] のどちらかを選択できます。
b) [Duration] ドロップダウンリストをクリックして期間を指定します。
c) [Select Client Devices] ドロップダウンリストをクリックすると、カテゴリの一致を返す検索文字列を入力できます（クライアント ユーザー ID、ホスト名、MAC アドレス）。

（注） 検索では、カテゴリごとに最大 10 個の一致が返されるため、エントリが見つからない場合は検索文字列を再調整します。

（注） キャプチャセッションの詳細については、クライアントデバイス向けキャプチャセッションについて （344 ページ） を参照してください。

d) [Save] をクリックします。

ステップ 3 実行中のキャプチャセッションを停止するには、次の手順を実行します。

a) [In-progress Captures] タブをクリックします。
b) テーブルからクライアントを選択します。
c) [Stop Capture] をクリックします。

ステップ 4 将来の時間にスケジュールされたキャプチャセッションを編集するには、次の手順を実行します。

a) [Scheduled Captures] タブをクリックします。
b) テーブルからクライアントを選択します。

c) [Edit Schedule] をクリックします。

ステップ 5 完了したキャプチャセッションを削除するには、次の手順を実行します。

a) [Completed Captures] タブをクリックします。
b) テーブルからクライアントを選択します。
c) [Delete Schedule] をクリックします。

クライアントデバイス向けデータパケットキャプチャ

クライアントデバイス向けデータパケットキャプチャについて

データパケットキャプチャを使用すると、ネットワークデータをPCAPファイルにキャプチャできます。このファイルはWiresharkでダウンロードして表示できます。さらに、Network Analysis Module（NAM）と統合すれば、クライアントデバイスに関する情報（アクセスされたアプリケーションとポート、QoSデータ、パケット損失、ワイヤレス遅延、ジッター）をキャプチャできます。NAMの統合については、NAM統合について（354ページ）を参照してください。

データパケットキャプチャを実行するには、クライアントデバイスのデータパケットキャプチャの実行（356ページ）を参照してください。

データパケットキャプチャの制限事項

データパケットキャプチャには、次の制限事項があります。

- データパケットキャプチャは、Cisco Aironet 4800 APおよびCisco Catalyst 9130 APでのみサポートされます。データパケットキャプチャが有効になっていて、クライアントがパケットキャプチャに対応していないAPにローミングした場合、クライアントがパケットキャプチャ対応のAPに再接続するまで、パケットキャプチャは停止します。
- 一度に実行できるデータ パケット キャプチャ セッションは1つだけです。
- すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Centerとシスコ ワイヤレス コントローラの間でクロックを同期させる必要があります。ワイヤレスコントローラがNetwork Time Protocol（NTP）サーバーに接続されていることを確認します。
- 各データ パケット キャプチャ セッションで最大1 GBのローリングデータをキャプチャできます。ダウンロードを高速化するために、1 GBのデータが10個の100 MBのファイルに分割されます。

NAM 統合について

ソフトウェアバージョン 6.4(2) 以降を実行中の Network Analysis Module（NAM）または vNAM サーバーをご使用の場合は、お使いの NAM サーバーを Cisco DNA Center と統合できます。インストールと設定の詳細については、*Cisco Prime* 仮想ネットワーク解析モジュール（*vNAM*）インストールおよびコンフィギュレーション ガイド [英語] を参照してください。

クライアントに対して NAM 統合とフルパケットキャプチャを有効にすると、**[Client 360]** > **[Intelligent Capture]** ウィンドウの [Wireless Packet Application Analysis] チャートにデータが提供されます。このテーブルとチャートには、クライアントが使用するアプリケーション、その QoS 設定、パケット損失、ワイヤレス遅延、およびジッターに関する情報が表示されます。

NAM サーバーを Cisco DNA Center と統合するには、次の手順を実行します。

1. NAM データポートで IP アドレスを設定します。
2. gRPC コレクタを設定します。

（注） NAM 統合は、IPv6 アドレスを使用する Cisco DNA Center クラスタではサポートされません。

NAM データポートでの IP アドレス設定

NAM や vNAM のデータポートに有効な IP アドレスを設定するには、次の手順を実行します。この手順は、NAM と統合するために必要です。

（注） データポートはパケットを受信するためだけのもので、要求には応答しません。したがって、IP アドレスを正しく設定していても、データポートに ping を実行するとタイムアウトになります。IP アドレスが有効で、Cisco DNA Center から到達可能であることを確認します。

ステップ 1 NAM サーバーの CLI にログインします。

ステップ 2 コマンド **show data-port ip-addresses** を入力します。
コマンドにより、ポート番号と IP アドレスが表示されます。

```
Device# show data-port ip-addresses
Port number: 1
IPv4 address: 172.20.125.125
```

ステップ 3 **show data-port ip-addresses** コマンドで何も表示されない場合、コマンド **data-port 1 ip-address** *ip-address* を入力して、IP アドレスをポート 1 に割り当てます。

ステップ 4 **show data-port ip-addresses** コマンドを再度実行し、そのデータポート 1 が IP アドレスに割り当てられたことを確認します。

ステップ 5 データ ポート 1 またはその他の表示されているポートの IP アドレスの 1 つを記録します。

ステップ 6 **cdb-export** が Cisco DNA Center で有効であることを確認します。そのためには、**show cdb-export all** コマンドを入力します。何も表示されない場合は、コマンド **cdb-export collector 1 ip-address** *IP-address-of-Cisco-DNA-Center* を入力します。

ステップ 7 コマンド **autocreate-data-source erspan** を入力して、Cisco DNA Center からのデータパケットが処理されていることを確認します。

ステップ 8 NAM や vNAM サーバーと Cisco DNA Center で時間が同期していることを確認します。NAM ユーザーインターフェイスから **[Administration]** > **[System]** > **[System Time]** の順に選択することにより、時刻を同期できます。

gRPC コレクタの設定

この手順を gRPC コレクタに対して実行して NAM を統合します。gRPC は、オープンソースの高パフォーマンス RPC（リモートプロシージャコール）フレームワークです。

始める前に

NAM データポートで IP アドレスを設定します。NAM データポートでの IP アドレス設定 （354 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Data Platform]**。

[Data Centers] ウィンドウが表示されます。

ステップ 2 [Collectors] タブをクリックします。

[Collectors] ウィンドウが表示されます。

ステップ 3 [GRPC-COLLECTOR] をクリックします。

[GRPC-COLLECTOR] ウィンドウが表示されます。

ステップ 4 **[+ Add]** をクリックします。

[gRPC Collector Configuration] ウィンドウが表示されます。

ステップ 5 [GRPC-COLLECTOR] 設定を 1 つだけ追加します。次の手順を実行します。

a) [ConfigData] エリアで [Agent Export] チェックボックスをオンにして、ネットワークパケットデータの NAM へのエクスポートを有効にします。

b) [Agent IP Address] フィールドに、記録したデータポートの IP アドレスを入力します（NAM データポートでの IP アドレス設定 （354 ページ） の ステップ 5 （354 ページ） を参照してください）。

c) [Configuration Name] フィールドに、GRPC-コレクタ設定の一意の名前を入力します。

d) [Save Configuration] をクリックします。

クライアントデバイスのデータパケットキャプチャの実行

この手順では、クライアントデバイスのデータパケットキャプチャを実行する方法を示します。

始める前に

アクセスされたアプリケーションとポート、QoSデータ、パケット損失、ワイヤレス遅延、およびジッターに関する情報を取得するには、NAM 統合を有効にする必要があります。詳細については、「NAM 統合について （354 ページ）」を参照してください。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

[クライアントの健全性（Client Health）] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- **[クライアントデバイス（Client Devices）]**表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索（Search）] フィールド（右上端）に次のいずれかを入力します。ユーザ ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレス。

クライアント デバイスの 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンがクライアント名の横に表示される場合は、クライアントまたはアクセスポイントがインテリジェント キャプチャ データを送信できない Cisco DNA Center （370 ページ） を参照してください。

図 *41* : クライアントの *[Intelligent Capture]* ウィンドウ

ステップ 5 タイムラインスライダは、次の機能に使用できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注） タイムラインには、最長で過去 2 週間のデータを表示できます。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

ステップ 6 データパケットキャプチャを実行するには、[Data Packet Capture] エリア（右上隅）で次の機能を使用します。

[Data Packet Capture] エリア	
アイテム	説明
[Run Data Packet Capture] ボタン	このボタンを使用して、クライアントのデータパケットキャプチャを開始します。データ パケット キャプチャ ファイルは、トラブルシューティングと [Wireless Packet Application Analysis] ダッシュレットに使用されます。 データパケットキャプチャがクライアントに対して現在実行されている場合は、[Data Packet Capturing Stop] をクリックして停止します。 （注） 一度に実行できるデータ パケット キャプチャ セッションは 1 つだけです。データパケットキャプチャの実行中に [Run Data Packet Capture] をクリックすると、現在のキャプチャを終了するか、または新しいキャプチャを開始するかのオプションが表示されたダイアログボックスが現れます。 データ パケット キャプチャ セッションが Cisco DNA Center で設定されている場合、Cisco DNA Center が認識していないデータ パケット キャプチャ セッションはすべて削除されます（ワイヤレスコントローラで直接設定されたフルパケット キャプチャ セッションなど）。 （注） すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Center とシスコ ワイヤレス コントローラの間でタイムゾーンを同期させる必要があります。ワイヤレスコントローラが Network Time Protocol（NTP）サーバーに接続されていることを確認します。 （注） 新しいキャプチャセッションが開始されるたびに、新しい一連の PCAP ファイルが開始されます。
[Download] ボタン	フルパケット PCAP ファイルがセッションからキャプチャされたら、このボタンクリックして PCAP ファイルをダウンロードします。データパケットファイルをダウンロードするには、[Download] 列にあるアイコンをクリックします。次のいずれかのファイルをダウンロードできます。 • ワイヤレスデータ：AP とクライアント間のパケットの 802.11 ファイル。 • 有線データ：AP とスイッチまたはワイヤレスコントローラ間のパケットのイーサネットファイル。 （注） データ パケット キャプチャ ファイルには、100 MB の制限があります。すべてのデータ パケット キャプチャ ファイルの合計は、3.5 GB を超えることはできません。 （注） 過去 7 日間の PCAP ファイルのみダウンロードできます。

ステップ 7 [Wireless Packet Application Analysis] ダッシュレットでは、データパケットキャプチャの詳細を確認できます。

データパケットキャプチャが実行されている場合、このダッシュレットには、アクセスされたアプリケーションとポート、QoS データ、パケット損失、ワイヤレス遅延、およびジッターなど、分析されたパケットに関する詳細が表示されます。

（注） このダッシュレットにデータを表示するには、NAM の統合を設定する必要があります。NAM 統合について （354 ページ）を参照してください。

クライアントの データパケットキャプチャ履歴の表示

クライアントのデータ パケット キャプチャ セッションの履歴（最初のパケットと最後のデータパケットがキャプチャされた時刻、キャプチャされたデータパケットの合計サイズ、パケットのタイプなど）を表示するには、以下の手順を実行します。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 [Client Data Packet Capture] タブをクリックします。

[Client Data Packet Control] ウィンドウが表示されます。

ステップ 3 [Intelligent Capture Settings - Client Data Packet Capture] ウィンドウには、次の情報が表示されます。

オプション	説明
[Identifier]	クライアントのユーザー ID またはホスト名が表示されます。ユーザー ID またはホスト名をクリックすると、[Intelligent Capture: Client Device] ウィンドウが開きます。
[MAC Address]	クライアントデバイスの MAC アドレスが表示されます。
[First Packet Time]	最初のデータパケットがキャプチャされた時刻が表示されます。
[Last Packet Time]	最後のデータパケットがキャプチャされた時刻が表示されます。
[Total Size]	キャプチャされたデータの合計サイズが表示されます。
[Currently Running]	データパケットキャプチャが実行中かどうかを表示します。
[Type of Packet]	パケットのタイプ（[Wired]、[Wireless] など）が表示されます。

アクセスポイント向けインテリジェントキャプチャ

アクセスポイントのインテリジェントキャプチャについて

AP インテリジェントキャプチャ機能を使用すると、1 つ以上の AP で次のデータをキャプチャできます。

- **AP 統計情報キャプチャ**には、次の情報が含まれます。
  - **[Device 360]** > **[Intelligent Capture]** ウィンドウの [RF Statistics] タブに表示される AP 無線および WLAN 統計情報。
  - 選択した AP に関連付けられているすべてのクライアントの **[Client 360]** > **[Intelligent Capture]** ウィンドウで [RF Statistics] エリアに表示される AP クライアントの統計情報（サンプリング時間は 30 秒）。
- **異常キャプチャ**は、選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント（グローバルまたは選択した AP に関連付けられているすべてのクライアント）をキャプチャして、ダウンロードまたは表示できます。

キャプチャの制限事項

Cisco DNA Center に格納する異常をトリガーしたパケットファイルの合計サイズには、1.05 GB の制限があります。制限を超えると、合計サイズが 1.05 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

アクセスポイントのインテリジェントキャプチャの有効化と管理

1 つまたは複数のアクセス ポイント（AP）を有効にして次のデータをキャプチャするには、以下の手順を実行します。

- **AP 統計情報**：AP 無線の統計情報、WLAN 統計情報、および AP クライアントの統計情報が含まれます。
- **異常キャプチャ**：選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント（グローバルまたは選択した AP に関連付けられているすべてのクライアント）をキャプチャして、ダウンロードまたは表示できます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Assurance]** > **[Intelligent Capture Settings]**。

[Client Schedule Capture] ウィンドウが表示されます。

ステップ 2 [Access Points] タブをクリックします。

[Access Point] ウィンドウが表示されます。

ステップ 3 AP 統計情報キャプチャを有効または無効にするには、次のいずれかを実行します。

- 有効な AP がない場合は、[Configure AP Enablement] エリアが表示されます。[Specific] または [Global] のいずれかのオプションを選択し、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[AP Stats Capture] ウィンドウが表示されます。[AP Stats Capture] ウィンドウで、次のいずれかのオプションを選択します。

オプション	説明
None - disable all APs	1 つ以上の AP が有効になっている場合は、「None - disable all APs」 と表示されます。 現在有効になっているすべての AP で 統計情報キャプチャを無効にできます。
Specific - select specific APs and enable	選択した AP の 統計情報キャプチャを有効にできます。次の手順を実行します。 **1.** [Specific - select specific APs and enable] オプションボタンをクリックします。 **2.** 左側のペインで、[Global] を展開し、サイト > ビルディング > フロア の順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。 **3.** 選択した AP の統計情報キャプチャを有効にするには、次の手順を実行します。 • [Disabled APs] タブをクリックします。統計情報キャプチャが現在無効になっている AP のリストが表示されます。 • 統計情報キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。 **4.** 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 （注） 互換性のない AP の条件は次のとおりです。 • 動作モードが [local] または [FlexConnect] に設定されていない。 • AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。
Global - enable all capable APs	すべての対応 AP で統計情報キャプチャを有効にできます。

ステップ 4 異常キャプチャを有効または無効にするには、[Anomaly Capture] タブをクリックして、次のいずれかを実行します。

- 有効になっている AP がない場合は、[Configure AP Enablement] エリアが表示されます。次のいずれかのオプションを選択してから、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[Anomaly Capture] ウィンドウが表示されます。[Anomaly Capture] ウィンドウで、次のいずれかのオプションを選択します。

オプション	説明
None - disable all APs	1 つ以上の AP が有効になっている場合は、「None - disable all APs」 と表示されます。 現在有効になっているすべての AP で異常キャプチャを無効にできます。

オプション	説明
Specific - select specific APs and enable or disable	選択した AP の異常キャプチャを有効または無効にできます。次の手順を実行します。 **1.** [Specific - select specific APs and enable or disable] オプションボタンをクリックします。 **2.** 左側のペインで、[Global] を展開し、サイト > ビルディング > フロア の順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。 **3.** 選択した AP の異常キャプチャを有効にするには、次の手順を実行します。 • [Disabled APs] タブをクリックします。異常キャプチャが現在無効になっている AP のリストが表示されます。 （注） 以前に AP を有効にしようとして失敗した場合、[Config Status] 列にエラーメッセージが表示されます。 • 異常キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。 **4.** 選択した AP の異常キャプチャを無効にするには、次の手順を実行します。 • [Enabled APs] タブをクリックします。異常キャプチャが現在有効になっている AP のリストが表示されます。 • 異常キャプチャを無効にする AP の横にあるチェックボックスをオンにして、[Disable] をクリックします。 **5.** 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 （注） 互換性のない AP の条件は次のとおりです。 • 動作モードが [local] または [FlexConnect] に設定されていない。 • AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。 **6.** インテリジェントキャプチャをサポートしている AP のリストを表示するには、[Not-Ready APs] タブの横にある情報（I）アイコンをクリックします。

オプション	説明
Global - enable all capable APs	すべての対応 AP の異常キャプチャを有効にできます。

RF統計情報の表示とアクセスポイントのスペクトル解析データの管理

RF 統計情報を表示し、特定のアクセスポイントのスペクトル解析データを開始および管理するには、次の手順を実行します。

ステップ 1 [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network Health] タブをクリックします。

[Network Health] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名（ハイパーリンクされた識別子）をクリックし、AP の詳細を表示します。
- [Search] フィールド（右上隅にあります）で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

注目 AP 名の横にメッセージ「**GRPC リンクはまだ利用できません（接続中）（GRPC link is not ready（CONNECTING））**」付きの ⚠ アイコンが表示された場合、詳細についてはクライアントまたはアクセスポイントがインテリジェント キャプチャ データを送信できない Cisco DNA Center （370 ページ）を参照してください。

ステップ 5 [RF Statistics] タブをクリックすると、RF 統計情報の詳細が表示されます。

（注） [AP Stats Capture] が有効になっていない場合は、有効にします。アクセスポイントのインテリジェントキャプチャの有効化と管理 （360 ページ）を参照してください。

ステップ 6 [RF Statistics] タブでは、次の操作を実行できます。

a) タイムラインを使用すると、指定された時間の RF 統計情報を表示し、データの範囲を指定できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。タイムラインスライダは、APの正常性を表示するために色分けされています。特定の時刻にカーソルを合わせると、デバイスの正常性スコア、システムリソース、データプレーンなどの詳細を表示できます。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

b) タイムラインの下にある無線周波数セレクタを使用すると、周波数帯域に基づいてダッシュレットに表示されるデータをフィルタ処理できます。ドロップダウンリストをクリックして、[Radio 0 (2.4 GHz or 5 GHz)] または [Radio 1 (5 GHz)] を選択します。

（注） AP に 3 つの無線がある場合、ドロップダウンリストには [Radio 0 (2.4 GHz)]、[Radio 1 (5 GHz)]、または [Radio 2 (5 GHz)] のオプションが示されます。

c) このダッシュレットで、RF 統計情報の詳細を確認できます。

（注） ダッシュレットに表示されるチャートでは、次の操作を実行できます。

- 詳細を表示するには、チャートにカーソルを合わせます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルトに変更するには、 をクリックします。
- チャートの下の色分けされたデータタイプをクリックすると、チャートに表示されているそのデータタイプを無効化または有効化できます。

ダッシュレット	説明
[Clients] ダッシュレット	この AP を使用しているクライアントの数が表示されます。データソースは AP WLAN 統計情報からのものです。
[Top Clients with Tx Failed Packets by SSID] ダッシュレット	テーブル内の SSID のリストが表示されます。テーブルのデータソースは、AP WLAN 統計情報からのものです。棒グラフのデータソースは、AP クライアントの統計情報からのものです。 SSID を選択すると、その SSID の送信に失敗したパケットの上位のクライアントが表示されます。

ダッシュレット	説明
[Channel Utilization] ダッシュレット	AP およびその他のワイヤレスおよびワイヤレス以外のデバイスで使用されているチャネル使用率が表示されます。棒グラフのデータソースは、AP 無線統計情報からのものです。
[Channel Utilization by this Radio] ダッシュレット	AP によって使用されている現在のチャネル使用率、SSID のリスト、接続されているクライアントの数、およびクライアントの過去 15 分間に送受信されたパケット数が表示されます。 テーブルのデータソースは、AP WLAN 統計情報からのものです。円グラフのデータソースは、AP 無線統計情報からのものです。
[Frame Count] ダッシュレット	管理フレームとデータフレームの数が表示されます。データソースは AP 無線統計情報からのものです。
[Frame Errors] ダッシュレット	送受信エラーの数が表示されます。データソースは AP 無線統計情報からのものです。
[Tx Power and Noise Floor] ダッシュレット	送信電力とノイズフロアが表示されます。データソースは AP 無線統計情報からのものです。
[Multicast/Broadcast Counter] ダッシュレット	各 SSID のマルチキャストおよびブロードキャストの数が表示されます。データソースは AP WLAN 統計情報からのものです。

ステップ 7 [Spectrum Analysis] タブをクリックします。

ステップ 8 [Start Spectrum Analysis] タブをクリックし、ペクトル解析セッションを開始します。

（注）
- スペクトル解析期間は 10 分です。
- 同時スペクトル解析セッションの最大数は 20 です。

ステップ 9 [Spectrum Analysis] タブでは、次の操作を実行できます。

a) タイムラインを使用すると、指定された時間のスペクトル解析データを、データの範囲を指定して表示できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。

タイムラインスライダ	
アイテム	説明
タイムラインスライダ	タイムラインスライダは、表示されるデータの時間枠を決定します。タイムラインスライダは、APの正常性を表示するために色分けされています。特定の時刻にカーソルを合わせると、デバイスの正常性スコア、システムリソース、データプレーンなどの詳細を表示できます。 スペクトル解析の場合、時間範囲は 5 分の枠に設定されます。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注） タイムラインには、最長で過去 2 週間のデータを表示できます。 境界線をクリックしてドラッグすると、特定の時間のデータが表示されます。

b) タイムラインの下にある無線周波数セレクタを使用すると、周波数帯域に基づいてチャートに表示されるデータをフィルタ処理できます。ドロップダウンリストをクリックして、[Radio 0 (2.4 GHz)] または [Radio 1 (5 GHz)] を選択します。

（注） AP に 3 つの無線がある場合、ドロップダウンリストには [Radio 0 (2.4 GHz)]、[Radio 1 (5 GHz)]、または [Radio 2 (5 GHz)] のオプションが示されます。

（注） [Radio Mode] と [Channel]（[Spectrum Analysis] チャートの上）にデータが表示されない場合、その AP には選択された帯域を使用している無線がないことを示します。これは、AP に [5 GHz] の無線を出力するクライアントがあるが、無線周波数セレクタが [2.4 GHz] に設定されている場合に発生します。

詳細については、スペクトル解析時の Cisco AP 機能について （369 ページ）を参照してください。

c) [Spectrum Analysis] チャートには、次の機能が用意されています。

スペクトル解析チャート	
アイテム	説明
上位チャート（パーシステンス）	このチャートは、RF環境で検知された各信号の振幅（電力）とチャネル周波数をリアルタイムで提供します。X 軸は振幅を表し、Y 軸はチャネル周波数を表します。 チャート内の色は、選択された 5 分間で同じ振幅およびチャネル周波数で検知される信号の数を表します。 • 青色は、オーバーラップする信号の数が少ない（または信号が同じ振幅と周波数で検知される）ことを示します。 • 赤色は、オーバーラップする信号の数が多いことを示します。 より多くの信号が検知されるにつれ、色の強度が増加します（青色 > 緑色 > 黄色 > オレンジ色 > 赤色）。チャート内の線がオーバーラップし、交差すると、色が変わります。 色の透過性は、信号データの経過時間を表し、古いデータはより透過的になります。 リアルタイムでRF 環境を表示するには、[Real-TimeFFT（Fast Fourier Transform）] をクリックして有効にします。リアルタイム FFT を有効にすると、永続化チャートが制限されて 5 分間のデータストリームのコレクションではなく、「1 つ」の最新データストリームが表示されます。 特定の範囲のチャネルのデータをズームインして表示するには、マウスをクリックしてドラッグし、範囲を選択します。チャートが更新され、選択した特定のチャネルのデータが表示されます。 チャート全体をズームアウトして表示するには、右上隅の虫めがねをクリックします。
ボトムチャート（ウォーターフォール）	このチャートは、データの時間的な解釈を提供します。このチャートは、パーシステンスチャートと同じ情報を提供しますが、フォーマットは異なります。X 軸は時間を表し、Y 軸はチャネル周波数を表します。チャート内の行は、イベントが発生した正確な順序を表します。これにより、問題が発生した場合に根本原因をトラブルシュートすることができます。 チャート内の色は、振幅を表します。青色は低い値（-100 dBm）を示し、赤色は高い値（-20 dBm）を示します。

d) [Interference and Duty Cycle] チャートには、次の情報が表示されます。

- 検出された干渉とその重大度：
  - 干渉は、半径が干渉の帯域幅を表す円としてプロットされます。X 軸は干渉が検出された周波数を表し、Y 軸は重大度を表します。

- [Severity] は、干渉と範囲の影響を測定します。範囲は 0（影響がないことを示す）から 100（大きな影響を示す）です。
- 干渉タイプは RF 署名から決定され、Cisco CleanAir テクノロジーによって識別され ます。

- 各チャネルのデューティサイクル。

スペクトル解析時の Cisco AP 機能について

Cisco Aironet 2800 シリーズ、3800 シリーズ、および 4800 シリーズ アクセスポイント（AP）には、フレキシブル ラジオ アサインメント（FRA）を備えたデュアルバンド無線がスロット 0 に搭載されています。この FRA 無線は 2.4 GHz で動作しますが、5 GHz で動作するように割り当てることができます。このモードは、AP の動作モードとは異なるように変更できます。AP の FRA 無線を 5 GHz で動作するように設定すると、クライアント無線は 2.4 GHz 帯域で動作できなくなります。

（注） スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、および Catalyst 9115 AP ではサポートされていません。

（注） AP に正しいソフトウェアバージョンがインストールされていることを確認します。インテリジェントキャプチャ対応デバイス （342 ページ） に記載された「**サポート対象の Cisco AP** 」の表を参照してください。

スペクトル解析のための無線スロットの割り当ては次のとおりです。

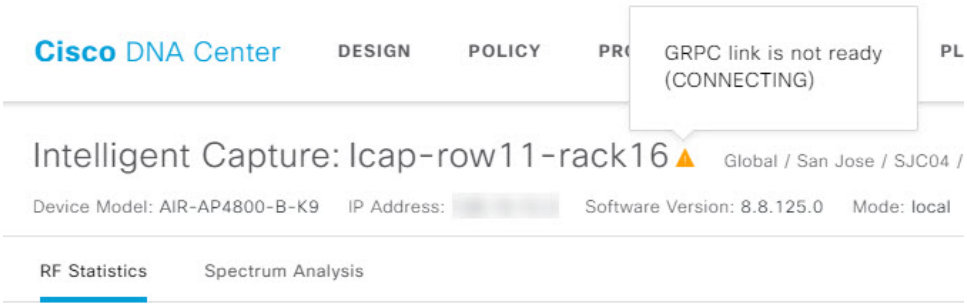
デバイス モデル	スペクトル解析の無線スロットの割り当て
Aironet 2800 シリーズ AP Aironet 3800 シリーズ AP Aironet 1560 AP Catalyst IW6300 Heavy Duty シリーズ AP Catalyst IW6300 Heavy Duty シリーズ AP	無線スロット 0 および 1 が有効になっています。

デバイス モデル	スペクトル解析の無線スロットの割り当て
Aironet 4800 シリーズ AP Catalyst 9120 AP Catalyst 9130 AP	これらの AP には、3 つの無線スロットがあります。 データパケットキャプチャが実行されている場合は、無線スロット 0 および 1 が有効になります。 データパケットキャプチャが実行されていない場合は、無線スロット 2 が有効になります。 （注） AP スペクトル解析データは、2.4 GHz チャネル帯域では表示されません。また、2.4 GHz 帯域を提供する AP 無線がない場合、[Radio Mode] フィールドと [Channel] フィールドは空になります。こうした状況になるのは、FRA 無線が 5 GHz で動作するように設定され、パケットキャプチャが有効になっている場合です。

インテリジェントキャプチャのトラブルシューティング

クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center

問題：クライアントまたはアクセスポイントがインテリジェント キャプチャ データを Cisco DNA Center に送信できません。警告（⚠）アイコンが「**GRPC link is not ready (CONNECTING)**」というメッセージと共に表示されます。

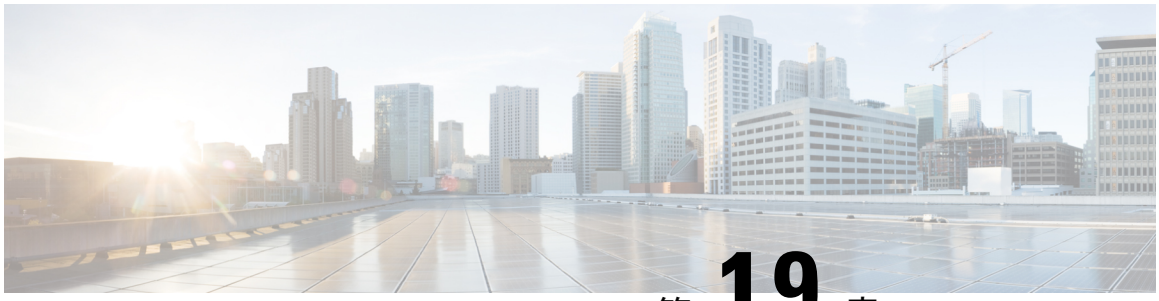


バックグラウンド：AP がインテリジェント キャプチャ データを Cisco DNA Center に送信するためには、eWLC または WLC のインテリジェント キャプチャ ポート番号を 32626 に設定する必要があります。通常、eWLC または WLC が Cisco DNA Center によって検出されると、ポート番号は自動的に 32626 に設定されます。

ただし、Cisco DNA Center のアップグレードパスによっては、ポート番号が適切に設定されない場合があります。

解決策：この問題を解決するには、次の作業を実行します。

1. eWLC または WLC でインテリジェント キャプチャ サーバーのポート番号が 32626 に設定されていることを確認します。
2. ポート番号が 32626 に設定されていない場合は、手動で設定します。



第 19 章

デバイスのパスをトレース

パス トレースについて

ネットワーク内の2つのノード（指定された送信元デバイスと指定された接続先デバイス）間でパストレースを実行できます。2 つのノードは、有線または無線ホスト、レイヤ 3 インターフェイスの組み合わせ、あるいは両方で構成できます。さらに、Cisco DNA Center コントローラがパストレース接続（TCP または UDP）を確立する際に使用するプロトコルを指定できます。

パストレースを開始すると、Cisco DNA Center コントローラは、検出されたデバイスのネットワークトポロジおよびルーティングデータを確認して収集します。Cisco DNA Center コントローラはこのデータを使用して、2 つのホストまたはレイヤ 3 インターフェイス間のパスを計算し、パストレーストポロジにパスを表示します。このトポロジには、パスの方向とパスに沿ったデバイスが含まれ、デバイスの IP アドレスも表示されます。ディスプレイには、パスに沿ったデバイスのプロトコル（**Switched**、**STP**、**ECMP**、**Routed**、**Trace Route**）や、その他のソース タイプも表示されます。

パス トレースの既知の制限事項

パストレースには次の制限事項および制約があります。

- ファブリッククライアントと非ファブリッククライアントの間のパストレースは、サポートされていません。
- 複数の Virtual Routing Forwarding（VRF）仮想ネットワーク（VN）上にある 2 つのファブリッククライアント間のパストレースは、サポートされていません。
- 複数のサイト（ドメイン）上にある 2 つのファブリッククライアント間のパストレースは、サポートされていません。

- いずれかのエッジスイッチがファブリックに含まれていない、同じファブリックの同じサイト内に接続されているクライアントは、サポートされていません。
- ルータのループバック インターフェイスからのパス トレースは、サポートされていません。
- 重複する IP アドレスは、ファブリックの有無にかかわらずサポートされていません。
- パストレースを Locator/ID Separation Protocol（LISP）ファブリックで機能させるには、トラフィックが実行されていて、エッジスイッチでキャッシュを利用できることを確認します。
- Cisco 適応型セキュリティアプライアンス（ASA）は CDP をサポートしていないため、Cisco ASA のパストレースはサポートされていません。Cisco ASA アプライアンスを通るパスを識別することはできません。
- タグなしモードのワイヤレスコントローラの管理インターフェイスでは、パストレースはサポートされていません。
- 集中管理型ワイヤレス モビリティ モードの非対称モビリティ トンネリングに対するパストレースは、サポートされていません。
- 仮想スイッチング システム（VSS）、マルチリンク集約制御プロトコル（MLACP）、または仮想 PortChannel（vPC）のパス トレースはサポートされていません。
- スイッチ仮想インターフェイス（SVI）上の等コスト マルチパス ルーティング（ECMP）のパス トレースは、サポートされていません。
- NAT またはファイアウォールを使用するデバイスでのパストレースはサポートされていません。
- Cisco Performance Routing（PfR）は DMVPN トンネルでサポートされていません。
- VLAN ACL（VACL）が有効になっているパストレースは、サポートされていません。
- 非周期的な更新（NPR）パスシナリオでは、アップグレード後にコントローラでパスは更新されません。また、統計収集が停止します。統計収集を続行するには、新しいパス要求を開始する必要があります。
- Hot Standby Router Protocol（HSRP）VLAN のホストから任意の HSRP ルータに接続されている 非 HSRP VLAN のホストへのパス トレースは、サポートされていません。
- オブジェクト グループは ACL トレースでサポートされていません。
- ポートチャネルのポート集約プロトコル（PAgP）モードは、サポートされていません。LACP モードのみがサポートされています。
- インターフェイスに異なるパフォーマンス モニター ポリシーが設定されている場合は、Cisco DNA Centerを使用したパフォーマンスモニター設定の適用が失敗します。インターフェイスのパフォーマンスモニター設定を削除して、パストレース要求を再送信します。
- パフォーマンスモニター統計情報のパストレースは、Cisco ASR 1000 シリーズルータ（Cisco IOS XE 16.3.1）ではサポートされていません。

- パフォーマンスモニター統計情報のパストレースは、Cisco Catalyst 3850 スイッチ（Cisco IOS XE 16.2.x および 16.3.1）ではサポートされていません。
- Cisco Mobility Express（ME）ワイヤレスコントローラのパストレースはサポートされていません。
- Cisco SD-Access ファブリックで OTT を使用するワイヤレスクライアントのパストレースはサポートされていません。
- レイヤ 2 スイッチからのパストレースはサポートされていません。
- シスコの産業用イーサネット（IE）スイッチは、SD-Access ソリューションの一部として拡張されたノードです。現在、パストレースは拡張ノードを認識していないため、トポロジに拡張ノードが含まれている場合は、エラーメッセージが表示されます。
- デバイス用に IPv4 アドレスと IPv6 アドレスの両方を使用するデュアルスタックはサポートされていません。この状況になると、指定されたアドレスが不明であることを示すエラーメッセージが表示されます。
- シスコ ワイヤレス コントローラは SNMP モビリティトラップを送信しないため、次の点に注意してください。
  - パストレース要求の場合、Cisco DNA Centerの外部ワイヤレスコントローラでは、右側の出力仮想インターフェイスは強調表示されません。
  - パストレース要求では、外部ワイヤレスコントローラに適用されている ACL は強調表示されません。

（注） 回避策は、インベントリサイクルが完了するまで待機することです。

パス トレースの実行

パス トレース機能は、すべてのデバイスで同様の方法で動作します。[Client 360] または [Device 360] ウィンドウからパス トレースを実行できます。

始める前に

- パス トレースの既知の制限事項を確認してください。パス トレースの既知の制限事項（373 ページ）を参照してください。
- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲を使用したネットワークの検出（30 ページ）、CDP を使用したネットワークの検出（23 ページ）、またはLLDP を使用したネットワークの検出（36 ページ）を参照してください。

• デバイスで CDP が有効であることを確認してください。

ステップ 1 [Client 360] または [Device 360] ウィンドウの [Path Trace] カテゴリで、[Run New Path Trace] をクリックします。
[Set up Path Trace] スライドインペインが表示されます。

ステップ 2 送信元の IP アドレス、インターフェイス、およびポート番号、宛先の IP アドレス、インターフェイス、およびポート番号を入力します。

フィールド	アクション
[Source] フィールド	[Source] フィールドの IP アドレスは事前に入力されていますが、次の操作を実行して別の送信元 IP アドレスを入力できます。 • 送信元 IP アドレスを入力します。 • [Source] フィールドをクリックして、使用可能なオプションから IP アドレスを選択します。
[Interface（optional）] フィールド	ドロップダウンリストからインターフェイスを選択します。 （注） 送信元 IP アドレスがネットワーク デバイスの場合は、このフィールドが表示されます。
[Port（optional）] フィールド	トレースを開始するホストのポート番号を入力します。
[Destination] フィールド	次のいずれかを実行します。 • トレースを終了するホストまたはレイヤ 3 転送インターフェイスの IP アドレスを入力します。 • [Destination] フィールドをクリックして、使用可能なオプションから IP アドレスを選択します。
[Interface（optional）] フィールド	ドロップダウンリストからインターフェイスを選択します。 （注） [Destination] フィールドで選択した IP アドレスがネットワーク デバイスの場合、このフィールドが表示されます。
[Port（optional）] フィールド	トレースを終了するホストのポート番号を入力します。

ステップ 3 [Options] エリアで、必要に応じて次の操作を実行します。

フィールド	アクション
[Protocol] ドロップダウンリスト	（オプション）[tcp] または [udp] を選択します。

フィールド	アクション
[Live Traffic]	[On] に切り替えて有効にすると、選択したデバイスを通過するネットワークパケットを .pcap ファイルとしてリアルタイムでキャプチャできます。 [Max number of packets to capture] ドロップダウンリスト：キャプチャするパケットの最大数を選択します。 （注） [Live Traffic] トグルボタンを有効にすると、[Refresh Every 30sec] トグルボタンが自動的に無効になります。その逆も同様です。
[Refresh Every 30sec]	（オプション）パストレーストポロジを30秒ごとに更新するように設定するには、このトグルを [On] に設定します。
[ACL Trace]	（オプション）一致したACLと特定のトラフィックフローのACL結果（許可または拒否）を表示するには、このトグルを [On] に設定します。
[Include Stats] オプション	（オプション）追加の統計を収集するようにパス トレースを設定するには、必要に応じて次のチェック ボックスをチェックします。 • [Device]：デバイス CPU やメモリ使用率などの情報を収集して表示します。 • [Interface]：デバイスインターフェイスに関する情報を収集して表示します。 • [QoS]：collector-voice-egress、collector-broadcast-video-egress、collector-real-time-interactive-egress などの QoS 情報を収集して表示します。

ステップ 4 [Start] をクリックします。
パス トレース トポロジが表示されます。IP アドレス、プロトコル、およびパス トレースの最終更新日時を示すタイムスタンプが、トポロジの上に表示されます。

ステップ 5 パストレーストポロジでは、次の操作を実行できます。

a) デバイスにカーソルを合わせると、CPU 使用率、メモリ使用率、およびパケット転送の決定（トレースタイプ、転送、および差異を含む）が表示されます。

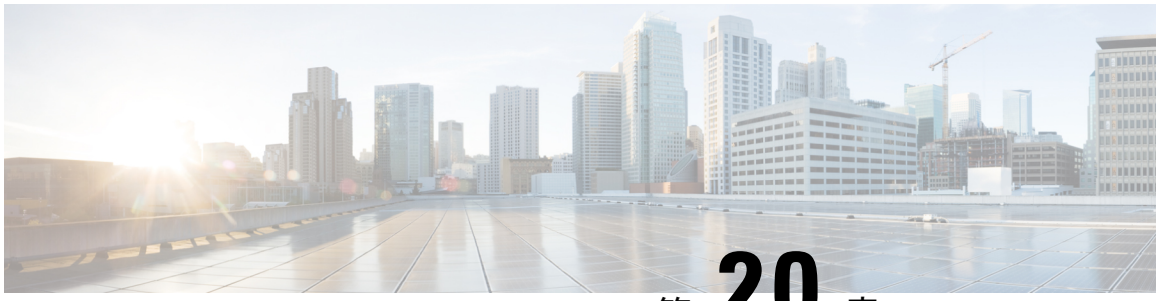
[ACL Trace] が [On] に設定されている場合、ACL 名と ACL の結果（許可または拒否など）が表示されます。

次の 5 タプル値（送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、使用されているプロトコル）が指定されている場合、表示されている ACL トレースは 100% 正確です。情報が部分的に指定されている場合、表示されているACLトレースはベストエフォートに基づきます。このような場合、ACL 結果に許可と拒否の両方が表示される可能性があります。

特定のトラフィック フローで一致したACLは、色付きのアイコンで表示されます。緑は許可を示します。赤は拒否を示します。入力 ACL の場合、アイコンはデバイスの左側に表示されます。出力 ACL の場合、アイコンはデバイスの右側に表示されます。

b) デバイスをクリックすると、デバイスの詳細情報を含むスライドインペインが開きます。

c) レイヤ 2 または レイヤ 3 ポート チャネル インターフェイスの上にカーソルを重ねると、使用された VLAN や出力ドロップなどの情報が表示されます。[More Details] をクリックすると、追加情報を含むスライドインペインが開きます。
d) パスの上にカーソルを重ねると、パスに沿ったデバイスのプロトコル（Switched、STP、ECMP、Routed、Trace Route）や、その他のソース タイプも表示されます。



第 20 章

ワイヤレスマップ向け Cisco CMX の統合

Cisco Connected Mobile Experiences の統合について

Cisco DNA Center は、ワイヤレスマップのためのオンプレミス コネクテッド モバイル エクスペリエンス（CMX）の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディングレベルで、大企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX API サーバーへのユーザーの追加

Cisco CMX インスタンスを Cisco DNA Center ネットワーク設定に追加する前に、Cisco CMX API サーバーにユーザーを追加する必要があります。

ステップ 1 cmxadmin アカウントを使用して Cisco CMX に SSH 接続します。次のコマンドを入力します。

```
ssh -l cmxadmin (cmx-ip-address)
```

ステップ 2 Cisco CMX API サーバーを起動します。次のコマンドを入力します。

```
# cmxos apiserver start
```

Example

```
The following example shows how to start the Cisco CMX API server:
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

ステップ 3 Cisco CMX API サーバーへのユーザーの追加次のコマンドを入力します。

```
cmxos apiserver user add
```

パスワード プロンプトが表示されたら、Cisco CMX Web 管理画面のユーザー パスワードと同じパスワードを入力します。

Example

```
The following example shows how to add a user for the Cisco CMX API server:
[root@server]# cmxos apiserver user add
Please enter the userid for the CMX API Server: user1
Please enter the password for the CMX API Server: password
Please re-enter the password for the CMX API Server: password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

次のタスク

Cisco DNA Center で Cisco CMX の設定を作成します。Cisco CMX 設定の作成 （380 ページ）を参照してください。

Cisco CMX 設定の作成

始める前に

Cisco CMX API ユーザーを追加します。Cisco CMX API サーバーへのユーザーの追加 （379 ページ）を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。

結果：[DNA Spaces/CMX Servers] ウィンドウが表示されます。

ステップ 3 [CMX Servers] テーブルから、[Add] をクリックします。

ステップ 4 [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address]：CMX Web GUI の有効な IP アドレスを入力します。
- [User Name]：CMX Web GUI のユーザー名を入力します。
- [Password]：パスワードログイン情報を入力します。

- [SSH User Name]：CMX 管理者のユーザー名を入力します。
- [SSH Password]：CMX 管理者のパスワードログイン情報を入力します。

（注）　CMX が到達可能であることを確認してください。

ステップ 5　[Add]をクリックします。

結果：CMX サーバーが正常に追加されました。

ステップ 6　CMXサーバーをサイト、建物、またはフロアに割り当てるには、[Menu]アイコンをクリックし、**[Design]**>**[Network Settings]** の順に選択します。

ステップ 7　[Wireless] タブをクリックします。

ステップ 8　左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。

ステップ 9　[DNA Spaces/CMX Servers] セクションで、ドロップダウンリストを使用して、CMX サーバーを選択します。

ステップ 10　**[Save]** をクリックします。

結果：[Create CMX Settings] ページが表示されます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

ステップ 11　フロアマップでは、次のことを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] タブで表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアント デバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイド バーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

ステップ 12　変更を加えたときにCMXがダウンした場合は、手動で同期する必要があります。同期するには、[Network Hierarchy] ページで、左側のツリーペインで変更を加えた建物やフロアの隣にある省略記号 ••• の上にカーソルを置き、[Sync: DNA Spaces/CMX] を選択して、変更を手動でプッシュします。

ステップ 13　CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) メニューアイコン（≡）をクリックして、**[System]** > **[Settings]**の順に選択します。
b) [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。
c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
d) 削除する CMX サーバーを選択し、[Delete] をクリックします。

e) [OK] をクリックして削除を実行します。

Cisco CMX のトラブルシューティング

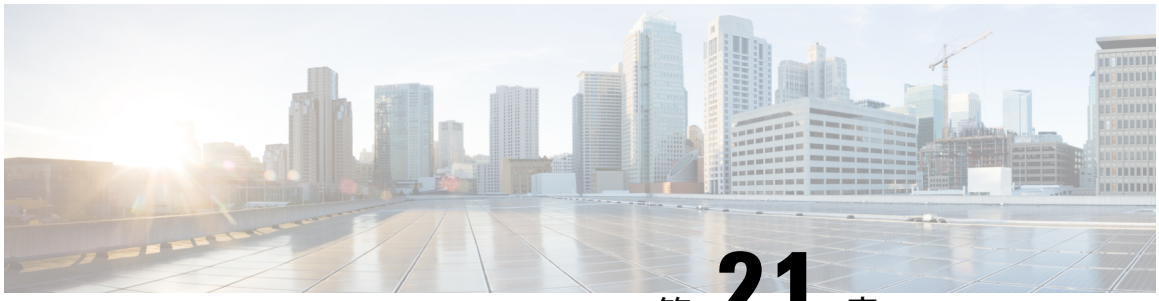
CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web UI にログインできるかどうかを確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX UI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

クライアントがフロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブであるかどうか確認します。
- CMX UI がフロア マップにクライアントを表示するかどうか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```



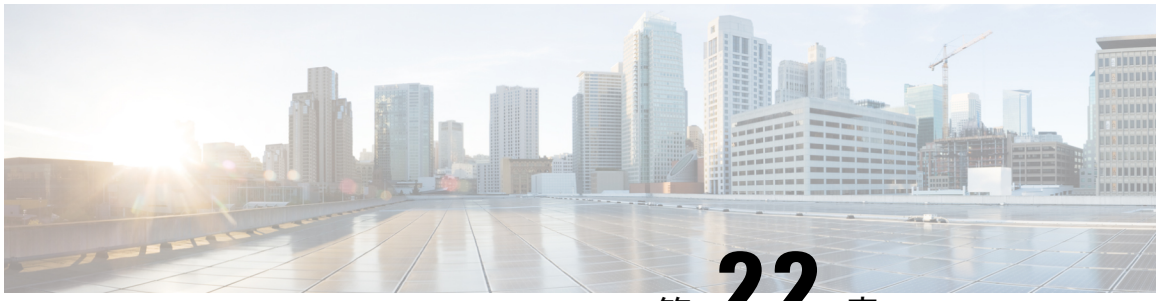
第 21 章

レポート

レポートの概要

レポート機能のデータを使用すると、ネットワークとその動作に関する洞察を得ることができます。このデータがいくつかの形式でレポートされることと、柔軟なスケジューリングおよび設定オプションが提供されることにより、データとレポートの両方を運用上のニーズに合わせて容易にカスタマイズできます。

Cisco DNA Center レポートの詳細については、『Cisco DNA Center Platform User Guide』を参照してください。



第 22 章

アシュアランス監査ログの表示

監査ログの表示 アシュアランス

監査ログは、設定の変更が要求されたとき、設定の変更が実行されたとき、設定中にエラーが発生したかどうかなどの重要なアクティビティを記録するために作成されます。アシュアランスでは、インテリジェントキャプチャ、問題のしきい値、センサー、および AI ネットワーク分析の設定が変更されると、監査ログが提供されます。

Cisco DNA Center の GUI を使用して監査ログにアクセスするには、メニューアイコン（☰）をクリックし、**[Activity]** > **[Audit Logs]** の順に選択します。詳細な手順については、*Cisco DNA Center* 管理者ガイドの「監査ログの表示」を参照してください。

アシュアランスでは、次のデータが監査ログにキャプチャされます。

表 *22 :* 監査ログ

アイテム	説明
Date and Time	ログが受信または実行された日時。
Description	監査ログについて簡単な説明。
User	変更を要求または実行したユーザー。

インテリジェントキャプチャの監査ログ

インテリジェントキャプチャについては、次の設定変更をキャプチャするために監査ログが提供されます。

- AP 統計情報のグローバルな有効化/無効化。
- 一連の個々の AP に関する統計情報の有効化/無効化。
- 異常キャプチャのグローバルな有効化/無効化。

- 一連の個々の AP についての異常キャプチャの有効化/無効化。
- スペクトラム解析の有効化。
- スケジュールされたキャプチャの有効化/無効化。
- ライブキャプチャの有効化/無効化。
- データパケットキャプチャの有効化/無効化。

また、設定中にエラーが発生した場合は、その情報も監査ログに記録されます。

問題のしきい値の監査ログ

問題のしきい値については、次の更新をキャプチャするために監査ログが提供されます。

- サイトの正常性の更新。
- 正常性スコアの更新。
- 問題設定の更新。

センサー監査ログ

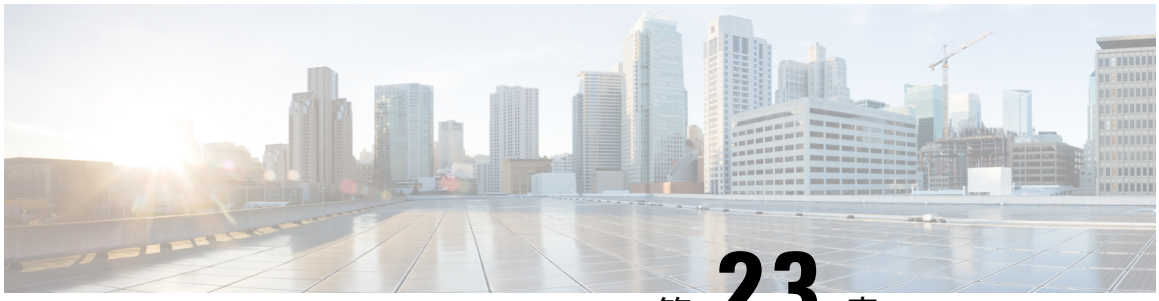
センサーについては、次の設定要求をキャプチャするために監査ログが提供されます。

- テストスイートの追加要求を受信。
- テストスイートの更新要求を受信。
- テストスイートの削除要求を受信。
- 証明書バンドルに関するテストの更新要求を受信。
- テストステータスの追加要求を受信。

AI 分析の監査ログ

AI 分析については、次の AI エージェントの設定変更をキャプチャするために監査ログが提供されます。

- エージェントのオンボード。
- エージェントの復元。
- エージェントの再設定。



第 23 章

関連資料

関連資料

Cisco DNA Center の参照ドキュメントとして以下をお勧めします。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

情報のタイプについては、	このドキュメントを参照してください...
リリース情報（新機能、制限事項、未解決および解決済みのバグなど）。	Cisco DNA Center リリースノート
Cisco DNA Center のインストールと設定（設置作業を含む）について。	Cisco DNA Center 設置ガイド
Cisco DNA Center の最新リリースに関するアップグレード情報。	Cisco DNA Center アップグレードガイド
Cisco DNA Center GUI とアプリケーションの使用について。	Cisco DNA Center ユーザガイド
ユーザアカウント、セキュリティ証明書、認証およびパスワードポリシー、バックアップと復元の設定について。	Cisco DNA Center 管理者ガイド
セキュリティの機能、強化、ベストプラクティスを通じて安全に展開する方法について。	Cisco DNA Center セキュリティのベストプラクティスガイド

関連資料

情報のタイプについては、	このドキュメントを参照してください...
サポートされているデバイスについて（ルータ、スイッチ、ワイヤレスアクセスポイント、 ソフトウェアリリースなど）。	サポートされるデバイス
Cisco SD-Access 向けハードウェアおよびソフトウェアのサポートについて。	Cisco SD-Access ハードウェアおよびソフトウェア互換性マトリックス
Cisco DNA アシュアランス GUI の使用について。	Cisco DNA Assurance ユーザガイド
Cisco DNA Center プラットフォーム GUI とアプリケーションの使用について。	Cisco DNA Center プラットフォーム ユーザガイド
Cisco DNA Center プラットフォーム リリース情報（新機能、展開、バグなど）。	Cisco DNA Center プラットフォーム リリース ノート
Cisco Wide Area Bonjour アプリケーション GUI の使用について。	Cisco Wide Area Bonjour アプリケーション ユーザガイド
Cisco DNA Center での Stealthwatch Security Analytics Service の使用について。	Cisco Stealthwatch Analytics Service ユーザガイド
Cisco DNA Center GUI の Cisco DNA アシュアランス 内のダッシュボードとして不正管理機能を利用する方法について。	Cisco DNA Center の不正管理アプリケーション クイック スタート ガイド

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。