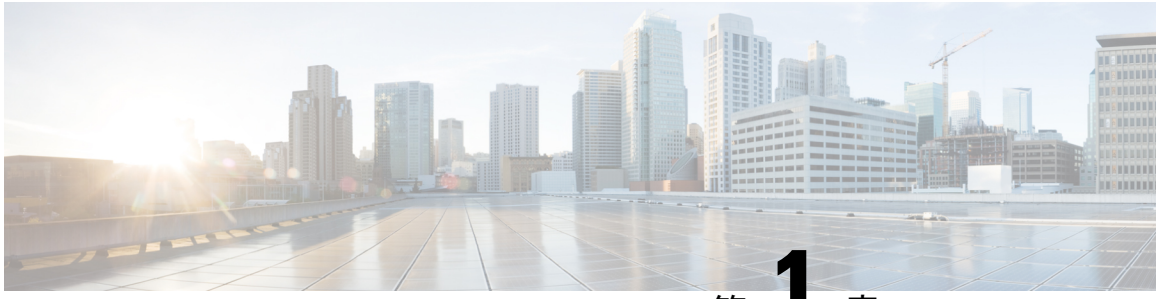
Cisco DNA Assurance リリース 1.3.3.0 ユーザガイド

初版：2020 年 1 月 17 日

最終更新：2020 年 2 月 20 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/

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 1.3.3.0 の新機能

Cisco DNA Assurance ユーザーガイド、リリース *1.3.3.0* に記載された新機能と機能変更の概要を次の表に示します。

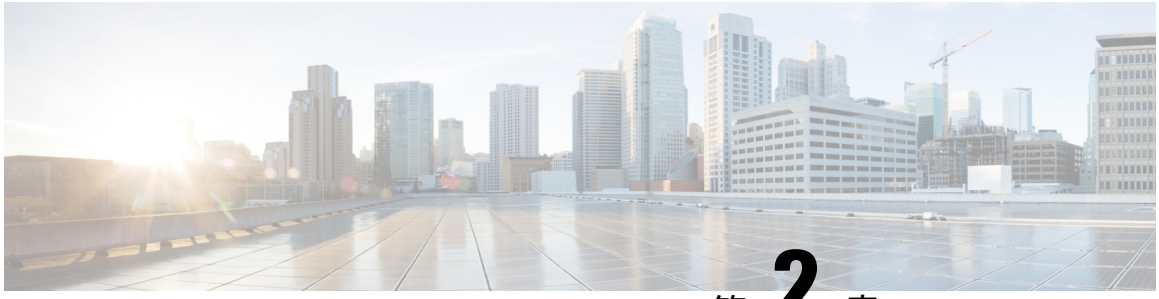
表 *1* : 新機能および変更された機能 *Cisco DNA Assurance*

機能	説明
ネットワークデバイスの正常性スコアの設定	**[Assurance]** > **[Manage]** > **[Health Score Settings]** ウィンドウが新たに追加されました。 ネットワークデバイスで正常性スコアの設定を行うには、このウィンドウを使用します。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。 「ネットワークデバイスの正常性スコアの設定 （119 ページ）」を参照してください。
ワイヤレスクライアントの過剰なオンボード時間の問題に関するトリガー条件	ワイヤレスクライアントの過剰なオンボード時間の問題に関するトリガー条件が追加されました。オンボード時の次のフェーズで制限時間を指定できます。 • AAA 認証 • IP アドレスの取得 トリガー条件を設定するには、**[Assurance]** > **[Manage]** > **[Issue Settings]** ウィンドウに移動します。

機能	説明
ワイヤレスセンサーダッシュボードの変更	ワイヤレス センサー ダッシュボードの更新で、次の点が変更になりました。 • タイムラインが変更され、特定の時間枠で発生したセンサーテストエラーの全体に対する割合が、色分けされたブロックで示されるようになりました。 • 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を表示する [Overall Summary] ダッシュレットが追加されました。 このダッシュレットには、すべてのセンサーで実行されたテストの合計数やテストカテゴリごとのテスト結果の内訳も表示されます。テスト結果に関する詳細情報が、テストカテゴリごとに表示されます。 • [Test Results] ダッシュレットが変更され、[Heatmap View] と [Card View] が追加されました。 [Heatmap View] には、統計カテゴリの上位 5 つのランキングが表示されます。このビューでは、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。 [Card View] では、テスト結果データがカード形式で表示されるため、高レベルのモニタリングや比較が可能です。 ワイヤレス センサー ダッシュボードにアクセスするには、**[Assurance]** > **[Dashboards]** > **[Wireless Sensors]** ウィンドウに移動します。 「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とトラブルシューティング （188 ページ）」を参照してください。
センサー 360 ウィンドウ	特定のワイヤレスセンサーの 360 度ビューを提供する新しいウィンドウが追加されました。このウィンドウでは、センサーのテスト結果、パフォーマンスの傾向、および隣接する 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可能です。 「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とトラブルシューティング （194 ページ）」を参照してください。
センサーテストのテンプレート	センサー主導テストを作成および実行するための新しいメソッドが追加されました。 テンプレートを使用すると、センサー主導テストを再利用して、ネットワーク内の複数のロケーションに迅速に展開できます。 テストテンプレートにアクセスするには、**[Assurance]** > **[Manage]** > **[Sensors]** > **[Test Templates]** ウィンドウに移動します。 「センサー主導テストの作成と実行（テンプレート） （206 ページ）」を参照してください。

機能	説明
センサーのレガシーテスト	メソッドの名が**テストスイート**から**レガシーテスト**に変更されました。 レガシーテストにアクセスするには、**[Assurance]** > **[Manage]** > **[Sensors]** > **[Legacy Tests]** ウィンドウに移動します。 「センサー主導テストの作成と実行（レガシー） （201 ページ）」を参照してください。
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	センサーデバイスに永続的なワイヤレスバックホール接続のサポートが追加されました。これにより、ワイヤレステストのアクティビティに関係なく、ワイヤレス接続が「常にオン」になります。 「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 （199 ページ）」を参照してください。
インテリジェントキャプチャの機能拡張	メニューオプション **[Manage]** > **[Intelligent Capture Settings]** > **[Client]**が、**[Manage]** > **[Intelligent Capture Settings]** > **[Client Schedule Capture]** に変更されました。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 （227 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 セッションの履歴を表示できるようになりました。クライアントの データパケットキャプチャ履歴の表示 （234 ページ）を参照してください。 有効になっている AP がない場合は、[Configure AP Enablement] エリアで AP の有効化を開始できます。すべての AP で AP 統計情報のキャプチャを無効にできます。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 （235 ページ）を参照してください。 スペクトル解析チャートが拡充され、より詳細なデータが提供されるようになりました。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 （240 ページ）を参照してください。
Cisco StackWise Virtual リンク（SVL）のサポート	Cisco Catalyst 9500 シリーズ スイッチに搭載されている Cisco StackWise Virtual のサポートが追加されました。 デバイスの健全性のモニタとトラブルシューティング （110 ページ）およびCisco StackWise Virtual と制限事項について （125 ページ）を参照してください。
有線クライアントの syslog とイベントをイベントビューアで表示	Cisco ISE サーバイベント、スイッチのシステムレベルの syslog、スイッチポートや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イベントビューアに表示されるようになりました。 「Monitor and Troubleshoot the Health of a Client Device （145 ページ）」でイベントビューアのカテゴリを参照してください。

機能	説明
ISSU の強化	一度に大量の問題を解決または無視できます。問題の解決または無視 （275 ページ）を参照してください。 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。この機能がサポートされるのは、インターフェイスがダウンしている場合、ワイヤレスコントローラ/スイッチ/ルータが到達不能な場合、および AP がダウンしている場合です。 「自動問題解決 （277 ページ）」を参照してください。
エグゼクティブ サマリー レポート	エグゼクティブ サマリー レポートをスケジュールして、ネットワークデバイスとクライアントに関する詳細データをキャプチャし、ネットワークパフォーマンスの分析に利用できるようになりました。 「定期レポート （309 ページ）」を参照してください。
Samsung デバイスのサポート	Samsung デバイスのサポートが追加されました。[Detail Information] > [Device Info] タブに、Samsung デバイスの詳細情報（ビルド番号、製造元、国番号、モバイルやタブレットなどのデバイスタイプ、ホストのオペレーティングシステムなど）が表示されます。 「Monitor and Troubleshoot the Health of a Client Device （145 ページ）」を参照してください。
AI ネットワーク分析設定ワークフロー	AI ネットワーク分析 の設定ワークフローがシンプルになりました。 Cisco AI Network Analytics データ収集の設定 （89 ページ）およびCisco AI Network Analytics データ収集の無効化 （92 ページ）を参照してください。



第 2 章

Cisco DNA Assurance の概要

About Cisco DNA Assurance

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

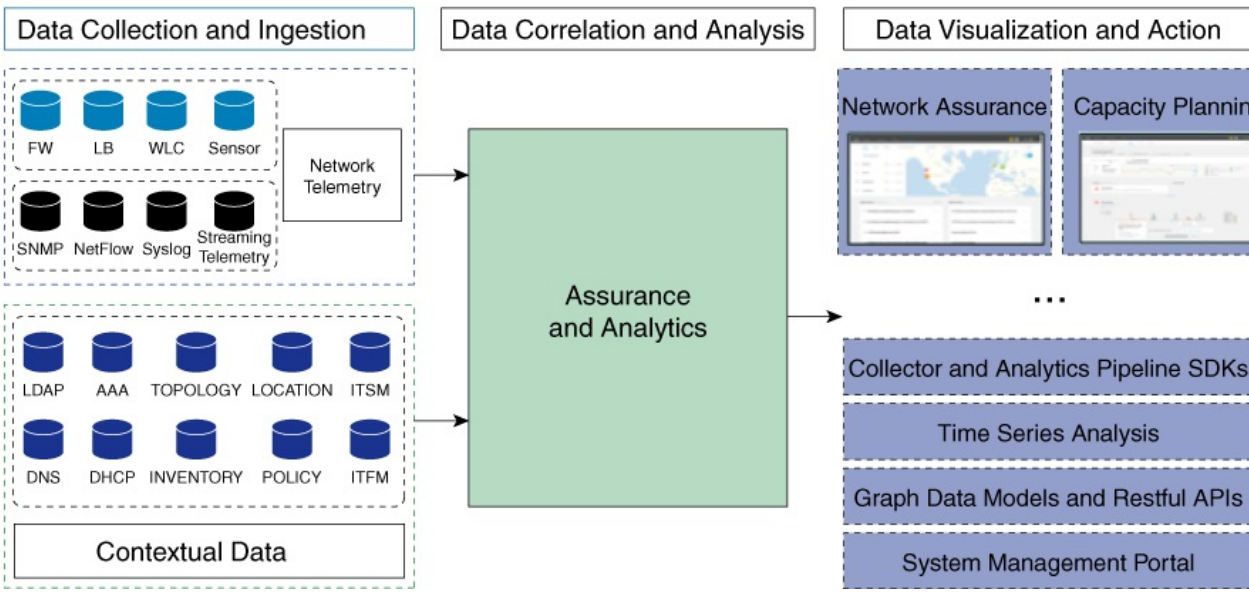
企業は多数のネットワークデータを扱っています。IT組織にとっては、ネットワークデータの量、多様性、速度、および精度への対応が重要です。アシュアランスは、ネットワークデータの問題（ある場合）を処理するために設計されています。

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

ログイン

ブラウザで Cisco DNA Center のネットワーク IP アドレスを入力してアクセスします。互換性のあるブラウザについては、Cisco DNA Center のリリース ノートを参照してください。この IP アドレスで外部ネットワークに接続します。これは、Cisco DNA Center のインストール時に設定されます。Cisco DNA Center のインストールと設定の詳細については、『Cisco Digital Network Architecture Center インストール ガイド』[英語] を参照してください。

ログイン状態を維持するには、Cisco DNA Center を継続的に使用する必要があります。長時間非アクティブ状態が続くと、Cisco DNA Center のセッションから自動的にログアウトします。

ステップ 1 次のフォーマットで、Web ブラウザのアドレスバーにアドレスを入力します。ここで、*server-ip* は Cisco DNA Center をインストールしたサーバの IP アドレス（またはホスト名）です。

https://*server-ip*

例：https://192.0.2.1

ネットワーク構成によっては、ブラウザを更新して Cisco DNA Center サーバのセキュリティ証明書を信頼する必要が生じる場合があります。これを行うと、クライアントと Cisco DNA Center 間の接続のセキュリティが確保されます。

ステップ 2 システム管理者により割り当てられた、Cisco DNA Center のユーザ名とパスワードを入力します。Cisco DNA Center にホーム ページが表示されます。

使用しているユーザ ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じ権限を持つ他のユーザが先にログインしていない場合、ホームページではなく初回セットアップ ウィザードが表示されます。詳細については、ネットワーク管理者として初回ログイン （8 ページ）を参照してください。

ステップ 3 ログアウトするには、右上隅の歯車アイコン（⚙）をクリックし、[Sign Out] をクリックします。

ネットワーク管理者として初回ログイン

使用しているユーザ ID に NETWORK-ADMIN-ROLE が割り当てられていて、同じロールを持つ他のユーザが先にログインしていない場合は、[Get Started] ウィザードにリダイレクトされます。

このウィザードを使用すると、Cisco DNA Center から即時値をすぐに取得できます。これは複数の画面で構成され、ネットワーク デバイスの状況の検出とモニタに必要な情報を収集します。さらに、Cisco DNA Center ホームページ ダッシュ ボードを使用してネットワークの全体的な健全性を視覚化できます。

ウィザードで行うタスクと同じタスクはすべて、その他の Cisco DNA Center の機能で実行できます。ウィザードを使用しても、このような機能を使うことができます。任意の時点でウィザード全体をスキップできます。ウィザードが再び表示されることはありません。ただし、Cisco DNA Center では、同じ権限を持つユーザがこのウィザード手順を完了するまで、このようなユーザのログイン時に同じロールが表示され続けます。ウィザードの完了後は、Cisco DNA Center でウィザードが再度表示されることはありません。

[Get Started] ウィザードをスキップした場合でも、ホームページの右上にある [Get Started] リンクからいつでも再アクセスできます。

始める前に

ウィザードを完了するには、以下の情報が必要です。

- SYSLOG サーバと SNMP サーバの IP アドレス
- Netflow サーバの IP アドレスとポート
- ディスカバリ：開始する IP アドレス（CDP ディスカバリを選択している場合）または開始と終了の IP アドレス（範囲ディスカバリを選択している場合）
- オプション：優先される管理 IP アドレス
- デバイス CLI クレデンシャル（イネーブル パスワードなど）
- SNMP v2c クレデンシャル（read コミュニティ ストリングなど）

ステップ 1 ログイン （7 ページ）の説明に従って、通常の手順で Cisco DNA Center にログインします（まだログインしていない場合）。

初めてログインした場合は、[Get Started] ウィザードにリダイレクトされます。

ステップ 2 [Get Started] ウィザードで [Get Started] をクリックしてデバイスの検出を続行するか、または [Exit] をクリックしてホームページに戻ります。

ステップ 3 デバイス検出のネットワークプロパティを入力し、[Save & Next] をクリックします。

前の画面に戻るには、[Back] をクリックします。

ステップ 4 [Discovery Type]、[Starting IP Address]、および [CLI Credentials] を指定します。

[Device Controllability] はデフォルトで有効になっています。[Disable] をクリックしてデバイス可制御性を無効にすることはできますが、ネットワークデバイスでテレメトリを手動で有効にする必要があります。「デバイスにテレメトリ プロファイルを適用 （166 ページ）」を参照してください。

ステップ 5 完了したら [検出を開始する（Begin Discovery）] をクリックすると Cisco DNA Center にホーム ページが表示されます。ここに、検出が完了するにつれネットワークの健全性情報が徐々に表示されていきます。

デフォルト ホームページ

ログインすると、Cisco DNA Center のホームページが表示されます。ホームページには、主要エリアとして、[Summary]、[Network Snapshot]、[Network Configuration]、および**アシュアランス** [Tools] があります。

[Summary]**アシュアランス** エリアには次の内容が含まれます。

- [Health]：企業全体の正常性スコア（ネットワークデバイス、有線クライアント、ワイヤレスクライアントなど）が提供されます。[View Details] をクリックすると、[Overall Health] ウィンドウが表示されます。
- [Critical Issues]：P1 と P2 の問題の数が表示されます。[View Details] をクリックすると、[Open Issues] ウィンドウが表示されます。
  - [P1]：ネットワーク運用に幅広い影響を与える前に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主要な問題。
- [Trends and Insights]：ネットワークのパフォーマンスに関するインサイトが提供されます。[(View Details] をクリックすると、[Network Insights] ウィンドウが表示されます。

[ネットワーク スナップショット（Network Snapshot）] エリアには次のコンポーネントが含まれます。

- [サイト（Sites）]：ネットワーク上で検出されたサイトの数と、DNS サーバおよび NTP サーバの数が示されます。[Add Sites] をクリックすると、[Add Site] ウィンドウが表示されます。
- [ネットワークデバイス（Network Devices）]：ネットワーク上で検出されたネットワークデバイスの数と、要求されていないデバイス、プロビジョニングされていないデバイス、および到達不能なデバイスの数が示されます。[Find New Devices] をクリックすると、[New Discovery] ウィンドウが表示されます。
- [アプリケーションポリシー（Application policies）]：ネットワーク上で検出されたアプリケーションポリシーの数と、成功およびエラーになった展開の数を表示します。[Add New Policy] をクリックすると、[Application Policies] ウィンドウが表示されます。

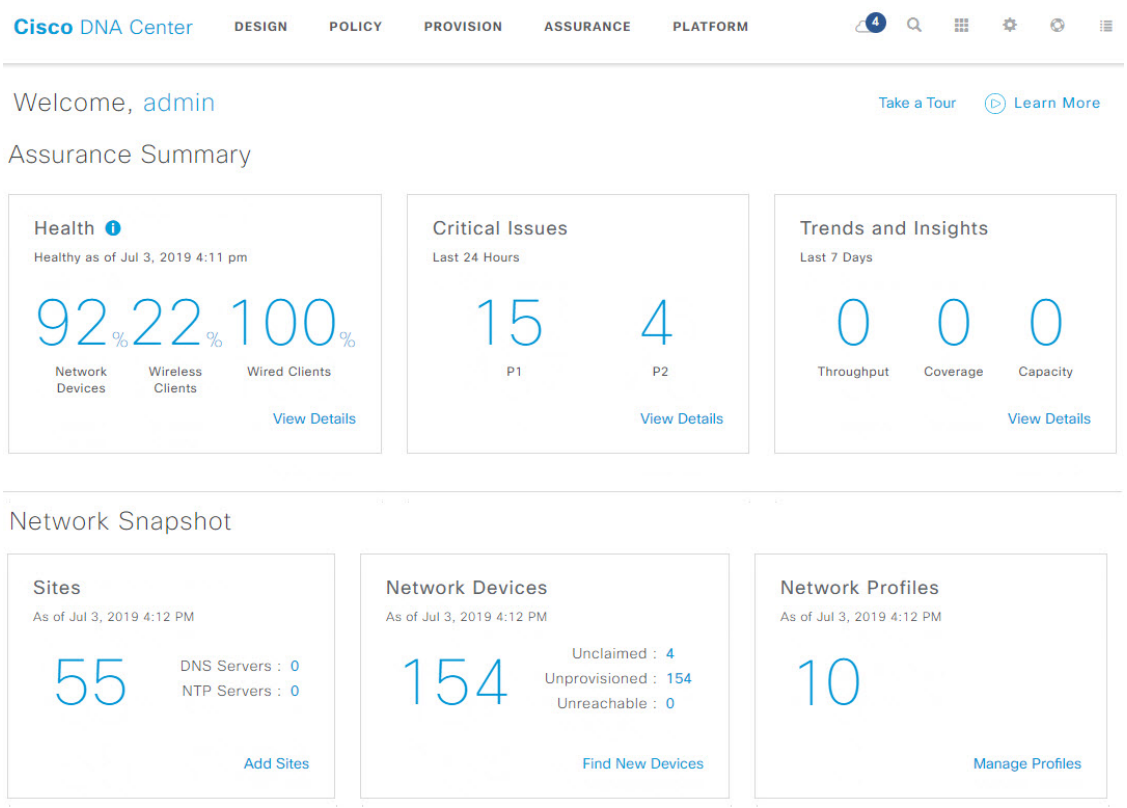
- [ネットワークプロファイル（Network Profiles）]：ネットワーク上で検出されたプロファイルの数を示します。[Manage Profiles] をクリックすると、[Network Profiles] ウィンドウが表示されます。
- [イメージ（Images）]：ネットワーク上で検出されたイメージの数と、タグなしイメージおよび未検証イメージの数が示されます。[Import Images/SMUs] をクリックすると、[Image Repository] ウィンドウが表示されます。
- [Licensed Devices]：Cisco DNA Center ライセンスを持つデバイスの数と、スイッチ、ルータ、およびアクセスポイントの数が示されます。[Manage Licenses] をクリックすると、[License Management] ウィンドウが表示されます。

[Network Configuration] エリアには次の内容が含まれます。

- [設計（Design）]：ネットワーク全体のデバイスに適用できるネットワークの構造とフレームワーク（物理トポロジ、ネットワーク設定、デバイス タイプ プロファイルなど）を作成します。
- [ポリシー（Policy）]：ネットワークの特定の側面（ネットワーク アクセスなど）に対する組織のビジネス目標を反映したポリシーを作成します。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワークデバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。
- [Provision]：デバイスの準備と設定（サイトへのデバイスの追加、デバイスのインベントリへの割り当て、必要な設定とポリシーの展開、ファブリックドメインの作成、ファブリックへのデバイスの追加など）を行います。
- **アシュアランス**：ネットワークインフラストラクチャ、アプリケーション、およびエンドユーザクライアントのパフォーマンスと正常性について、プロアクティブで予測型の実用的洞察を提供します。
- [Platform]：インテント API を使用してネットワークにプログラムでアクセスできます。最適な IT システムと統合してエンドツーエンドのソリューションを作成し、マルチベンダーデバイスのサポートを追加できます。

[ツール（Tools）]：[ツール（Tools）]エリアを使用して、ネットワークを設定および管理します。

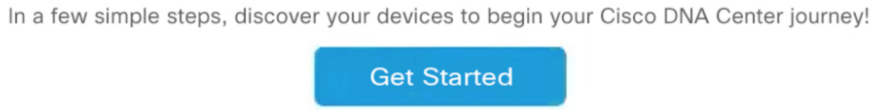
図 *1 : Cisco DNA Center* ホームページ



ホーム ページのさまざまなビュー：

使用する前に

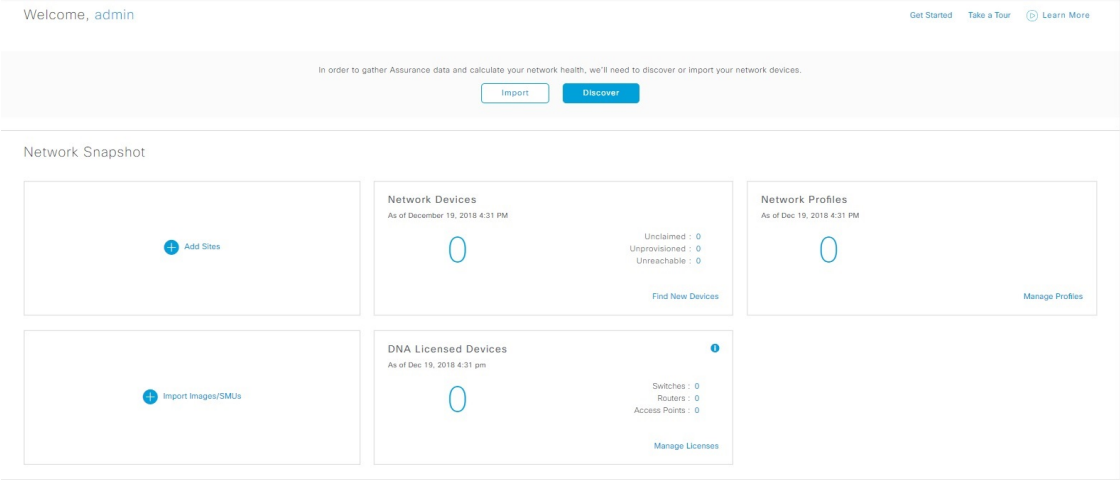
ネットワーク管理者またはシステム管理者として初めて Cisco DNA Center にログインするとき、またはシステムにデバイスが存在しない場合は、次のダッシュレットが表示されます。[Get Started] をクリックして開始ワークフローを完了し、ネットワーク内の新しいデバイスを検出します。



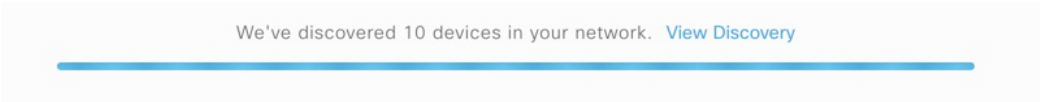
初めてオブザーバとして Cisco DNA Center にログインすると、次のメッセージが表示されます。

0 日目のホームページ

開始をスキップした場合、またはシステム内にデバイスが存在しない場合は、次のホーム ページが表示されます。



検出が進行中の場合は、[ディスカバリ（Discovery）] ウィンドウへのリンクが付いた進捗状況メッセージが表示されます。



システム内にデバイスがある場合は、検出されたデバイスのネットワーク スナップショットが表示されます。

重要な共通タスクを実行するには、ホームページの右上隅にあるアイコンをクリックします。

アイコン	説明
	[Software Updates]：利用可能なソフトウェアアップデートのリストが表示されます。[Go to Software Updates] リンクをクリックすると、システムとアプリケーションのアップデートを表示できます。
	[Search]：デバイス、ユーザ、ホスト、およびその他の項目が保存されている Cisco DNA Center データベース内の任意の場所で、それらを検索します。
	[Tools]：使用可能なツールにアクセスします。
	[Settings]：システム設定の構成、監査ログの表示、ログインしたユーザ名の表示、およびログアウトを行います。

アイコン	説明
	ヘルプ： • [About]： 現在の Cisco DNA Center のソフトウェアバージョンが表示されます。 [Release Notes] をクリックすると、別のブラウザタブでリリースノートが起動します。 [Packages] をクリックすると、システムおよびアプリケーションパッケージのバージョンが表示されます。 [Serial number] をクリックすると、Cisco DNA Center のアプライアンスのシリアル番号が表示されます。 • [API Reference]：Cisco DevNet に Cisco DNA Center プラットフォーム API のドキュメントが開きます。 • [Developer Resources]：開発者ツールにアクセスできる Cisco DevNet が開きます。 • [Help]：状況に応じたオンラインヘルプが、ブラウザの別のタブに表示されます。 • [Contact Support]：Cisco Technical Assistance Center（TAC）でサポートケースが開きます。 • [Make a Wish]：コメントや提案事項が Cisco DNA Center 製品チームに送信されます。
	[Notifications]：最近スケジュールされたタスクやその他の通知が表示されます。 （注） 通知アイコンの横に色のバッジが表示される場合があります。バッジは、タスクまたは通知の変更を示します。青色のバッジは、新しい通知、新しいタスク、または成功したタスクを示します。赤色のバッジは、失敗したタスクを示します。

Cisco DNA Center を初めて使用する場合は、始める アシュアランス （13 ページ） で使い方のヒントや提案を参照してください。

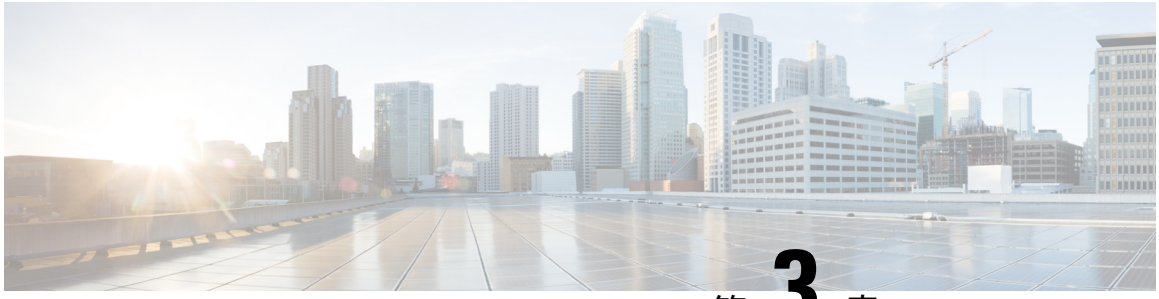
（注） デフォルトでは、入力したログイン名がウェルカムテキストに表示されます。名前を変更するには、名前のリンク（例：**admin**）をクリックします。**[Users]** > **[User Management]** に移動し、表示名を編集できます。

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 **[インベントリ（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 （19 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。



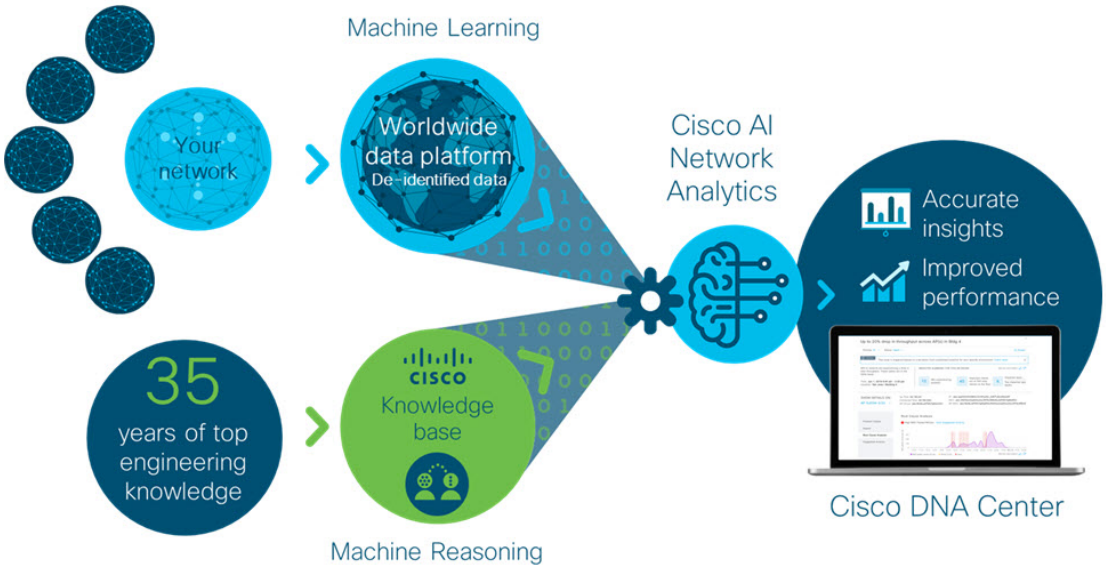
第 3 章

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 2 : *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。

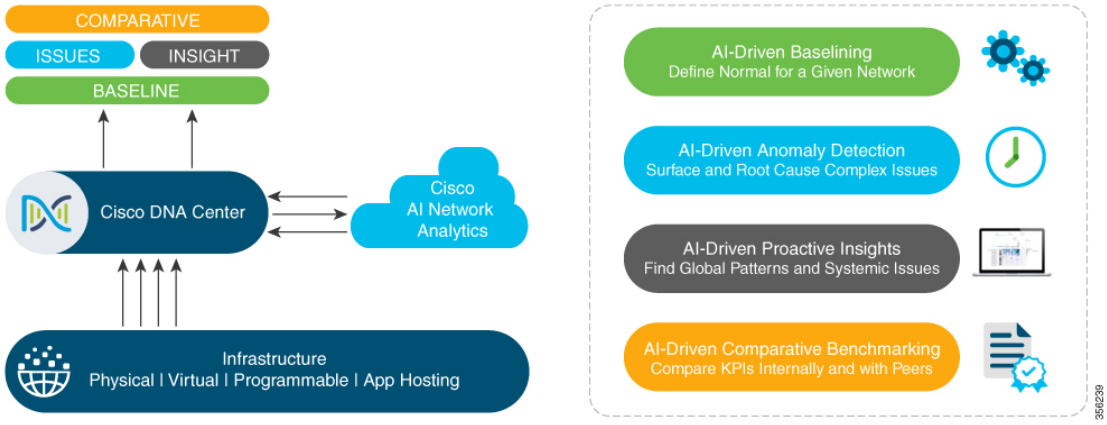
（注） 現在、Cisco AI Network Analytics のユースケースは、AireOS コントローラが稼働するワイヤレス環境でのみサポートされています。

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、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 Assurance 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。

次の図とその後の情報で、Cisco AI Network Analytics の機能について説明します。

図 3 : *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、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

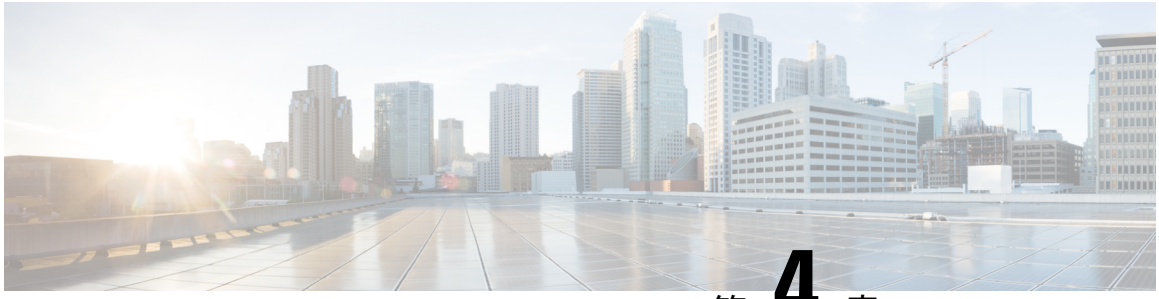
Cisco AI Network Analytics には、次のような利点があります。

- **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、プロキシサーバを介してもサポートされます。HTTPS 接続にプロキシサーバを使用する場合、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 ユーザインターフェイスに直接表示されます。詳細については、https://www.cisco.com/c/en/us/about/trust-center/data-privacy.html で公開されている「Cisco AI Network Analytics Privacy Data Sheet」を参照してください。



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 ガイド と併用してください。

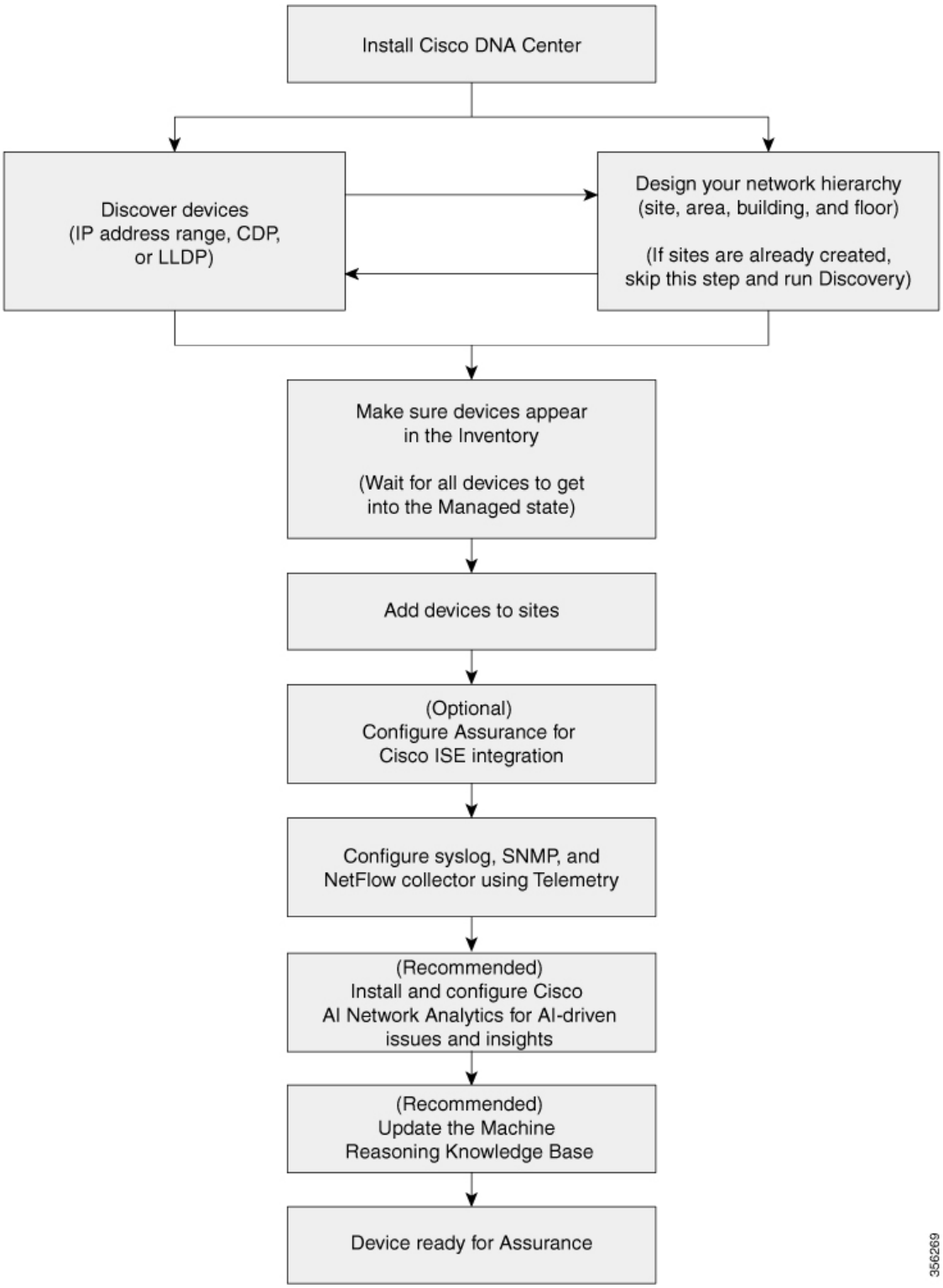
基本的な設定のワークフロー

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。

（注） アシュアランス Cisco DNA Center 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 *4 :* 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



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。

  Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 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 （47 ページ）、ビルディングの追加 （48 ページ）、およびビルディングへのフロアの追加 （48 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 （72 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 （77 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 （49 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 版 Cisco DNA Center の統合の設定 （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 サーバの設定 （82 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 （89 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 （93 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。

Discover Devices

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 Assurance 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 とデバイス間の最大ネットワーク遅延は 100 ミリ秒であることに注意してください（最大遅延は 200 ミリ秒です）。
- 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 2 つの基準のうち、少なくとも 1 つっが満たされる場合、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 （24 ページ）を参照してください。
  - 重要 ディスカバリの実行後にデータを匿名化すると、システムに投入される新規データは匿名になりますが、既存のデータは匿名になりません。

優先管理 IP アドレス

Cisco DNA Center は、デバイスを検出すると、そのデバイスのいずれかの IP アドレスをそのデバイスの優先管理 IP アドレスとしてログに記録します。IP アドレスは、デバイスの組み込み管理のインターフェイスまたは別の物理的インターフェイス、あるいは 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 アドレスとして記録するように 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）。

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場合、Cisco DNA Center は、優先管理 IP アドレスを次のように決定します。

- 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、**[インベントリ（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、Discover Your Network Using an IP Address Range （31 ページ）およびLLDP を使用したネットワークの検出 （37 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 （23 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。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 Cisco DNA Centerのホームページで、[ディスカバリ（Discovery）] をクリックします。

ステップ 2 [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 3 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 （24 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 4 [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、[クレデンシャルの追加（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 2：CLI クレデンシャル

フィールド	説明
名前/説明	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。

フィールド	説明
[パスワードを有効にする（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 *3 : 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 *4 : SNMPv3* のクレデンシャル

フィールド	説明
名前/説明	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。
モード	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。

フィールド	説明
[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。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • **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	DES または 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 プロパティ（SNMP PROPERTIES）] をクリックして、次のフィールドを設定します。

表 *5 : SNMP Properties*

フィールド	説明
リトライ	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。
タイムアウト	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 *6 : HTTPS* クレデンシャル

フィールド	説明
タイプ	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、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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 830 に設定する必要があります。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 5 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 6 [Start] をクリックします。[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。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（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。

Discover Your Network Using an IP Address Range

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 （25 ページ）およびLLDP を使用したネットワークの検出 （37 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 （23 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 Cisco DNA Centerのホームページで、[ディスカバリ（Discovery）] をクリックします。

ステップ 2 [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 3 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) [ディスカバリ タイプ（Discovery Type）] で、[範囲（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 の最初の 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) [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 （24 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 4 [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、[クレデンシャルの追加（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 *7: CLI* クレデンシャル

フィールド	説明
名前/説明	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。
[パスワードを有効にする（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 *8 : 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 *9 : SNMPv3* のクレデンシャル

フィールド	説明
名前/説明	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。
モード	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。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • **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	DES または 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 プロパティ（SNMP PROPERTIES）] をクリックして、次のフィールドを設定します。

表 *10 : SNMP Properties*

フィールド	説明
リトライ	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。

フィールド	説明
タイムアウト	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 *11 : HTTPS* クレデンシャル

フィールド	説明
タイプ	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、[読み取り（Read）] または [書き込み（Write）] です。
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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 830 に設定する必要があります。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。

ステップ 5 （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 6 [Start] をクリックします。[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。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（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 （25 ページ）およびDiscover Your Network Using an IP Address Range （31 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 （23 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。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 Cisco DNA Centerのホームページで、[ディスカバリ（Discovery）] をクリックします。

ステップ 2 [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 3 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、[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 （24 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 4 [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。クレデンシャルを設定する場合は、[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、[クレデンシャルの追加（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 *12 : CLI* クレデンシャル

フィールド	説明
名前/説明	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。
[パスワードを有効にする（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 *13 : 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 *14 : SNMPv3* のクレデンシャル

フィールド	説明
名前/説明	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
モード	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。 • [DES]：CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • **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	DES または 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 プロパティ（SNMP PROPERTIES）] をクリックして、次のフィールドを設定します。

表 *15 : SNMP Properties*

フィールド	説明
リトライ	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。
タイムアウト	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 *16 : HTTPS* クレデンシャル

フィールド	説明
タイプ	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、[読み取り（Read）] または [書き込み（Write）] です。

フィールド	説明
Read	最大 5 つの HTTPS 読み取りログイン情報を設定できます。 • [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 5 つの HTTPS 書き込みログイン情報を設定できます。 • [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 5 （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 6 [Start] をクリックします。[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。

[検出（Discoveries）] ウィンドウにスキャンの結果が表示されます。

[検出の詳細（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。

[検出ジョブの管理（Manage Discovery Jobs）]

ディスカバリ ジョブの停止および開始

ステップ 1 Cisco DNA Centerのホームページで、[ディスカバリ（Discovery）] をクリックします。

ステップ 2 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) **[ディスカバリ（Discoveries）]** ペインで、関連するディスカバリ ジョブを選択します。

b) [Stop] をクリックします。

ステップ 3 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) **[ディスカバリ（Discoveries）]** ペインで、関連するディスカバリ ジョブを選択します。

b) [Re-discover] をクリックして、選択した検出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、そのディスカバリ ジョブ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 Cisco DNA Center のホームページで、**[ディスカバリ（Discovery）]** をクリックします。

ステップ 2 **[ディスカバリ（Discovery）]** ペインで、検出ジョブを選択します。

ステップ 3 [Clone & 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 4 （任意） 検出ジョブの名前を変更します。

ステップ 5 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。

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 Cisco DNA Center のホームページで、**[ディスカバリ（Discovery）]** をクリックします。

ステップ 2 **[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 3 [削除（Delete）] をクリックします。

ステップ 4 [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 Cisco DNA Center のホームページで、**[ディスカバリ（Discovery）]** をクリックします。

ステップ 2 **[ディスカバリ（Discovery）]** ペインで、検出ジョブを選択します。もしくは、**[検索（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 3 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を指定します。
- [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

[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 （22 ページ）」を参照してください。

これらのタスクは、[設計（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。

About Network Hierarchy

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。

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（47 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 （52 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、.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できます。
- 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確認してください。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 複数の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 Cisco DNA Center のホームページから、**[Design]** > **[Network Profiles]** を選択します。

世界のマップが表示されます。

ステップ 2 **[ネットワーク階層（Network Hierarchy）]** ウィンドウで、**[+ サイトの追加（+ Add Site）]** をクリックするか、または左側のペインにある親サイトの隣にある歯車アイコン をクリックして、適切なオプションを選択します。

ステップ 3 サイトの名前を入力し、親ノードを選択します。デフォルトでは、**[グローバル（Global）]** が親ノードです。

ステップ 4 [Add] をクリックします。

左側ペインの親ノードにサイトが作成されます。

既存の階層をアップロードすることもできます。詳細については、「既存のサイト階層をアップロード（52 ページ）」を参照してください。

ビルディングの追加

ステップ 1 Cisco DNA Center のホームページから、**[設計（Design）] > [ネットワーク階層（Network Hierarchy）]** を選択します。

世界のマップが表示されます。

ステップ 2 [ネットワーク階層（Network Hierarchy）] ウィンドウで、[+サイトの追加（Add Site）] をクリックするか、または左側のツリー ペインの親サイトの隣にある歯車アイコン をクリックして、[ビルディングの追加（Add Building）] を選択します。

ステップ 3 既存の階層をアップロードすることもできます。既存のサイト階層をアップロード （52 ページ）を参照してください。

ステップ 4 ビルディングの名前を入力します。

ステップ 5 [アドレス（Address）]テキストフィールドに、アドレスを入力します。インターネットに接続している場合、アドレスを入力すると同時に、設計アプリケーションが、入力されたアドレスを既知のアドレスを絞り込みます。適切なアドレスがウィンドウに表示されたことを確認したら、それを選択します。既知の所在地を選択すると、[経度（Longitude）]および[緯度（Latitude）]の座標フィールドが自動的に設定されます。

ステップ 6 [Add] をクリックします。

左側のメニューの親サイトの下に、作成したビルディングが追加されます。

ステップ 7 別のエリアまたはビルディングを追加するには、階層フレームで、既存のエリアまたは親ノードにしたいビルディングの隣にある歯車アイコン をクリックします。

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、フロアを作成し、フロア マップをアップロードします。

ステップ 1 Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] を選択します。

ステップ 2 [グローバル（Global）]サイトと以前に作成した領域を展開し、以前に作成したすべてのビルディングを確認します。

ステップ 3 フロアを追加するビルディングの横にある歯車アイコン をクリックし、次に[フロアを追加（Add Floor）] をクリックします。

ステップ 4 フロアの名前を入力します。フロア名には21文字の制限があります。フロア名は文字またはハイフン（-）で始める必要があり、最初の文字に続く文字列は、次の 1 つ以上を含めることができます。

- 大文字または小文字、またはその両方

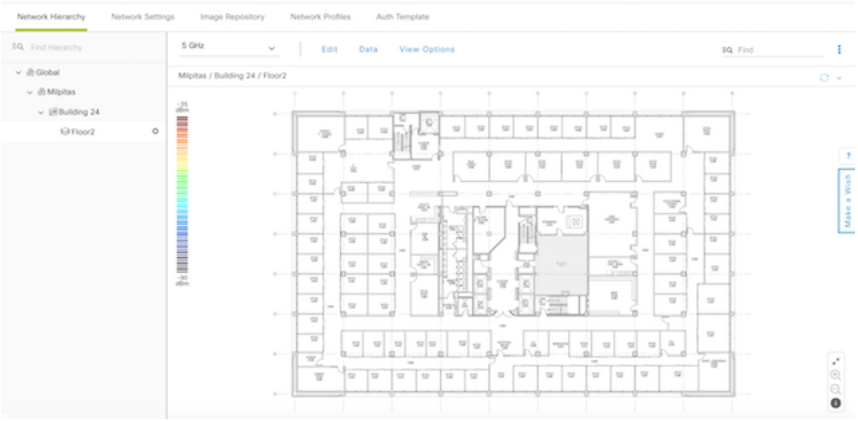
- 数字
- アンダースコア（_）
- ハイフン（-）
- ピリオド(.)
- スペース ( )

ステップ 5 [タイプ（RFモデル）（Type（RF Model））] ドロップダウン リストから無線周波数（RF）モデルを選択して、フロアのタイプを定義します（[屋内天井高（Indoor High Ceiling）]、[屋外オープンスペース（Outdoor Open Space）]、[乾式壁オフィスのみ（Drywall Office Only）]、および [キューブと壁で囲まれたオフィス（Cubes And Walled Offices）]）。これにより、フロアがオープンスペースであるか、乾式壁のオフィスであるかなどを定義します。選択した RF モデルに基づいて、ワイヤレス信号強度、ヒートマップの分布が計算されます。

ステップ 6 フロア プランをマップにドラッグしたり、ファイルをアップロードしたりできます。Cisco DNA Center は、.jpg、.gif、.png、dxf、および .dwg の各ファイル タイプをサポートしています。

マップをインポートした後は、必ず [オーバーレイの可視性（Overlay Visibility）] を [ON] にしてください（[フロア（Floor）]>[表示オプション（View Option）]>[オーバーレイ（Overlays）]）。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。

図 *5*: フロア プランの例



ステップ 7 [追加（Add）] をクリックします。

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。このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値に過ぎません。

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 （22 ページ）」を参照してください。

Cisco DNA Center Cisco DNA Center では、次の 802.11ax AP がサポートされています。

- Cisco Catalyst 9100 アクセスポイント
- Cisco Catalyst 9115 アクセス ポイント
- Cisco Catalyst 9117 アクセス ポイント
- Cisco Catalyst 9120 アクセス ポイント

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [APの追加（Add Aps）] ウィンドウで、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、[選択項目の追加（Add Selected）] をクリックします。または、アクセス ポイントに隣接する [追加（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。

ステップ 6 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 7 新しく追加した AP はフロア マップの右上隅に表示されます。

ステップ 8 [アクセスポイント（Access Points）] の横にある[フロア要素（Floor Elements）] ペインで、 [位置（Position）] をクリックして AP をマップに正しく配置します。

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細（Selected AP Details）] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセスポイントをドラッグすると、その水平（x）と垂直（y）の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセスポイントの詳細が表示されます。[選択したAPの詳細（Selected AP Details）] ウィンドウには、次の情報が表示されます。
  - [3点による位置決め（Position by 3 points）] : フロア マップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
    1. [3ポイントによる位置付け（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。

- [2つの壁による位置決め（Position by 2 Walls）] : フロア マップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。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. [2つの壁による位置付け（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、[距離の設定（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。

   AP が、壁の間の定義された距離に従って自動的に配置されます。

- [AP名（AP Name）] : AP 名を表示します。
- [APモデル（AP Model）] : 選択したアクセス ポイントの AP モデルを示します。
- [MACアドレス（MAC Address）] : MAC アドレスが表示されます。
- [X] : マップの水平の距離をフィートで入力します。
- [Y] : マップの垂直の距離をフィートで入力します。
- [AP高さ（AP Height）] : アクセス ポイントの高さを入力します。
- [プロトコル（Protocol）] : このアクセス ポイントのプロトコル : [802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
- [アンテナ（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。選択しなければ、AP はマップに存在しません。

- [アンテナ画像（Antenna Image）] : AP イメージが表示されます。
- [アンテナの方向（Antenna Orientation）] : [方位角（Azimuth）] と [仰角（Elevation）] の方向を度数で入力します。
- [方位角（Azimuth）] : 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。

  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。

ステップ 9 アクセス ポイントの設定と調整が完了したら、[保存（Save）] をクリックします。

ヒート マップは、AP の新しい位置に基づいて生成されます。

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 （214 ページ）」を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[APの削除（Delete APs）] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

ステップ 11 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、[選択済みの削除（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、[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。
- **クイック フィルタ**を使用して、AP 名、MAC アドレス、モデル、またはコントローラにより検索します。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。

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。詳細については、Prime Infrastructure からマップをエクスポートする方法に関する マップ アーカイブのエクスポート（53 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、Cisco 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 Cisco DNA Center のホームページから、**[Design]** > **[Network Hierarchy]**を選択し、[mport] > [Import Sites] を選択します。

世界地図が右側のペインに表示されます。

ステップ 2 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、**[インポート（Import）]** をクリックして、Cisco Prime Infrastructure グループ CSV ファイルをインポートします。

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 3 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]**をクリックします。

ステップ 4 **[サイト階層アーカイブのインポート（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するか、または、**[クリックして選択（click to select）]** リンクをクリックして、アーカイブ ファイルを参照します。

ステップ 5 **[Save（保存）]** を選択してファイルをアップロードします。

[インポート プレビュー（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、**オンまたはオフ** 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、**オンまたはオフ** 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、[すべて選択（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。

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。

Search the Network Hierarchy

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。ツリー階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

サイトの編集

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左側のツリー ペインで、編集するサイトに移動します。

ステップ 3 サイトの横にある歯車アイコン ⚙ をクリックし、[サイトの編集（Edit Site）] を選択します。

ステップ 4 必要な変更を行って、[更新（Update）] をクリックします。

サイトの削除

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左側のペインで、削除するサイトに移動します。

ステップ 3 対応するサイトの隣にある歯車アイコン ⚙ をクリックし、[サイトの削除（Delete Site）] を選択します。

ステップ 4 削除を確認します。

ビルディングの編集

ステップ 1 **[設計（Design）]** > **[ネットワーク階層（Network Hierarchy）]** を選択します。

ステップ 2 左側のツリー ペインで、編集するビルディングに移動します。

ステップ 3 ビルディングの横にある歯車アイコン ⚙ をクリックし、[ビルディングの編集（Edit Building）] を選択します。

ステップ 4 [ビルディングの編集（Edit Building）] ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

ビルディングの削除

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左側のペインで、削除するビルディングに移動します。

ステップ 3 ビルディングの隣にある歯車アイコン をクリックし、[ビルディングの削除（Delete Building）] を選択します。

ステップ 4 削除を確認します。

（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 Cisco DNA Center のホームページで、[Design] > [Network Hierarchy] を選択します。

ステップ 2 ネットワーク階層を展開して編集するフロアを見つけるか、または左側のペインで [階層の検索（Search Hierarchy）] テキスト フィールドにフロア名を入力します。

ステップ 3 [フロアの編集（Edit Floor）] ダイアログ ウィンドウで必要な変更を加え、[更新（Update）] をクリックします。

フロア マップのモニタリング

[フロア ビュー（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 [検索（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。

フロア要素とオーバーレイの編集

フロア領域で使用できる **[編集（Edit）]** オプションにより、次の操作を実行できます。

- 次のフロア要素を追加、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
  - 障害物
  - ロケーション リージョン
  - Rails
  - 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アクセス ポイントを設置します。このようなカバレッジ領域の中心に設置されたアクセス ポイントからは、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。

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。このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値に過ぎません。

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 （22 ページ）」を参照してください。

Cisco DNA Center Cisco DNA Center では、次の 802.11ax AP がサポートされています。

- Cisco Catalyst 9100 アクセスポイント
- Cisco Catalyst 9115 アクセス ポイント
- Cisco Catalyst 9117 アクセス ポイント
- Cisco Catalyst 9120 アクセス ポイント

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

フロアに割り当てられていないアクセス ポイントが一覧に表示されます。

ステップ 5 [APの追加（Add Aps）] ウィンドウで、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、[選択項目の追加（Add Selected）] をクリックします。または、アクセス ポイントに隣接する [追加（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。

ステップ 6 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 7 新しく追加した AP はフロア マップの右上隅に表示されます。

ステップ 8 [アクセスポイント（Access Points）] の横にある[フロア要素（Floor Elements）] ペインで、 [位置（Position）] をクリックして AP をマップに正しく配置します。

- AP を配置するには、AP をクリックして、フロア マップ上の適切な場所にドラッグアンドドロップします。または、[選択したAPの詳細（Selected AP Details）] ウィンドウで x 座標と y 座標および AP の高さを更新することもできます。マップ上のアクセスポイントをドラッグすると、その水平（x）と垂直（y）の位置が、テキストフィールドに表示されます。選択すると、右ペインにアクセスポイントの詳細が表示されます。[選択したAPの詳細（Selected AP Details）] ウィンドウには、次の情報が表示されます。
  - [3点による位置決め（Position by 3 points）] : フロア マップに 3 つの点を記入し、その点を使用して AP の位置決めができます。手順は次のとおりです。
    1. [3ポイントによる位置付け（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。
  - [2つの壁による位置決め（Position by 2 Walls）] : フロア マップに 2 つの壁を定義し、定義した壁の間に AP の位置決めができます。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. [2つの壁による位置付け（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、[距離の設定（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。

       AP が、壁の間の定義された距離に従って自動的に配置されます。
  - [AP名（AP Name）] : AP 名を表示します。
  - [APモデル（AP Model）] : 選択したアクセス ポイントの AP モデルを示します。
  - [MACアドレス（MAC Address）] : MAC アドレスが表示されます。
  - [X] : マップの水平の距離をフィートで入力します。
  - [Y] : マップの垂直の距離をフィートで入力します。
  - [AP高さ（AP Height）] : アクセス ポイントの高さを入力します。
  - [プロトコル（Protocol）] : このアクセス ポイントのプロトコル : [802.11a/n/ac]、[802.11b/g/n]（ハイパー ロケーション AP の場合）、または [802.11a/b/g/n]。
  - [アンテナ（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。選択しなければ、AP はマップに存在しません。

- [アンテナ画像（Antenna Image）]：AP イメージが表示されます。
- [アンテナの方向（Antenna Orientation）]：[方位角（Azimuth）] と [仰角（Elevation）] の方向を度数で入力します。
- [方位角（Azimuth）]：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。

  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。

ステップ 9 アクセス ポイントの設定と調整が完了したら、[保存（Save）] をクリックします。

ヒート マップは、AP の新しい位置に基づいて生成されます。

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 （214 ページ）」を参照してください。

ステップ 10 [アクセス ポイント（Access Points）] の横にある [フロア要素（Floor Elements）] パネルで、[削除（Delete）] をクリックします。
[APの削除（Delete APs）] ウィンドウには、割り当てられて、配置されたアクセス ポイントすべてを一覧表示します。

ステップ 11 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、[選択済みの削除（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、[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。
- **クイック フィルタ** を使用して、AP 名、MAC アドレス、モデル、またはコントローラにより検索します。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。

- [情報（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ネイバー（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「*Monitor and Troubleshoot the Health of a Device*」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 AP 1800S 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「*Provision the Wireless Cisco Aironet 1800s Active Sensor*」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。AP 1800S 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 サーバと直接通信します。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 フロア プランの上にある [編集（Edit）] をクリックします。

ステップ 4 [センサー（Sensors）] の横にある [フロア要素（Floor Elements）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [Add Sensors] ウィンドウで、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。

ステップ 6 フロア マップへセンサーを割り当てたら、[センサーの追加（Add Sensors）] ウィンドウを閉じます。
新しく追加したセンサーはフロア マップの右上隅に表示されます。

ステップ 7 センサーを正しく設定するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[位置（Position）] をクリックして、マップに正しくセットします。

ステップ 8 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 9 センサーを削除するには、[センサー（Sensors）] の横にある [フロア要素（Floor Elements）] ペインで、[削除（Delete）] をクリックします。
[Delete Sensors] ウィンドウには、割り当てられて設定されたすべてのセンサーが一覧表示されます。

ステップ 10 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。[削除（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 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 [オーバーレイ（Overlays）] パネルで、[カバレッジエリア（Coverage Areas）] の横にある [追加（Add）] をクリックします。
[カバレッジの作成（Coverage creation）] ダイアログボックスが表示されます。

ステップ 5 カバレッジ領域を描画するには、[タイプ（Type）] ドロップダウンリストから、[カバレッジエリア（Coverage Area）] を選択します。

1. 定義するエリアの名前を入力し、[カバレッジを追加（Add Coverage）]をクリックします。カバレッジエリアは、頂点が3つ以上の多角形でなければなりません。
2. 輪郭を描く領域に描画ツールを移動します。
3. このツールをクリックして、描線を開始および停止します。
4. エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

（注） マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 6 多角形領域を描画するには、[タイプ（Type）] ドロップダウンリストから、[周辺（Perimeter）] を選択します。

1. 定義する領域の名前を入力し、[Ok] をクリックします。
2. 輪郭を描く領域に描画ツールを移動します。
   - このツールをクリックして、描線を開始および停止します。
   - エリアの輪郭を描いてからダブルクリックすると、そのエリアがページ上で強調表示されます。

ステップ 7 カバレッジ領域を編集するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [編集（Edit）]をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 8 変更を加え、変更後に [保存（Save）] をクリックします。

ステップ 9 カバレッジ領域を削除するのには、[オーバーレイ（Overlays）]パネルで、[カバレッジエリア（Coverage Areas）] の横にある [削除（Delete）] をクリックします。

使用可能なカバレッジ領域がマップ上で強調表示されます。

ステップ 10 カバレッジ エリアにマウス カーソルを合わせ、クリックして削除します。

ステップ 11 削除後に [保存（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 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 [障害（Obstacles）] の横にある [オーバーレイ（Overlays）] パネルで、[追加（Add）] をクリックします。

ステップ 5 [障害を作成（Obstacle Creation）] ダイアログ ボックスで、[障害のタイプ（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、[厚い壁（Thick Wall）]、[薄い壁（Light Wall）]、[重い扉（Heavy Door）]、[軽い扉（Light Door）]、[キュービクル（Cubicle）]、および [ガラス（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 [障害物の追加（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 エリアの輪郭を描いてからダブルクリックすると、そのエリアが強調表示されます。

ステップ 10 表示される [障害の作成（Obstacle Creation）] ウィンドウで [完了（Done）] をクリックします。

ステップ 11 [保存（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、[障害（Obstacles）] の隣にある [オーバーレイ（Overlays）] パネルで、[編集（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、[保存（Save）] をクリックします。

ステップ 14 障害を削除するには、[障害（Obstacles）] の隣にある [オーバーレイ（Overlays）] パネルで、[削除（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 **[保存 (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 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

ステップ 2 左ペインで、フロアを選択します。

ステップ 3 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 4 **[ロケーション リージョンの作成（Location Region Creation）]** ダイアログ ウィンドウで、**[包含タイプ（Inclusion Type）]** ドロップダウン リストからオプションを選択します。

ステップ 5 **[位置領域の追加（Add Location Region）]** をクリックします。

包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 6 包含領域の定義を開始するには、描画ツールをマップ上の開始ポイントに移動して、1回クリックします。

ステップ 7 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。

再びクリックすると、次の境界線を定義できます。

ステップ 8 領域の輪郭が描画されるまでステップ 7 を繰り返したら、描画アイコンをダブルクリックします。

水色の実線によって包含領域が定義されます。

ステップ 9 **[保存 (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 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[追加（Add）]** をクリックします。

ステップ 5 **[ロケーション リージョンの作成（Location Region Creation）]** ウィンドウで、**[除外タイプ（Exclusion Type）]** ドロップダウン リストから値を選択します。

ステップ 6 [ロケーションリージョン（Location Region）] をクリックします。

除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 除外領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8 除外するエリアの境界に沿って描画アイコンを移動させます。

1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9 エリアの輪郭が描画されるまで前の手順を繰り返したら、描画アイコンをダブルクリックします。定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。

ステップ 10 さらに除外領域を定義するには、手順 5 から手順 9 を繰り返します。

ステップ 11 すべての除外領域が定義されている場合は、**[保存（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 **[オーバーレイ（Overlays）]** パネルで、**[ロケーションリージョン（Location Regions）]** の横にある **[編集（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、**[保存（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 **[オーバーレイ（Overlays）]**パネルで、**[ロケーション リージョン（Location Regions）]** の横にある **[削除（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、**[削除（Delete）]** をクリックします。

ステップ 3 **[保存 (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）からモニタされる距離を表します。

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 **[レール（Rails）]** の横にある **[オーバーレイ（Overlays）]** パネルで、**[追加（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）を入力して [レールの追加（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 **[保存 (Save)]** をクリックします。

ステップ 9 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[編集（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、[保存（Save）] をクリックします。

ステップ 11 **[オーバーレイ（Overlays）]** パネルで、**[レール（Rails）]** の横にある **[削除（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、クリックして削除します。

ステップ 13 **[保存 (Save)]** をクリックします。

マーカーの配置

ステップ 1 Cisco DNA Center のホームページで、**[Design]** > **[Network Hierarchy]** の順に選択します。

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 **[編集（Edit）]** をクリックします。

ステップ 4 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[追加（Add）]** 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 5 マーカーの名前を入力し、[マーカーの追加（Add Marker）] をクリックします。

ステップ 6 描画アイコンをクリックし、マーカーをマップ上に配置します。

ステップ 7 **[Save（保存）]** をクリックします。

ステップ 8 [オーバーレイ（Overlays）] パネルで、[マーカー（Markers）] の横にある [編集（Edit）] をクリックします。

使用可能なマーカーがマップ上で強調表示されます。

ステップ 9 変更を加えて、[保存（Save）] をクリックします。

ステップ 10 **[オーバーレイ（Overlays）]** パネルで、**[マーカー（Markers）]** の横にある **[削除（Delete）]** をクリックします。

使用可能なすべてのマーカーがマップ上で強調表示されます。

ステップ 11 削除するマーカーの上にマウスのカーソルを合わせ、クリックして削除します。

ステップ 12 **[保存 (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 **[オプションを表示（View Options）]** をクリックします。フロア マップと **[アクセス ポイント（Access Points）]**、**[センサー（Sensor）]**、**[オーバーレイ オブジェクト（Overlay Objects）]**、**[マップ プロパティ（Map Properties）]**、および **[グローバル マップ プロパティ（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、[アクセスポイント（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 ポイントの横にある [オン（On）]/[オフ（Off）] ボタンをクリックして、アクセス ポイントをマップ上に表示します。[アクセスポイント（Access Points）] パネルを展開して、次の設定を行います。

- [表示ラベル（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。
  - [なし（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。
  - [名前（Name）]：AP 名。
  - [AP MAC アドレス（AP MAC Address）]：AP の MAC アドレス。
  - [コントローラIP（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。
  - [無線 MAC アドレス（Radio MAC Address）]：無線 MAC アドレス。
  - **[IP Address]**
  - [チャネル（Channel）]：Cisco Radio のチャネル番号または [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
  - [カバレッジホール（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 [使用不可（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。
  - [送信電力（TX Power）]：現在の Cisco Radio の送信電力レベル（1 が高い）または [使用不可（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。1000 シリーズの AP では 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。

- [チャネルおよび送信電力（Channel and Tx Power）]：チャネルと送信電力レベルまたは [使用不可（Unavailable）]（アクセス ポイントが接続されていない場合）。
- [使用率（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。
- [送信使用率（Tx Utilization）]：指定されたインターフェイスの送信（Tx）使用率。
- [受信使用率（Rx Utilization）]：指定されたインターフェイスの受信（Rx）使用率。
- [チャネル使用率（Ch Utilization）]：指定されたアクセス ポイントのチャネル使用率。
- **関連付けられたClients**）]：関連付けられたクライアントの総数。
- [デュアルバンド無線（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。
- [ヘルス スコア（Health Score）]：AP のヘルス スコア。
- **問題数**
- **カバレッジの問題**
- **APダウンの問題**

- [ヒートマップ タイプ（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。[ヒートマップ タイプ（Heatmap Type）] ドロップダウンリストから、ヒートマップのタイプ（[なし（None）] または [カバレッジ（Coverage）]）を選択してください。
  - **None**
  - [カバレッジ（Coverage）]：フロア プランにモニタ モード アクセス ポイントがある場合は、カバレッジ ヒートマップを選択できます。カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。
- [ヒートマップの不透明度（%）（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。
- [RSSIカットオフ（dBm）（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。
- [マップの不透明度（%）（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。

AP の詳細はすぐにマップに反映されます。マップ上の AP アイコンにマウス カーソルを合わせると、AP の詳細情報と RX ネイバー情報が表示されます。

View Options for Sensors

[センサー（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。**[センサー（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

展開、 **オーバーレイオブジェクト** これらの設定を構成するパネル。[オン（On）]/[オフ（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**
- ロケーション リージョン
- 障害物
- レール
- **Markers**

マップ プロパティの設定

[マッププロパティ（Map Properties）] パネルを展開して、以下を構成します。

- **[自動更新（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。[自動更新（Auto Refresh）] ドロップダウンリストから、時間間隔（[なし（None）]、[1 分（1 min）]、[2 分（2 mins）]、[5 分（5 mins）]、または [15 分（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

[グローバル マップ プロパティ（Global Map Properties）] パネルを展開し、次のように設定します。

- [測定単位（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 [フィート（Feet）] または [メートル（Meters）] のいずれかに設定します。

データのフィルタリング

アクセスポイントデータのフィルタ処理

右側のペインの [フィルタ（Filters）] パネルの下にある [アクセス ポイント（Access Point）] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。
- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップ上に表示するアクセスポイントの識別子を選択します。
  - アクセス ポイントをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のアクセスポイントを表示するには、表示されたテーブル内でアクセス ポイントのチェック ボックスをオンにし、[マップ上で選択を表示（Show Selected on Maps）] をクリックします。

テーブルの検索結果にマウスカーソルを合わせると、AP の位置がマップ上に線でマークされます。

センサーデータのフィルタ処理

右側のペインの [フィルタ（Filters）] パネルの下にある [センサー（Sensor）] をクリックします。

- 中央のペインでフロア マップの上にあるドロップダウン リストで無線の種類を選択します（**2.4 GHz**、**5 GHz**、または **2.4 GHz および 5 GHz**）。
- クエリを追加するには、[ルールの追加（Add Rule）] をクリックします。
  - マップで表示するセンサーの識別子（名前および MAC アドレス）を選択します。
  - センサーをフィルタリングするパラメータを選択します。
  - テキスト ボックスに、該当するパラメータに固有のフィルタ条件を入力し、[検索（Go）] をクリックします。検索結果が表形式で表示されます。
  - [リストにフィルタを適用（Apply Filters to List）] をクリックして、マップ上でフィルタ結果を表示します。マップ上で特定のセンサーを表示するには、表示されたテーブル内でセンサーのチェックボックスをオンにし、[Show Selected on Maps] をクリックします。

テーブルの検索結果にマウスカーソルを合わせると、センサーの位置がマップ上に線でマークされます。

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（ネットワーク設定がデバイスに存在しない場合）。

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 （23 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、「デバイスの再同期間隔の更新（71 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。

デバイスの再同期間隔の更新

[インベントリ（Inventory）] ウィンドウから、次の方法でデバイスの再同期を設定できます。

- 特定のデバイスのカスタム再同期間隔を有効にして、設定できます。
- すべてのデバイスに設定されている事前設定されたグローバル再同期間隔を有効にすることができます（この設定は、[Settings] > [System Settings] > [Settings] > [Network Resync Interval] ウィンドウで行います）。
- 再同期を無効にすることができます。

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 Cisco DNA Center ホームページで、**[プロビジョニング（Provision）]** をクリックします。

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。

ステップ 2 更新するデバイスを選択します。

ステップ 3 **[アクション（Actions）]** ドロップダウンリストから **[インベントリ（Inventory）]** > **[デバイスの編集（Edit Device）]** の順に選択します。

[デバイスの編集（Edit Device）] ダイアログボックスが表示されます。

ステップ 4 [Resync Interval] タブで、デバイスに設定する再同期オプションのタイプに対応するオプションボタンを選択します。有効な選択肢は [カスタム（Custom）]、[グローバル（Global）]、および [無効化（Disable）] です。

ステップ 5 [カスタム（Custom）] を選択した場合は、[再同期間隔（分単位）] フィールドで、連続するポーリング サイクル間の時間間隔（分単位）を入力します。有効な値は、25 ～ 1,440 分（24 時間）です。

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

[インベントリ（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。

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。

Cisco DNA Center ホームページで、**[プロビジョニング（Provision）]** をクリックします。

[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 *17 : Inventory*

カラム	説明
デバイス名（Device Name）	デバイスの名前。 名前をクリックすると、ダイアログボックスが開き、次の情報が表示されます。 • [Details]：デバイス名、デバイスタイプ、IP アドレス、シリアル番号、ソフトウェアイメージなど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。 （注） 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。 • [Interface]：デバイスのインターフェイスの [Interface Name]、[MAC Address]、および [Status] が表示されます。 • [Stack]：MAC アドレス、ロール、状態、プライオリティが表示されます。 （注） [Stack] タブは、プライマリスタックと複数の下位スタックを構成するスイッチスタックデバイスの場合のみ表示されます。 [Stack] タブには、通常のスタックの [Switch Port] > [Neighbor Port] 列が表示されます。 [Stack] タブには、SVL スタックの [SVL Local] > [SVL Remote] および [Dad Interface Name] 列が表示されます。 • [Run Commands]：デバイスで CLI コマンドを実行するためのコマンドランナーを開きます。 • [View 360]：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。 （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
サポートタイプ	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 Cisco 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、顧客/ビジネスパートナーによって構築され、認定プロセスを通過しています。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して修正を依頼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。 • [Connecting]：Cisco DNA Center がデバイスに接続しています。 • [Reachable]：Cisco DNA Center がデバイスに接続されており、CLI を使用して Cisco コマンドを実行できます。 （注） 失敗は、Cisco DNA Center がデバイスに接続されていますが、CLI を使用して Cisco コマンドを実行できなかったことを示します。この状態は通常、デバイスがシスコデバイスではないことを示します。 • [Authentication Failed]：Cisco DNA Center がデバイスに接続されていますが、デバイスのタイプを判別できません。 • [Unreachable]：Cisco DNA Center がデバイスに接続できません。 （注） デバイスに接続できないのは、ディスカバリ ジョブにクレデンシャルが存在しないか、ディスカバリ ジョブに誤ったクレデンシャルが存在するためである場合があります。これに該当する疑いがある場合は、新しいディスカバリ ジョブを実行し、デバイスの正しいクレデンシャルを指定します。
MAC アドレス	デバイスの MAC アドレス。
[Image Version]	デバイスで現在実行されている Cisco IOS ソフトウェア。

カラム	説明
Platform	シスコ製品の部品番号。
シリアル番号（**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。
デバイス ロール	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。 • 不明 • アクセス • **[Core]** • **[Distribution]** • **[Border Router]**
サイト	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、「About Network Hierarchy （46 ページ）」を参照してください。
最終更新日	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。
デバイス ファミリ	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）。
再同期間隔	デバイスのポーリング間隔。この間隔は、[設定（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]：デバイスログイン情報がデバイスをインベントリに追加した後に変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が発生しています。

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。

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。

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 Cisco DNA Center ホームページで、**[プロビジョニング（Provision）]** をクリックします。

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。

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 [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

サイトにデバイスを追加すると、Cisco DNA Center は Syslog として SNMP トラップ サーバを設定し、Syslog レベル 2 が有効になります。

ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング（Provision）]** をクリックします。
[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 **[保存 (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。

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 リリース 1.3 以降 、Cisco ISE の設定は NCP（ネットワーク制御プラットフォーム）内で一元管理されます。これにより、1 箇所の 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. NCP（ > **[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]**）で Cisco ISE の詳細設定を入力します。
2. Cisco ISE サーバ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。

Cisco ISE 版 Cisco DNA Center の統合の設定

Cisco ISE 版 Cisco DNA Center の統合を設定するには、次の手順を実行します。

始める前に

- Cisco ISE pxGrid サービスを有効にします。
- Cisco ISE の CLI と GUI のユーザアカウントには、同じユーザ名とパスワードを使用する必要があります。
- Cisco DNA Center のバージョンが 1.3 以降であることを確認してください。

（注） Cisco DNA Center は Cisco ISE の内部認証局（CA）を アシュアランス との統合の署名済み証明書として使用します。CA 署名付き証明書を使用するには：

- Cisco DNA Center pxGrid クライアント証明書には、拡張キー使用法（EKU）の拡張子に「クライアント認証」が含まれる必要があります。
- Cisco ISE truststore.jks ファイル内の証明書の発行元である必要があります。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Data Platform]** > **[Collectors]** を選択します。**[コレクタ（Collectors）]** ウィンドウが表示されます。

ステップ 2 [COLLECTOR-ISE] をクリックします。

[COLLECTOR-ISE] ウィンドウが表示されます。

（注） [COLLECTOR-ISE] ウィンドウは読み取り専用モードです。

ステップ 3 [Current Configurations] で、[Click to configure] をクリックします。
[Authentication and Policy Servers] ウィンドウが表示されます。

ステップ 4 Cisco ISE サーバを設定するには、認証サーバとポリシー サーバの設定 （79 ページ）を参照してください。

注目 ISE コレクタの設定は存在するものの、[Authentication and Policy Servers] ウィンドウで Cisco ISE が適切に設定されていない場合は、バナーが表示されます。バナーには、[Authentication and Policy Servers] ウィンドウで Cisco ISE の設定を追加するよう Cisco DNA Center の管理者に指示するメッセージが表示されます。

ステップ 5 （任意）ユーザ ID やデバイスホスト名などの個人識別データを匿名化（スクランブル）するには、次の手順を実行します。

a) ⚙ アイコンをクリックし、**[System Settings]** > **[Settings]** を選択します。
b) [Anonymize Data] をクリックします。
[Anonymize Data] ウィンドウが表示されます。
c) [Enable Anonymization] をクリックします。

（注）
- 匿名化を有効にすると、デバイスでは MAC アドレス、IP アドレスなどの匿名以外の情報を使用した検索機能のみ実行できます。
- Cisco DNA Center リリース 1.2.10 以前で匿名化が有効になっていた場合、その設定は、Cisco DNA Center リリース 1.3 にアップグレードしても維持されます。

注意 [Discovery] を実行する前に、匿名化が有効になっていることを確認します。[Discovery] を実行した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

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 と 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 サーバで Cisco DNA Center を登録します。これには、AAA サーバと 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、次のことを確認します。
  1. ネットワークに Cisco ISE バージョン 2.3 以降を導入した。マルチホスト Cisco ISE を導入している場合は、Cisco ISE 管理ノードと統合している。
  2. Cisco ISEノードで SSH を有効にしている。
  3. Cisco DNA Center と統合する予定の Cisco ISE ホストで pxGrid サービスが有効になっており、ERS サービスが読み取り/書き込み操作に対して有効になっている。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。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 は現在 2 つを超える pxGrid ノードをサポートしていません。

4. Cisco ISE GUI と Cisco ISE シェルのユーザ名とパスワードが同じである。
5. Cisco DNA Center と Cisco ISE の間にプロキシが設定されていない。プロキシサーバが Cisco ISE に設定されている場合、Cisco DNA Center の IP アドレスはそのプロキシサーバをバイパスする必要があります。
6. Cisco DNA Center と Cisco ISE の間にファイアウォールがない。ファイアウォールがある場合は、Cisco DNA Center と Cisco ISE 間の通信を開きます。
7. Cisco DNA Center と Cisco ISE の間の ping が、IP アドレスとホスト名の両方で成功する。
8. Cisco ISE 管理ノード証明書のサブジェクト名または 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。
9. サードパーティ証明書を使用している場合は、証明書の SAN フィールドにすべての IP アドレスが含まれている。
10. Cisco ISE の pxGrid 承認が自動または手動に設定されており、Cisco DNA Center の pxGrid 接続が有効になっている。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]** の順に選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 次の情報を入力して、プライマリ AAA サーバを設定します。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密情報の長さは、最大 128 文字です。

ステップ 4 AAA サーバ（Cisco ISE 以外）を設定するには [Cisco ISE Server] トグルボタンを [Off] 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、[Cisco ISE Server] トグルボタンを [On] に設定し、次の各フィールドに情報を入力します

- [Cisco ISE]：サーバが Cisco ISE サーバであるかどうかを示す設定。[Cisco ISE] トグルボタンをクリックして Cisco ISE を有効にします。
- [Username]：Cisco ISE CLI にログインするために使用する名前。

  （注） このユーザにはスーパーユーザの管理権限が必要です。

- [Password]：CLI ユーザ名に対応するパスワード。
- [FQDN]：Cisco ISE サーバ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 サーバの FQDN は ise.cisco.com である可能性があります。

- [Subscriber Name]：Cisco ISE pxGrid サービス登録時の pxGrid クライアントを識別する一意のテキスト文字列（例：`acme`）。サブスクライバ名は、Cisco DNA Center から Cisco ISE への統合時に使用されます。
- [SSHキ Key]：SSH キーは Base64 エンコード形式の Diffie-Hellman 暗号キーです。このキーは、Cisco ISE 管理コンソールへの SSH 接続にセキュリティを提供します。Cisco ISE CLI コマンド **show crypto authorized_keys** および **show crypto host_keys** を使用してキーを取得できます。
- [Virtual IP Address(es)]：Cisco ISE ポリシーサービスノード（PSN）の前面にあ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。

（注） 必要な情報を入力すると、Cisco ISE は Cisco DNA Center と 2 つのフェーズを経て統合されます。統合が完了するまでに数分かかります。フェーズごとの統合ステータスは、次のように [Authentication And Policy Servers] ページと [System 360] ページに表示されます。

Cisco ISE サーバ登録フェーズ：

- [Authentication and Policy Servers] ページ：「進行中」
- [System 360] ページ：「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] ページ：「アクティブ」
- [System 360] ページ：「プライマリ使用可能」および「PXGRID 使用可能」

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

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

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

注目　Cisco ISE サーバに [TACAS] を選択しない場合、Cisco ISE ノードの設定に使用できません。

- [Authentication Port]：AAA サーバへの認証メッセージのリレーに使用されるポート。デフォルト値は UDP ポート 1812 です。
- [Accounting Port]：AAA サーバへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。デフォルトの UDP ポートは 1813 です。
- [Port]：TACAS によって使用されるポート。デフォルト 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 サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ 6　[Add] をクリックします。

ステップ 7　セカンダリサーバを追加するには、ステップ 2 ～ 6 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 サーバの設定

ステップ 1　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 （47 ページ）」を参照してください。

ステップ 2　Syslog、SNMP、および Netflow コレクタ サーバの IP アドレスを設定します。次の手順を実行します。

a) Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[Network]** の順に選択します。

b) [SYSLOG Server] フィールドに、Syslog サーバの IP アドレスを入力します。

（注）　[Cisco DNA Center as syslog server] チェックボックスがオンになっていることを確認します。これは、アシュアランスに必要です。このオプションでは、アシュアランスを有効にして Syslog イベントを使用し、特定の問題をトリガーして [Device 360] ウィンドウに Syslog イベントを表示します。

c) [SNMP サーバ（SNMP Server）] フィールドに、SNMP サーバの IP アドレスを入力します。

（注）　[Cisco DNA Center as snmp server] チェックボックスがオンになっていることを確認します。これは、アシュアランスに必要です。

d) [Time Zone] ドロップダウンリストで、サイトの地理的な場所に基づいて選択したサイトのタイムゾーンを選択します。

（注） デフォルトでは、サーバタイムがタイムゾーン設定で使用されます。タイムゾーンは、デバイスの更新またはプロビジョニングをスケジュールする際に使用されます。

e) [Message of the day (MOTD)] フィールドに、デバイスにログオンするときに MOTD バナーとして表示されるメッセージを入力します。

（注） MOTD のカスタムメッセージは、最大 40 行まで設定できます。各行は 80 文字以下にする必要があります。英数字、大文字と小文字、#以外の特殊文字を使用できます。デバイス上の既存の MOTD メッセージをオーバーライドしない場合は、[MOTD] フィールドの下にあるチェックボックスをオンにします。

ステップ 3 サイトにデバイスを追加します。それにより、Cisco DNA Center からデバイスに設定がプッシュされます。

「デバイスをサイトに追加する （77 ページ）」を参照してください。

ステップ 4 デバイスのテレメトリ指数（TQ）プロファイルを適切なログレベルに適用します。次の手順を実行します。

a) **[Design]** > **[Network Settings]** > **[Network]** を選択し、**[Network Telemetry]** をクリックします。
b) [サイトの表示（Site View）] タブをクリックします。
デバイスのリストが表示されます。
c) ルータの横にあるチェック ボックスをオンにします。
d) [Actions] ドロップダウンリストから、次のログレベルを選択します。

- [Maximal Visibility]：これにより、Syslog レベル 6（情報）が有効になります。
- [Optimal Visibility]：これにより、Syslog レベル 6 およびルータ上のネットワークが有効になります。
- **テレメトリの無効化**

ステップ 5 （任意）NetFlow コレクタサーバを追加するには、**[Design]** > **[Network Settings]** > **[Network]** を選択し、[Add Servers] をクリックします。

[サーバの追加（Add Servers）] ウィンドウが表示されます。

a) [NetFlow Collector] のチェックボックスをオンにします。NetFlow Collector サーバが [Network] ウィンドウに追加されます。
b) [NetFlow コレクタ サーバ（NetFlow Collector Server）] エリアで、NetFlow コレクタ サーバの IP アドレスとポート番号を入力します。
c) **[保存 (Save)]** をクリックします。

スイッチの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
!
!
crypto pki certificate chain DNAC-CA
 certificate ca 009156FDDCC160F24A
```

```
  308202F7 308201DF A0030201 02020900 9156FDDC C160F24A 300D0609 2A864886
  F70D0101 0B050030 12311030 0E060355 04030C07 6B756265 2D636130 1E170D31
  38303530 33303035 3932335A 170D3231 30313237 30303539 32335A30 12311030
  0E060355 04030C07 6B756265 2D636130 82012230 0D06092A 864886F7 0D010101
  05000382 010F0030 82010A02 82010100 D04771B0 47DF3C65 26AF54CB 32D606B0
  CB9C6023 8CD6FDDD 5E26A340 715F506D AEF2BF13 37D9BA1C C79577A9 1800424F
  5FE5C49C 5694E6E2 A53EFE15 8AC8A186 161A8D88 D44F2F66 BD9D3142 743D20BA
  31DF43A5 E46E5E0B EEACE9BF 68280E1A 80622500 9D031B15 9FD45E18 121C2726
  69B7D768 8EDAC319 7CDBF68C 137A5676 8EE7D5C5 71B34592 CAD1A4B8 590DC27A
  A8172A76 104C0E50 1E0F1D0C 2E649C5B 734E5C9F 0453E248 36937F5E 486191C3
  65667BC9 9393B864 C0674594 9194EF4E C2B4845E 1ACCEB3F 82FE0C48 1548136C
  53015248 0FF8DEA5 3F4281BB 79A3183A 22E76AAF 20D91016 94CC9339 BF2F9C4A
  3D345E2F 8DDC0EA3 453D5FEB 670C9F6B 02030100 01A35030 4E301D06 03551D0E
  04160414 63528371 86225027 1A79B16E D2645368 929A96C0 301F0603 551D2304
  18301680 14635283 71862250 271A79B1 6ED26453 68929A96 C0300C06 03551D13
  04053003 0101FF30 0D06092A 864886F7 0D01010B 05000382 01010094 5751DB9B
  6C460EB0 892A32F2 450AAEFB 5C7D41AA 8E7CCD3D ECE78771 F3AD1CA2 76444620
  90CAB088 BE07A2ED A2D13325 019568BB F1FE9EAC 123A6A7F C81277D5 74556B3B
  4BBD6691 785EB7CD 581A95F0 8306101D 54AE51D0 02DB7F32 C210A14E 449A1F57
  02815C71 E8A53C33 1828B08D 4CCE3707 1FE4B867 5A88E1A2 9E8E106A 87F43E69
  37234473 F00E1773 733CAF76 E5807A00 158F6501 E1B45537 17E3F2BE BBC520D0
  C54EE06C B18A30F1 AC4D1A2E 809DFFB0 B282E318 18C95393 23A13FA8 45DBC79D
  01A90F87 C9262FDB DDF258AD 86E70B64 1426B072 3F31BAD8 14F4CAC5 FC039912
  E288A1CF 5F2EC94C ED0B820B 3AF84E3F 32C501F3 5E71A656 BEABE3
      quit
interface GigabitEthernet1/0/2
 ip device tracking maximum 10
!
interface GigabitEthernet1/0/3
 ip device tracking maximum 10

!
flow exporter 10.4.48.218
 destination 10.4.48.218
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
!
snmp-server community cisco1 RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint bsnRogue bsn80211Security bsnAutoRF

 bsnGeneral SI mobility mfp RRM AP rogue client
snmp-server enable traps cpu threshold
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
```

```
snmp-server enable traps flash insertion removal
snmp-server enable traps power-ethernet group 1
snmp-server enable traps power-ethernet police
snmp-server enable traps energywise
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps license
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps stackwise
snmp-server enable traps port-security
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps trustsec-server radius-server provision-secret
snmp-server enable traps trustsec authz-file-error cache-file-error keystore-file-error
keystore-sync-fail random-number-fail src-entropy-fail
snmp-server enable traps trustsec-interface unauthorized sap-fail authc-fail supplicant-fail authz-fail
snmp-server enable traps trustsec-policy peer-policy-updated authz-sgacl-fail
snmp-server enable traps bgp cbgp2
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps event-manager
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps local-auth
snmp-server enable traps msdp
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps syslog
snmp-server enable traps ipsla
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public
!
ip http client source-interface GigabitEthernet1/0/1
!
ip ssh source-interface GigabitEthernet1/0/1
```

ルータの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
```

```
 enrollment terminal
 usage ssl-client
 revocation-check crl none
!
crypto pki certificate chain DNAC-CA
 certificate ca 00D97DCBDFA3EB517E
  308202F7 308201DF A0030201 02020900 D97DCBDF A3EB517E 300D0609 2A864886
  F70D0101 0B050030 12311030 0E060355 04030C07 6B756265 2D636130 1E170D31
  38303531 35303531 3131375A 170D3231 30323038 30353131 31375A30 12311030
  0E060355 04030C07 6B756265 2D636130 82012230 0D06092A 864886F7 0D010101
  05000382 010F0030 82010A02 82010100 A68A3FCD 5423262C CD10E16B A0517BCF
  17E085F5 705B26E1 7B1251F2 353CB489 A049FB68 00E65F21 C15E14B5 D5EFF90C
  8B78CBC1 9F749819 466E5924 0B1780F2 4B31CDA3 1E0EED5D FFF4D29F FE935413
  DAD2DB46 9778ACD8 44FC1AD8 9042BE47 11ED9E29 97D9B4C9 E51C3767 98AE61B0
  38254DAB F4417F8B AE80695E 5236D36C 47052F02 E2E234A6 564D71D4 44F09D98
  C1B5BF3B CDED2108 DA04C6B0 7E9A8EE5 036F4913 575C1567 97EEC40A AA53E91A
  7E4E2419 D990E031 4E40F561 F766A4E2 B76B4281 E95AB7BA 01F6A42C 1EF040BD
  97358EBC 9A9BC46F C127DE3E FA1841F9 41B45392 4E546AE3 396D1D25 4B2DD897
  6D5CD7AF 6E342548 2CF1BA48 DAA51C21 02030100 01A35030 4E301D06 03551D0E
  04160414 A811B663 0573E872 B4913BEF 698A2405 9A92D2F5 301F0603 551D2304
  18301680 14A811B6 630573E8 72B4913B EF698A24 059A92D2 F5300C06 03551D13
  04053003 0101FF30 0D06092A 864886F7 0D01010B 05000382 0101007B 67E62397
  B47E806D 57E5F75B 18F567A5 1373E05E FB381F07 0F306852 A3DF1048 AB3D0F2C
  2CE40F77 8251F171 1B82E671 0BA0DC05 4694DA48 D13BC4FC 1482B0A1 6ECD607F
  EB03C9B9 A6BB99C3 649E1957 DD48E0E5 60FDEF22 E468997B 77BB91AB 4CC4B319
  1A21C571 804AEC36 BEC14C8F 78D1C133 E65B5D18 F4E310B6 3353EF73 511189CF
  CF47C243 8D40A0B3 738BB94E E6434F74 D20D3E99 D0E96858 B25DC9C7 08CAF030
  AE7A68C6 F9BC351C 97FEDF0E 76525B07 60E13693 583BAC0B 7AFB3DA4 8EF24861
  FAC8B688 0FB24D79 3E16B380 38A39B82 AD8D566B 16883040 A5415C5D 82E6C1BF
  AEDEBE91 12F4208B 88C9FC28 3A12B3EE 7EDFBA7B 588C355C D94B29
   quit
!
flow exporter 10.4.48.218
destination 10.4.48.218
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps entity-perf throughput-notif
snmp-server enable traps ds3
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps casa
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps cef resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
```

```
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ip local pool
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps atm subif
snmp-server enable traps pki
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps ether-oam
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps entity-state
snmp-server enable traps entity-qfp mem-res-thresh throughput-notif
snmp-server enable traps adslline
snmp-server enable traps vdsl2line
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps srp
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps cnpd
snmp-server enable traps bfd
snmp-server enable traps otn
snmp-server enable traps ipsla
snmp-server enable traps sonet
snmp-server enable traps dlsw
snmp-server enable traps resource-policy
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps c3g
snmp-server enable traps LTE
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps firewall serverstatus
snmp-server enable traps trustsec-sxp conn-srcaddr-err msg-parse-err conn-config-err binding-err
conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps lisp
snmp-server enable traps aaa_server
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps pw vc
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps rsvp
```

```
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps mvpn
snmp-server enable traps pimstdmib neighbor-loss invalid-register invalid-join-prune rp-mapping-change

 interface-election
snmp-server enable traps isis
snmp-server enable traps bgp cbgp2
snmp-server enable traps ospfv3 state-change
snmp-server enable traps ospfv3 errors
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps ike policy add
snmp-server enable traps ike policy delete
snmp-server enable traps ike tunnel start
snmp-server enable traps ike tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps gdoi gm-start-registration
snmp-server enable traps gdoi gm-registration-complete
snmp-server enable traps gdoi gm-re-register
snmp-server enable traps gdoi gm-rekey-rcvd
snmp-server enable traps gdoi gm-rekey-fail
snmp-server enable traps gdoi ks-rekey-pushed
snmp-server enable traps gdoi gm-incomplete-cfg
snmp-server enable traps gdoi ks-no-rsa-keys
snmp-server enable traps gdoi ks-new-registration
snmp-server enable traps gdoi ks-reg-complete
snmp-server enable traps gdoi ks-role-change
snmp-server enable traps gdoi ks-gm-deleted
snmp-server enable traps gdoi ks-peer-reachable
snmp-server enable traps gdoi ks-peer-unreachable
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps alarms informational
snmp-server enable traps ethernet cfm alarm
snmp-server enable traps rf
snmp-server enable traps transceiver all
snmp-server enable traps mpls vpn
snmp-server enable traps mpls rfc vpn
snmp-server enable traps vrfmib vrf-up vrf-down vnet-trunk-up vnet-trunk-down
snmp-server host 8.8.8.8 public

ip http client source-interface GigabitEthernet0/0/1
!
ip ssh source-interface GigabitEthernet0/0/1
```

シスコ ワイヤレス コントローラの Syslog、SNMP トラップ、および NetFlow コレクタとその他の設定の例

```
config snmp community create cisco
config snmp community create cisco123
config snmp community mode enable cisco
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco
config snmp community mode enable cisco123
config snmp community accessmode rw cisco123
config snmp community ipaddr 0.0.0.0 0.0.0.0 cisco123
```

```
config network assurance server idtoken 1 6b5af7c9808a0b1b7824fc9a801b5478
de751722396b0fe0b221b3be71f3a94ef2fe0716 16 88664b59c40e1f1f2ffc14097897ed620000000
config network assurance server url https://10.4.48.132
config network assurance on-change enable

config flow create exporter 10.4.48.218 10.4.48.218 port 6007
config logging level critical
config logging syslog level 2
config logging syslog facility syslog
config logging syslog host 7.7.7.7
config snmp trapreceiver create 8.8.8.8 8.8.8.8
config snmp trapreceiver ipsec profile none 8.8.8.8
config snmp trapreceiver mode enable 8.8.8.8

config trapflags client enhanced-802.11-deauthenticate enable
config trapflags client enhanced-802.11-associate enable
config trapflags client max-warning-threshold enable
config trapflags client 802.11-authfail disable
config trapflags client 802.11-associate disable
config trapflags client 802.11-disassociate disable
config trapflags client authentication disable
config trapflags client webauthuserlogout enable
config trapflags client 802.11-deauthenticate disable
config trapflags client neighborclientsignal disable
config trapflags client webauthuserlogin enable
config trapflags client 802.11-assocfail disable
config trapflags client excluded enable
config trapflags client enhanced-802.11-stats enable
config trapflags client enhanced-authentication enable
config trapflags client nac-alert enable
config trapflags client enhanced-802.11-disassociate-stats disable
```

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。

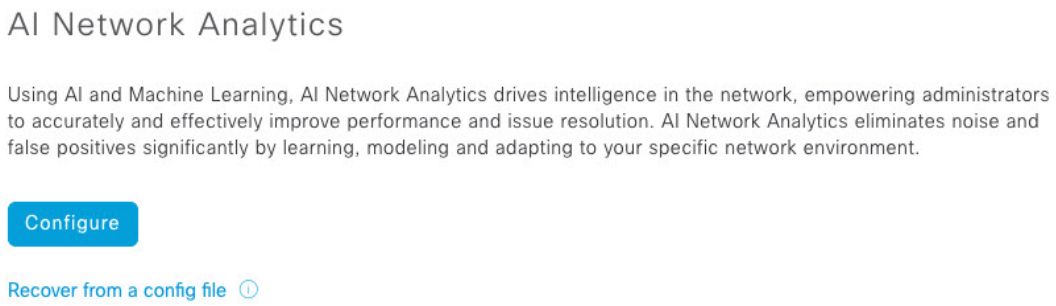
始める前に

- 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 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **AI ネットワーク分析** の順に選択します。
[**AI ネットワーク分析**（SIP MWI notification mechanism）] ウィンドウが表示されます。

図 *6 : [AI Network Analytics]* ウィンドウ



ステップ 2 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。

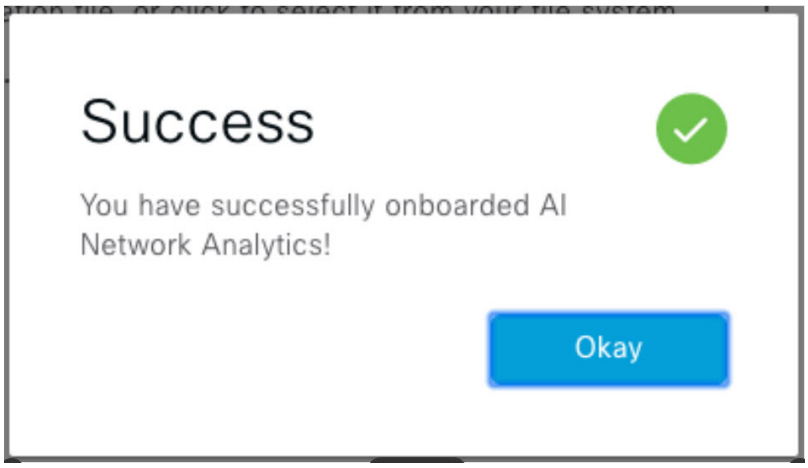
     [Restore AI ネットワーク分析] ウィンドウが表示されます。

  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。

図 *7 : [Success]* ダイアログボックス



- 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。

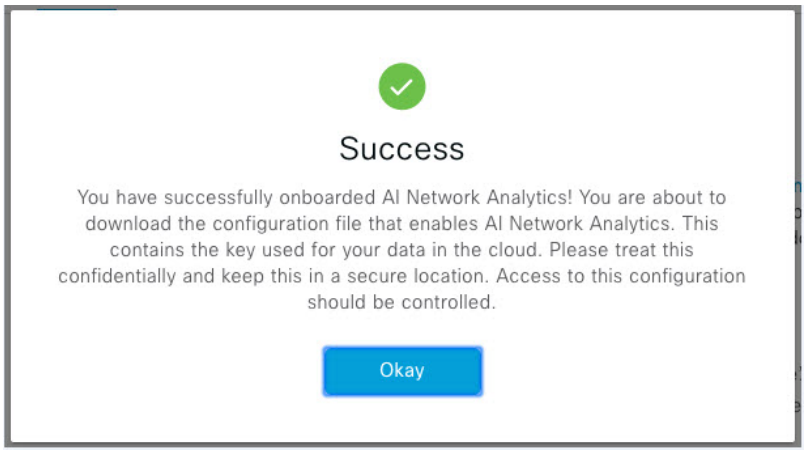
1. [Configure] をクリックします。
2. [Where should we securely store your data?] 領域で、データを保存する場所を選択します。[Europe (Germany)] または [US East (North Virginia)] を選択できます。

   [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。

図 *8 : [Success]* ダイアログボックス



ステップ 3 [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 4 （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。

関連トピック

Cisco AI Network Analytics データ収集の無効化 （92 ページ）

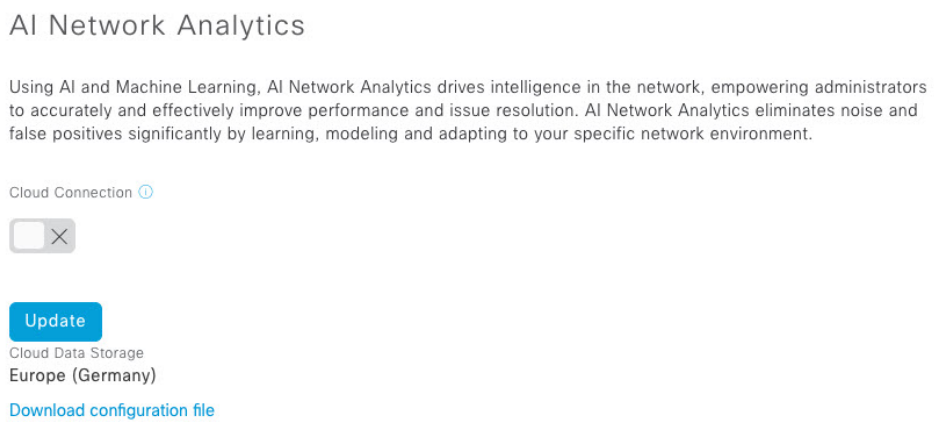
Cisco AI Network Analytics データ収集の無効化

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 Cisco DNA Center のホームページで、 > **[System Settings]** > **[Settings]** > **AI ネットワーク分析** の順に選択します。
[**AI ネットワーク分析**（SIP MWI notification mechanism）] ウィンドウが表示されます。

ステップ 2 [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。

図 *9 :* データ収集を無効にした *[AI Network Analytics]* ウィンドウ



ステップ 3 [Update] をクリックします。

ステップ 4 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てください。

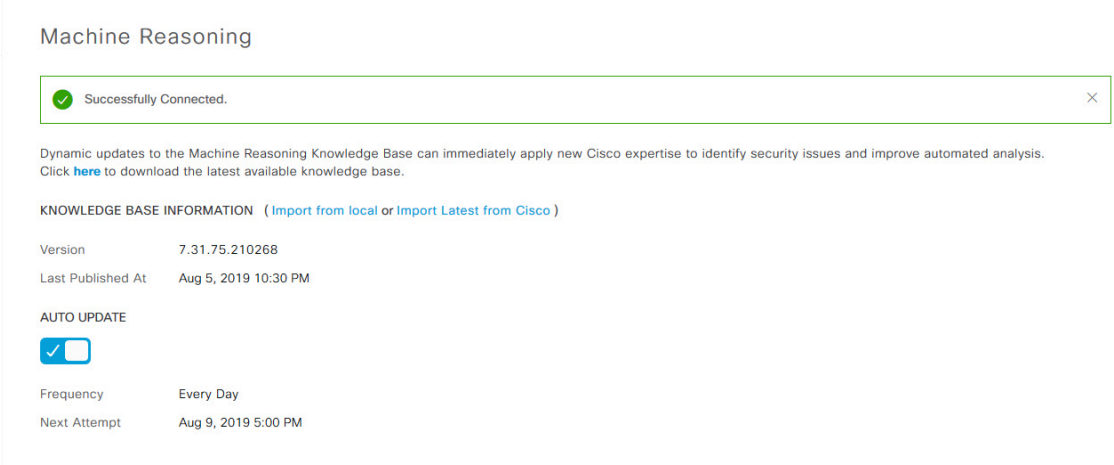
ステップ 5 （任意）以前の設定が間違って配置されている場合は、[Download configuration file] をクリックします。

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。

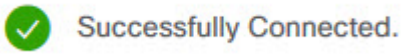
ステップ 1 Cisco DNA Center のホームページで、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[Machine Reasoning]** の順に選択します。
[Machine Reasoning] ウィンドウが表示されます。

図 *10 : [Machine Reasoning]* ウィンドウ



ステップ 2 （推奨）Cisco DNA Center で機械推論ナレッジベースを自動的に更新するには、[Auto Update] をクリックして有効にし、✔マークが表示されるようにします。
次の更新の頻度、日付、および時刻は、[Frequency] および [Next Attempt] エリアに表示されます。

（注） 自動更新を実行できるのは、 Cisco DNA Center がクラウド内の機械推論エンジンに正常に接続されている場合のみです。



ステップ 3 手動更新を実行するには、次のいずれかを実行します。

- 機械推論ナレッジベースをローカルマシンにダウンロードして、Cisco DNA Center にインポートします。次の手順を実行します。

  1. ハイパーリンクされた**ここ**のテキストをクリックします。

     ```
     Dynamic updates to the Machine Reasoning knowledge base can immediately apply new Cisco
     expertise to identify security issues
     and improve automated analysis.
     Click here to download the latest available knowledge base.
     ```

     [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. 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 にインポートするには、[Import from local] をクリックします。

- 最新の機械推論ナレッジベースをシスコから直接 Cisco DNA Center にインポートするには、[Import Latest from Cisco] をクリックします。[Success] ポップアップウィンドウが、更新のステータスとともに右下隅に表示されます。

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。

（注） ほとんどの画面（ホームページ、ツール、オンラインヘルプ、REST API など）はローカライズされていますが、アシュアランス 画面はローカライズされていません。

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。

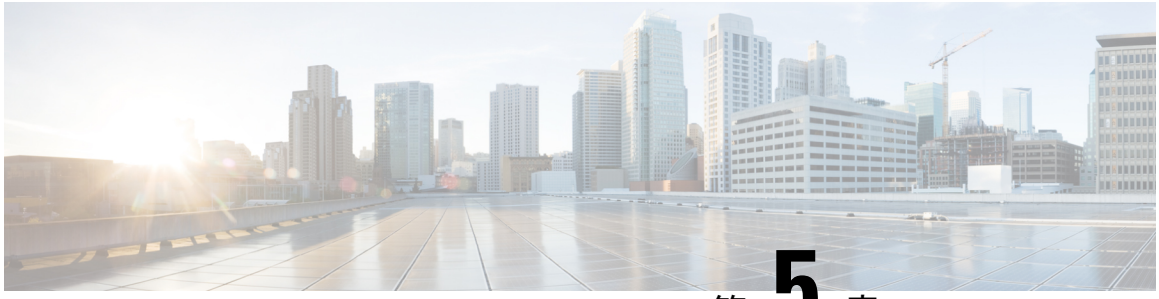
ステップ 1 ブラウザでロケールをサポートされている言語（中国語、日本語、または韓国語）のいずれかに変更します。

- 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 *11 :* ローカライズされたログイン画面の例



第 5 章

企業全体の健全性のモニタ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。クライアントはネットワーク健全性スコアの一部ではないことに注意してください。

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。

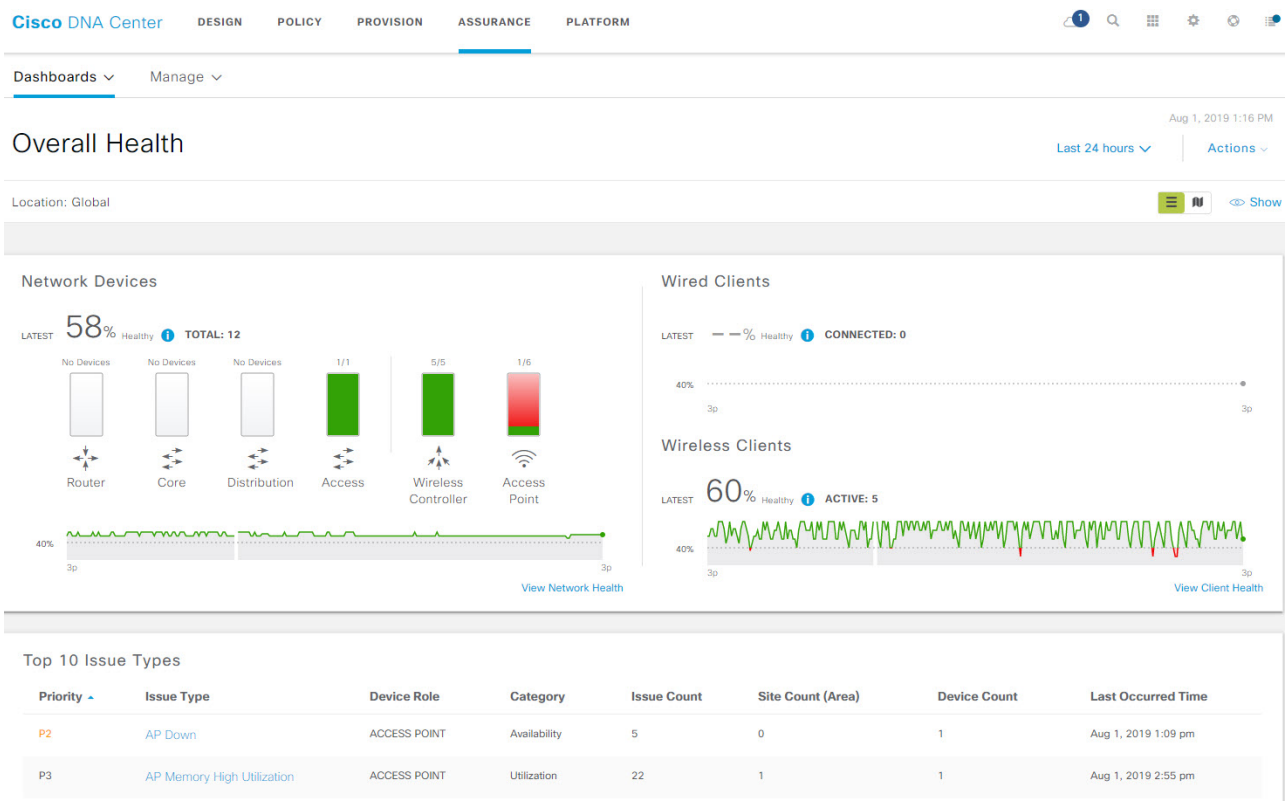
始める前に

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 （19 ページ） を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[全体的な健全性（Overall Health）] ダッシュボードが表示されます。

図 12 : [Overall Health] ダッシュボード



ステップ 2 次の機能には、[Overall Health] メニューバーを使用します。

[Overall Health] メニュー バー	
項目	**説明**
[Last 24 hours] 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時間範囲内でダッシュボードにデータを表示します。オプションは、[Last 3 hours]、[Last 24 hours]、および [last 7 days] です。 デフォルトは [Last 24 hours] です。
Actions	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 （256 ページ）およびカスタム ダッシュボードの作成 （251 ページ）を参照してください。

ステップ 3 [Location] ペインには、次の機能が用意されています。

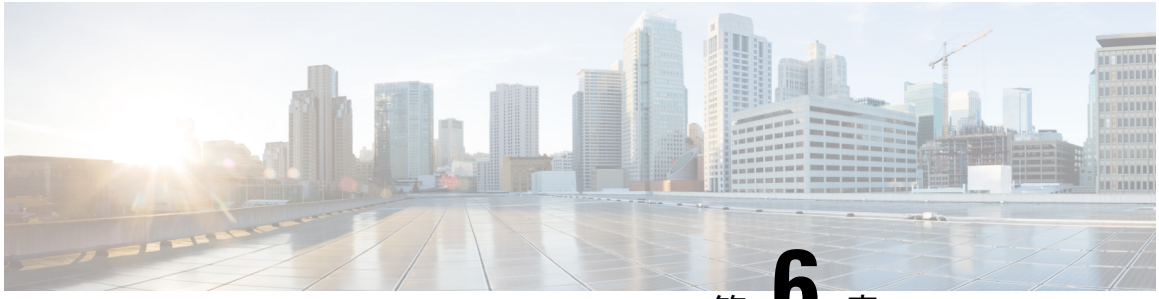
[Location] ペイン	
項目	説明
Show Hide	[Location] ペインは、表示または非表示にできます。デフォルトでは、[Location] ペインは非表示になっています。
	このボタンをクリックして、ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。テーブルには、特定のロケーションの正常なクライアントとネットワークデバイスの割合が選択に基づいて表示されます。
	[Overall Health Map]：このアイコンをクリックすると、企業のすべてのサイトの正常性が、地理的ロケーションに基づいたク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、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。健全性は 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。

ステップ 4 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	
項目	説明
[ネットワーク デバイス（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 （126 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） [Fabric Domain] 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とトラブルシューティング （101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 （151 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とトラブルシューティング （133 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 （260 ページ）を参照してください。



第 6 章

ネットワーク正常性のモニタ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。クライアントはネットワーク健全性スコアの一部ではないことに注意してください。

ネットワークの健全性のモニタ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。クライアントはネットワーク健全性スコアの一部ではないことに注意してください。

（注） ネットワーク ヘルス 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 （19 ページ） を参照してください。

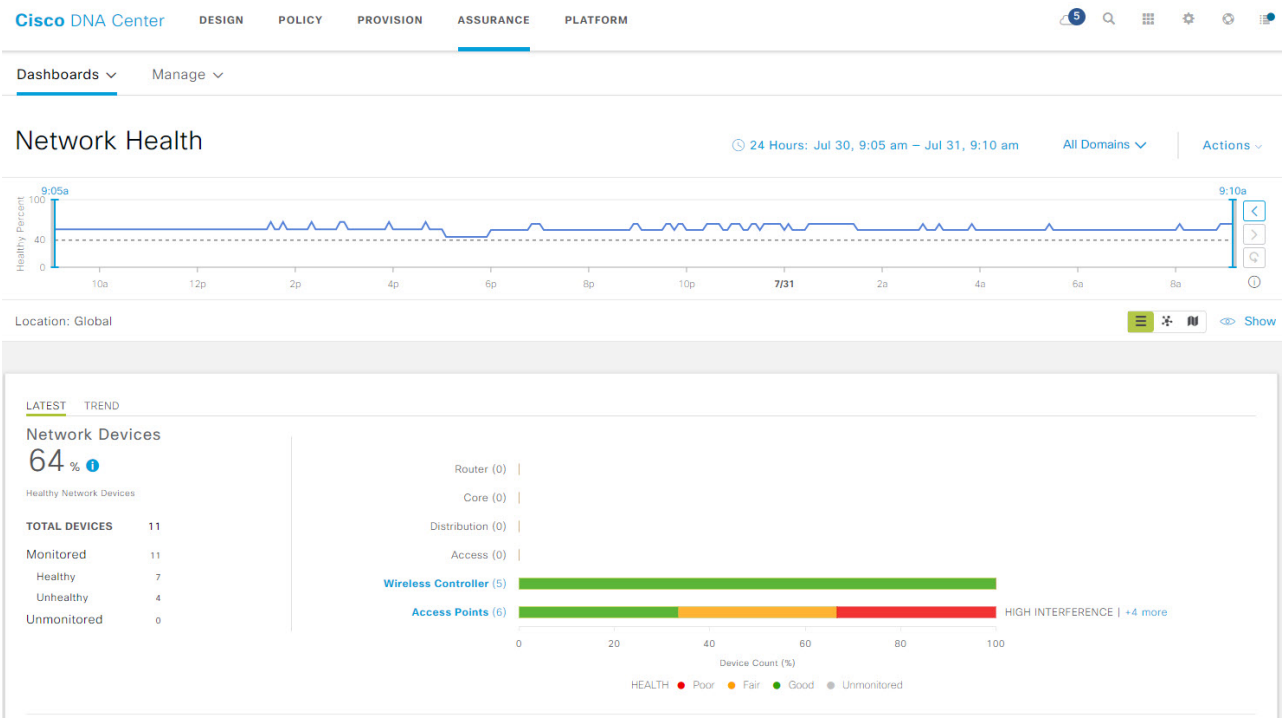
ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Health]** > **[Network Health]** の順に選択します。

[Network Health] ダッシュボードが表示されます。

図 *13 : [Network Health]* ダッシュボード



ステップ 3 次の機能には、[Network Health] タイムラインを使用します。

[Network Health] タイムライン	
項目	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.** **[開始日付（Start Date）]**と時刻、**[終了日付（End Date）]**と時刻を指定します。 **3.** [Apply] をクリックします。
すべてのドメイン	[All Domains]：すべてのドメインまたはファブリックドメインの情報を表示します。デフォルトは**すべてのドメイン** です。 [Fabric Domains]：ファブリックドメインに関する情報を表示するには、[All Domains] 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。マルチサイト ファブリックでは、ファブリック ドメインに接続されているサイトおよび中継エリアがドロップダウンリストで表示されます。 [Fabric Domains] の場合、[Hierarchical Site View] や [Building View] エリアからではなく、[All Domains] ドロップダウンリストからサイトまたはビルディングを選択する必要があります。 ファブリック ドメインのモニタおよびトラブルシューティングを行うには、最初にファブリック ドメインを設定する必要があります。ファブリック ドメインの作成 （121 ページ）およびファブリックへのデバイスの追加 （121 ページ）を参照してください。 マルチサイト ファブリック ドメインの詳細情報については、Cisco Digital Network Architecture Center ユーザ ガイドの「ネットワークのプロビジョニング」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いません。
Actions	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 （256 ページ）およびカスタム ダッシュボードの作成 （251 ページ）を参照してください。

[Network Health] タイムライン	
項目	説明
タイムラインスライダと正常なネットワークデバイス比率	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.** アイコンの上にマウスカーソルを合わせます。 **2.** ツールチップで、 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.** **[保存 (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 4 [Location] ペインには、次の機能が用意されています。

[Location] ペイン	
項目	説明
Show Hide	[Location] ペインは、表示または非表示にできます。デフォルトでは、[Location] ペインは非表示になっています。
	[Hierarchical Site View] と [Building View]：このアイコンをクリックすると、ドロップダウンリストを使用して、サイトまたはビルディングの正常なネットワークデバイス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、[Network Health] ダッシュボードにはロケーションのクライアント情報のみが表示されます。 （注） [Fabric Domains] の場合、[Hierarchical Site View] や [Building View] エリアからではなく、[All Domains] ドロップダウンリストからサイトまたはビルディングを選択する必要があります。

[Location] ペイン	
項目	説明
	[Network Topology]：このアイコンをクリックすると、ネットワーク内のコンポーネントの接続状況を示すトポロジビューが表示されます。 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、[詳細 360 の表示（View Details 360）] をクリックします。
	Network Health Map：このアイコ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、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。 ヘルス スコアの色は、その重大度を示します。健全性は 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。

ステップ 5 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	
項目	説明
[Network Device Health Summary] エリア	

[Network Device Health Summary] ダッシュレット	
項目	説明
	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。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。 • **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（126 ページ） を参照してください。 • **デバイス総数**：ネットワークデバイスの総数、およびモニタ対象、正常、異常、モニタ対象外のデバイスの数が表示されます。 • **チャート**：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、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、サイドペインに追加の詳細情報を表示できます。 （注） ファブリック ドメインの場合、色分けされたパーセンテージ チャートに、ファブリック カテゴリ（[ファブリック エッジ（Fabric Edge）]、[ファブリック境界（Fabric Border）]、[ファブリック コントロール プレーン（Fabric Control Plane）]、[ファブリック ワイヤレス（Fabric Wireless）]）のパフォーマンスが示されます。 • **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

[Network Device Health Summary] ダッシュレット	
項目	説明
	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。 ●：使用できるデータがありません。ヘルス スコアは 0 です。
[詳細の表示（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 6 [Top APs Up/Down]、[Top N APs by Client Count]、[Top N APs with High Interference] ダッシュレットを使用して、次の情報を表示します。

[Total APs Up/Down] ダッシュレット
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。 15 分のスナップショットビューと 24 時間のトレンドビューがあります。 [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。 15 分のスナップショットビューと 24 時間のトレンドビューがあります。 [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 with High Interference] 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。 15 分のスナップショットビューと 24 時間のトレンドビューがあります。 [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 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	
項目	説明
[DEVICE]	次のオプションを使用してテーブルをフィルタリングします。 • **監視対象** • [Unmonitored]：モニタ対象外デバイスは、指定された時間範囲内にアシュアランスがテレメトリデータを受信しなかったデバイスです。非モニタ対象デバイスは、ネットワーク ヘルス スコアの計算に含まれます。これらはデバイスの合計数の一部となり、この合計数に対して正常なデバイスのパーセンテージが計算されます。
[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。
[OVERALL HEALTH]	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。 • **すべて** • 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。
[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） 全体的な健全性スコアは、システムの健全性、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の KPI メトリックは、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）、およびコントロールプレーン（到達可能性）です。 [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	
項目	説明
デバイスの [Device 360] の表示	[デバイス（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。

デバイスの健全性のモニタ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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

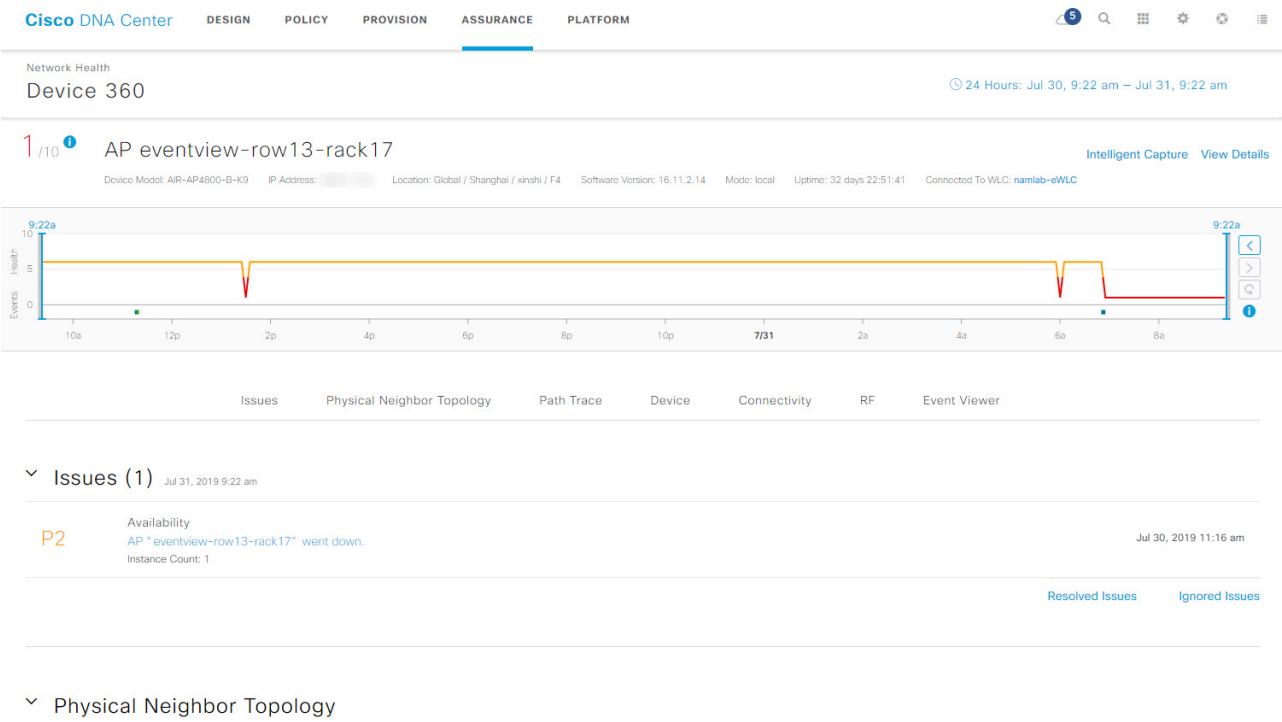
ステップ 2 **[Dashboards]** > **[Health]** > **[Network Health]** の順に選択します。
[ネットワークの健全性（Network Health）] ウィンドウが表示されます。

ステップ 3 次のいずれかを実行します。

- [ネットワーク デバイス（Network Devices）] ダッシュレットの [デバイス（Device）] 列で、デバイスの名前をクリックします。
- [検索（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。

[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 *14 : [デバイス 360（Device 360）] ウィンドウ*



ステップ 4 右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 ウィンドウの右上隅にある [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 （240 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 デバイスの正常性スコアがデバイス名の左側に表示されます。

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、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、コントロール プレーン ノードへの接続が含まれます。詳細については、「スイッチ 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、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 （125 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、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 （128 ページ）」を参照してください。

  （注） 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。

- [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 （129 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、コントロール プレーン ノードへの接続が含まれます。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 （130 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。健全性は 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。
- ●：使用できるデータがありません。ヘルス スコアは 0 です。

ステップ 7 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、稼働時間などのデバイスに関する最新情報を表示するには、タイムラインの上に表示される [Device 360] ヘッダーを使用します。

（注） Cisco StackWise Virtual の場合、ヘッダーには [Stack Status: Stackwise Virtual] と [Stackwise Virtual Domain] の 2 つの追加要素が含まれています。

ステップ 8 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を開くには、右上隅にある [View Details] をクリックします。

ステップ 9 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）の横のタイムスタンプも更新される点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 10 問題、物理ネイバートポロジ、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. [Status] 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、解決済みの問題の一覧が表示されます。 • 問題を無視するには、次の手順を実行します。 1. [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。 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 （259 ページ）を参照してください。

物理ネイバートポロジのカテゴリ
特定のデバイスのトポロジ ビューを表示し、そのデバイスがネイバー デバイスにどのように接続されているかを示します。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を示すスライドインウィンドウを表示します。 • 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、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。 （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） Cisco StackWise Virtual が スタックアイコンとともに表示されます。 Cisco StackWise Virtual がそのパスに含まれている場合、パストレースによってスイッチアイコンが表示されます。

イベントビューアのカテゴリ
• [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。送信電力の変更、RF チャネルの変更、無線のリセットなどの Radio Resource Management（RRM; 無線リソース管理）イベントが表示されます。 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 switches and routers]：エラー以上の重大度（緊急、アラート、クリティカル）を持つすべての syslog、アップ/ダウンしているあらゆるリンクのイベント、デバイスの到達可能性または非到達可能性イベントがイベントビューアに記録されます。加えて、エラーレベルより重大度が低い syslog（警告、通知、および情報）の選択されたリストのみが表示されます。選択した syslog メッセージのリストについては、スイッチおよびルータのエラーレベルに満たない選択済み Syslog（118 ページ） を参照してください。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
[新しいパストレースの実行（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 （157 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
ルータ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ラジオ 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。 シスコ アプリケーション エクスペリエンスについて （161 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 （167 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。

詳細情報のカテゴリ

詳細情報のカテゴリ
デバイスのタイプに応じて、一定期間のパフォーマンスの履歴KPIが次のタブの適切なチャートに表示されます。 • [Device Info]タブ：CPU、メモリ、稼働時間などのデバイスの詳細が表示されます。 • [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 でのみ使用できます。 使用可能なチャートは次のとおりです。 • [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、チャートの右側で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。 （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。 • [RF] タブ：無線チャンネルの幅、使用率、干渉、ノイズ、電波品質などが表示されます。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。 • [Interface] タブ：[All]、[Access]、[Auto]、[Routed]、[Trunk]、[SVL]、および [DAD] のポートタイプのタブが含まれます。クリックするタブに基づいて、テーブルが更新されます。 名前、説明、動作ステータス、リンク速度などのインターフェイス情報を含むテーブルが表示されます。インターフェイステーブルのカラムはソートできます。ただし、新しいパラメータを使用してカラム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] データのカラムには、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フォーマットで表示するには、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。[Interface Availability]、[Utilization]、

詳細情報のカテゴリ
および [Error] チャートがテーブルの下に表示されます。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。 • [Fabric] タブ：到達可能性やアップリンクステータスのチャートなどのファブリック KPI が表示されます。このタブは、ファブリックドメインにのみ表示されます。 （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。 • [StackWise Virtual] タブ：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、優先度、稼働時間、ポート番号など）を示すテーブルが表示されます。このタブは Cisco StackWise Virtual にのみ表示されます。

スイッチおよびルータのエラー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、エラーレベル（警告、通知、情報）に満たない syslog メッセージ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

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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[全体的な健全性（Overall Health）] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Health Score Settings]** を選択します。

[Health Score] ウィンドウが表示されます。

ステップ 3 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 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) 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。

c) 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 6 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。

ファブリックドメイン

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。

ファブリックの概要

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。ファブリックを使用すると、仮想ネットワークやユーザ/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 ドメインの作成

Cisco DNA Center では、デフォルト *LAN* ファブリックと呼ばれるデフォルトのファブリック ドメインが作成されます。

始める前に

ネットワークが設計されていること、ポリシーが Cisco Integrated Services Engine（ISE）から取得されているか Cisco DNA Center で作成されていること、デバイスがインベントリに登録され、サイトに追加されていることを確認してください。

ステップ 1 Cisco DNA Center ホームページで、**[プロビジョニング（Provision）]** をクリックします。

ステップ 2 **[ファブリック（Fabric）]** タブをクリックします。

ステップ 3 **[ファブリック ドメインまたはトランジットを追加（Add Fabric Domain or Transit）]** タブをクリックします。

ステップ 4 ポップアップから、**[トランジットを追加（Add Transit）]** を選択します。

ステップ 5 ファブリック名を入力します。

ステップ 6 ファブリック サイトの 1 つを選択します。

ステップ 7 [追加（Add）] をクリックします。

ファブリックへのデバイスの追加

ファブリック ドメインを作成した後にファブリック サイトを追加してから、このファブリック サイトにデバイスを追加できます。また、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を指定することもできます。

（注） ファブリック ドメイン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。デバイスによってはこれらのロールを実行しない場合があります。ただし、各ファブリック ドメインには、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。

（注） 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。デバイスをプロビジョニングするには、[プロビジョニング（Provision）] タブをクリックし、[デバイス（Devices）] を選択します。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、トポロジにデバイスがグレー色で表示されます。

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。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 Cisco DNA Center のホームページから、**[Provision]** > **[Devices]** の順に選択します。
すべてのプロビジョニングされたファブリック ドメインがウィンドウに表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。
結果の画面に、そのファブリック ドメイン内のすべてのサイトが表示されます。

ステップ 3 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 4 デバイスをクリックします。[デバイスの詳細（device details）] ウィンドウに、次のオプションが表示されます。

オプション	説明
エッジ ノード	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トグルボタンをクリックします。
ボーダー ノード	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トグルボタンをクリックします。詳細については、「**ボーダーノードとしてのデバイスの追加**」セクションを参照してください。
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トグルボタンをクリックします。
ゲスト境界/コントロールプレーン	次のオプションを使用できます。 • コントロールプレーン：デバイスをコントロールプレーンとして使用する場合はこのチェックボックスをオンにします。 • [Border]：デバイスをボーダーノードとして動作させる場合は、このチェックボックスをオンにします。

オプション	説明
	• [Select One Guest Virtual Network]：作成されたすべてのゲスト仮想ネットワークが一覧表示されます。ゲスト仮想ネットワークのチェックボックスをオンにして、[有効化（Enable）] をクリックします。 （注） [ポリシー（Policy）]アプリケーションでゲスト仮想ネットワークを作成したことを確認してください。
ランデブー ポイント	デバイスでランデブーポイントを設定するには、このトグルボタンをクリックします。 詳細については、「**ランデブーポイントとしてのデバイスの追加**」セクションを参照してください。

デバイスをファブリックインアボックスとして設定するには、**[コントロールプレーン（Control Plane）]**、**[ボーダーノード（Border Node）]**、および **[エッジノード（Edge Node）]** 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 Node] の両方を選択します。

ステップ 5 **[保存（Save）]** 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。

Enable SNMP Collector Metrics for Fabric Devices

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 Cisco DNA Center のホームページで、歯車のアイコン ⚙ をクリックして、[System Settings] > [Data Platform] の順に選択します。 >

ステップ 2 [コレクタ（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。

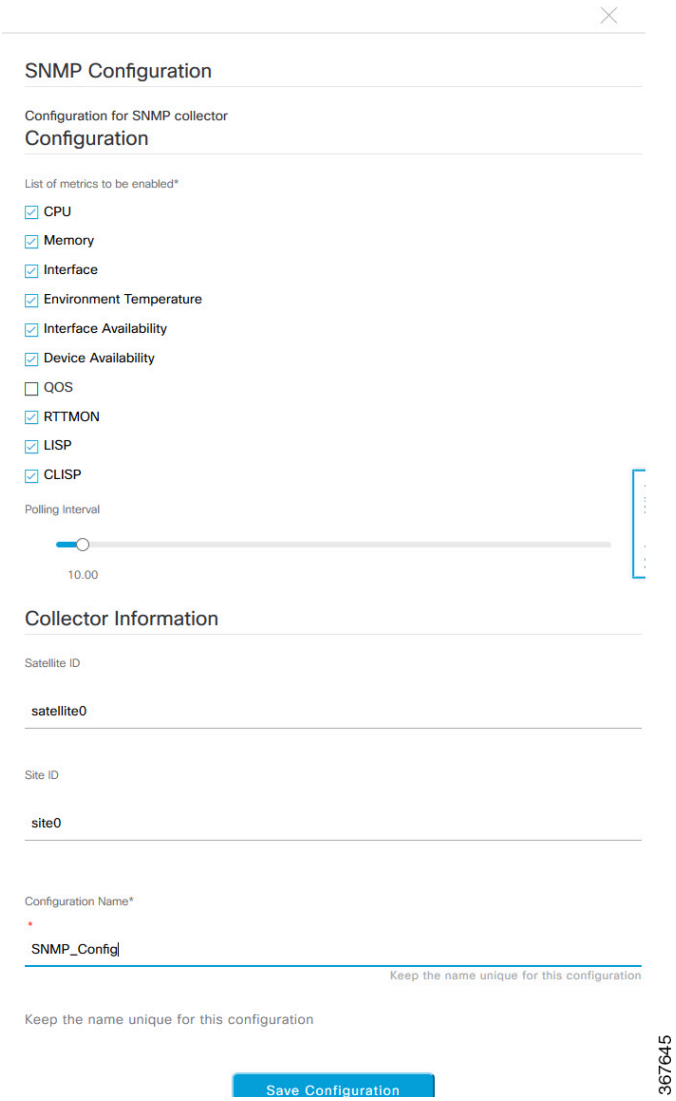
[COLLECTOR-SNMP] ウィンドウが開きます。

ステップ 4 **[+ Add（追加）]** をクリックします。

[SNMP Configuration（SNMP 設定）] 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 *15 : SNMP* の設定



ステップ 6 **[設定名（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。

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

Stackwise Virtual をサポートする Cisco Catalyst スイッチを次の表に示します。

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 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 （76 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。Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 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。Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 ページ）を参照してください。

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。

System Health	
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リングメトリックが含まれます。
Wireless	次のシステムモニタリング 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。

System Health	
デバイス タイプ	説明
ルータ（**Router**）	CPU使用率やメモリ使用率などのシステムモニタリング 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。
ワイヤレス	次のシステムモニタリング 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 Utilization	• 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。

パラメータ	スコアの計算
Memory Utilization	• 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。
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 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 ドメインに 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。「Enable SNMP Collector Metrics for Fabric Devices（123 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 Utilization	• 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。
Memory Utilization	• 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。
Link Errors	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。

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。

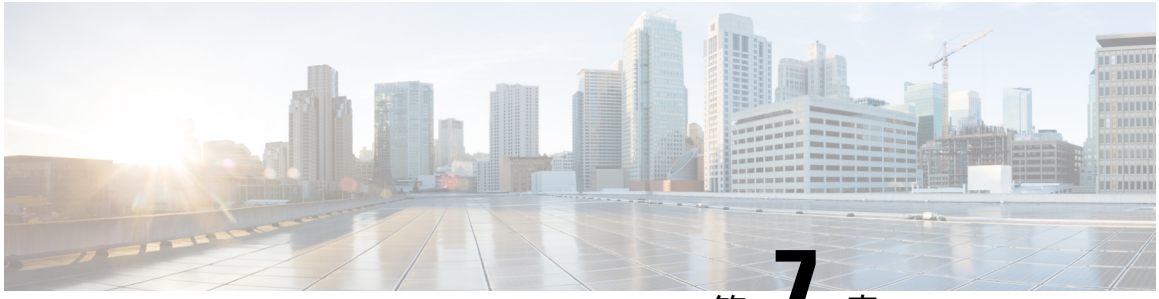
パラメータ	スコアの計算
CPU Utilization	• CPU 使用率が 90 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 90 パーセント以上の場合、スコアは 1 です。
Memory Utilization	• メモリ使用率が 90 パーセント未満の場合、スコアは 10 です。 • 利用可能メモリ率が 90 パーセント以上の場合、スコアは 1 です。
無線使用率スコア	スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。 • 無線使用率が 70 パーセント未満の場合、スコアは 10 です。 • 無線使用率が 70 パーセント以上の場合、スコアは 0 です。

パラメータ	スコアの計算
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 0 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 0 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 0 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 0 です。
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 0 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 0 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
Memory Utilization	• 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 ドメインに 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 7 章

クライアント正常性のモニタ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デバイス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。

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。

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 （19 ページ） を参照してください。

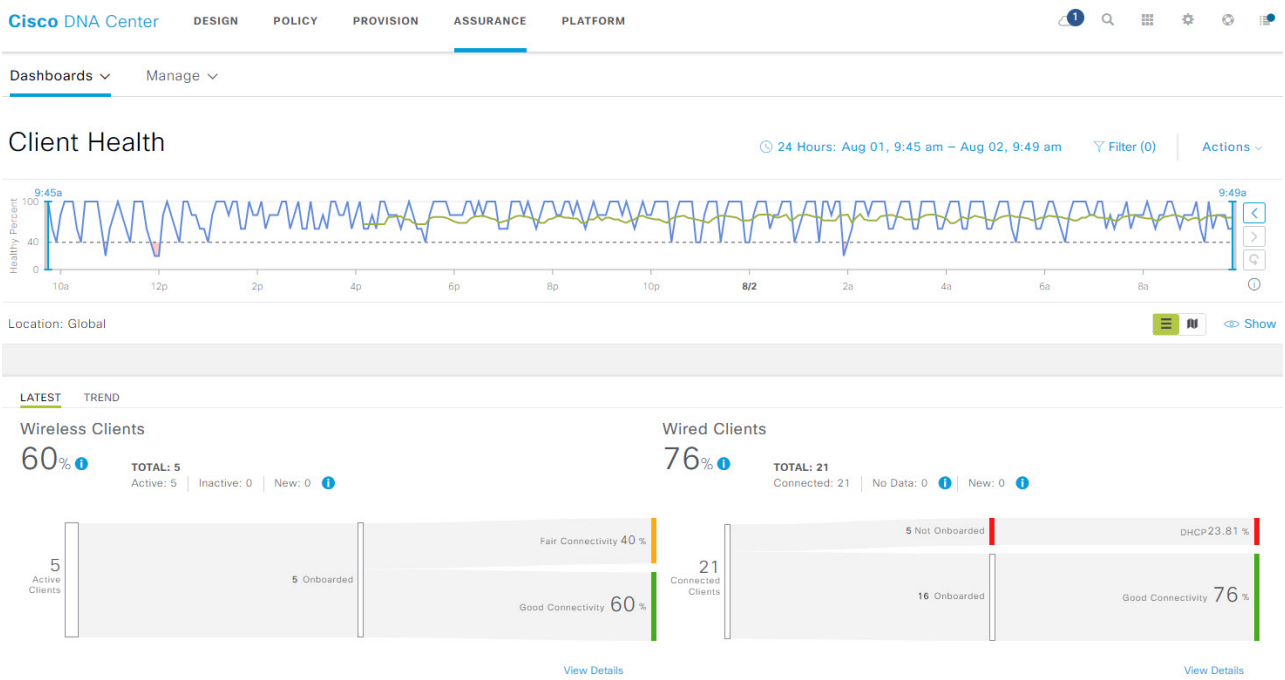
ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Health]** > **[Client Health]** を選択します。

[クライアントの健全性（Client Health）] ウィンドウが表示されます。

図 *16*：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 Health] タイムラインを使用します。

クライアントの正常性タイムライン	
項目	**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.** **[開始日付（Start Date）]**と時刻、**[終了日付（End Date）]**と時刻を指定します。 **3.** [Apply] をクリックします。

クライアントの正常性タイムライン	
項目	説明
Filter	[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、[適用（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 （256 ページ）およびカスタムダッシュボードの作成 （251 ページ）を参照してください。
タイムラインスライダと正常なクライアント比率チャート	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。 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.** アイコンの上にマウスカーソルを合わせます。 **2.** ツールチップで、 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.** **[保存 (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 4 [Location] ペインには、次の機能が用意されています。

[Location] ペイン	
項目	説明
Show Hide	[Location] ペインは、表示または非表示にできます。デフォルトでは、[Location] ペインは非表示になっています。

[Location] ペイン	
項目	説明
	[Hierarchical Site View] と [Building View]：このアイコンをクリックすると、ドロップダウンリストを使用して、サイトまたはビルディング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。
	[Client Health Map]：このアイコ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、提示されるクライアント 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。健全性は 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、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。

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	
項目	**説明**
[Client Health Summary] エリア	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。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 （151 ページ） を参照してください。 • [Total Devices]]：クライアントデバイスの合計数、およびアクティブ、非アクティブ、新しいクライアントデバイスの数が表示されます。 （注） 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。これらのクライアントのヘルス スコアは、次の 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]：トレンドチャートが表示されます。このトレンドチャートは、一定の期間にわたるクライアントの健全性を示します。 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分類されて示されます。たとえば、AAA、DHCP、その他、などです。 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。
[詳細の表示（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セグメントをクリックすると、次が表示されます。 • 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 ネットワーク上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	
項目	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たオンボーディング時間のチャートが表示されます。 **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分類されて示されます。たとえば、AAA、DHCP、その他、などです。

[Client Onboarding Times] ダッシュレット	
項目	説明

[詳細の表示（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**チャート**には、次の 2 つのタブがあります。
	  • **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。
	  左側の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]、[AAA]、および [DHCP] データの場合は、[Client Count]、[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。
	• 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	
項目	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。

[Connectivity RSSI] ダッシュレット	
項目	説明
[詳細の表示（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	
項目	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。
[詳細の表示（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	
項目	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。
[詳細の表示（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	
項目	**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た SSID 基準チャートが表示されます。 **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。
[詳細の表示（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。 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	
項目	**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。

[Connectivity Physical Link] ダッシュレット	
項目	説明
[詳細の表示（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	
項目	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。
[詳細の表示（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	
項目	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リングするには、[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。
[詳細の表示（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 ネットワーク上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	
項目	説明
[TYPE]	クライアントタイ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、[Wired] および [Wireless] クライアントです。
[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。
[DATA]	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 >= 10s：オンボーディング時間が 10 秒（しきい値）以上。 • Association >= 5s：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 >= 5s：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	
項目	**説明**
[Client Device] テーブル	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 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 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 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。 識別子列には、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。 • [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。 • **デバイス タイプ** • [Health]：このスコアは、オンボーディングスコアと接続済みスコアの平均です。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。 • **前回の検出（Last Seen）** • AP Name]（ワイヤレスクライアントの場合のみ）：これはアクセスポイント名です。 • [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） ⋮ 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。

[Client Devices] ダッシュレット	
項目	説明
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。 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。

Monitor and Troubleshoot the Health of a Client Device

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。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

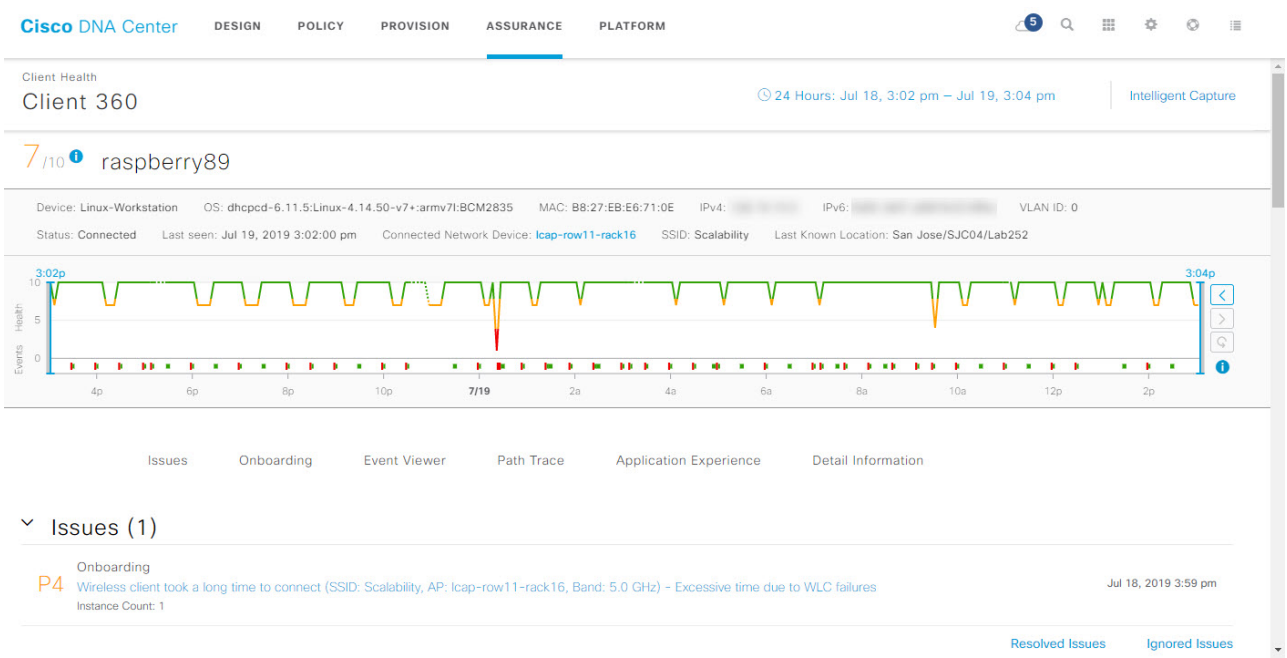
ステップ 2 **[Dashboards]** > **[Health]** > **[Client Health]** を選択します。
[Client Health] ダッシュボードが表示されます。

ステップ 3 次のいずれかを実行します。

- [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。
- [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 *17 : [クライアント 360（Client 360）] ウィンドウ*



ステップ 4 右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) 開始日時と終了日時を指定します。

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、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 （221 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 個々のクライアントの正常性スコアがクライアント名の左側に表示されます。

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 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 （153 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 7 タイムラインの上に表示される [Client 360] ヘッダーで、デバイスに関する最新情報を確認できます。

- 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、IPv4 および IPv6 アドレス、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、および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、この領域には、MAC アドレス、IPv4 および IPv6 アドレス、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、および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。

ステップ 8 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。

- [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 9 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. [Status] 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、解決済みの問題の一覧が表示されます。 • 問題を無視するには、次の手順を実行します。 1. [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。 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 （259 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** • **[削除（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 （150 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
[新しいパストレースの実行（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 （157 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。 シスコ アプリケーション エクスペリエンスについて （161 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 （167 ページ）を参照してください。

詳細情報のカテゴリ
[Device Info]、[RF]（ワイヤレスクライアントのみ）、[Connectivity] タブがあります。各タブをクリックして、適切な情報を取得します。 （注） Samsung デバイスについては、[Device Info] 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。 （注） Apple 製デバイスの場合、[iOS 分析（iOS Analytics）] タブも表示されます。

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。

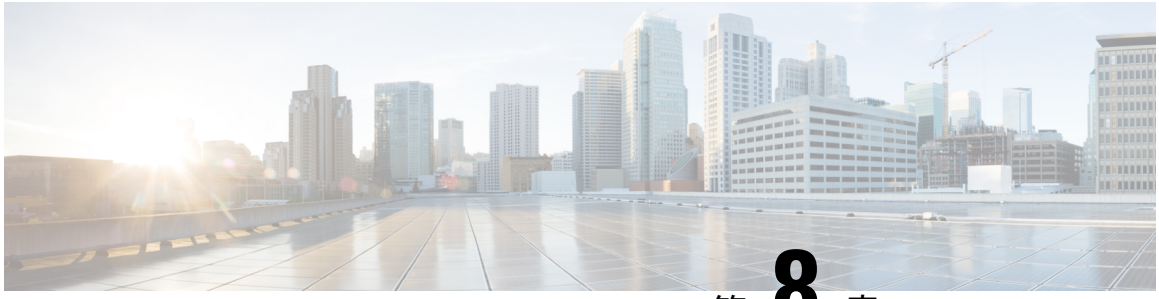
個別のクライアント ヘルス スコア

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

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）のパストレースは、サポートされていません。これは、Cisco ASA が CDP をサポートしていないためです。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 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。
- IPv6 アドレスのパストレース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。
- SDA 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。
- 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。
- 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。[クライアント 360（Client 360）] または [デバイス 360（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 （155 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。Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 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 [クライアント 360（Client 360）] または [デバイス 360（Device 360）] ウィンドウの [パス トレース（Path Trace）] カテゴリで、[新しいパス トレースの実行（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	Action
[送信元（Source）] フィールド	[送信元（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。 • [送信元（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。
[インターフェイス（オプション）（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。
[ポート（オプション）（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。 • [宛先（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。
[インターフェイス（オプション）（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） [宛先（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。
[ポート（オプション）（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 [オプション（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	Action
[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。
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。

フィールド	Action
ACL トレース	（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。
[統計を含める（Include Stats）] のオプション	（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 **[開始（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) デバイスの上にカーソルを重ねると、CPU およびメモリの使用率が表示されます。

[ACL トレース（ACL Trace）] が [オン（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。

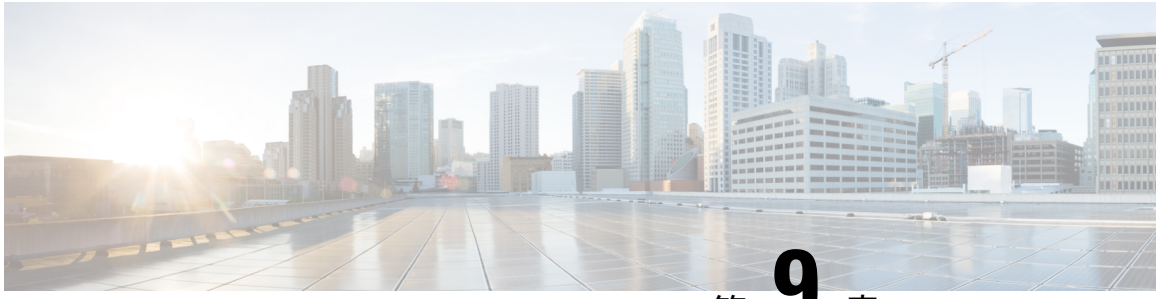
次の 5 タプル値（送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、使用されているプロトコル）が指定されている場合、表示されている ACL トレースは 100% 正確です。情報が部分的に指定されている場合、表示されている ACL トレースはベストエフォートに基づきます。このような場合、ACL 結果に許可と拒否の両方が表示される可能性があります。

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 9 章

Monitor Application Health

シスコ アプリケーション エクスペリエンスについて

Cisco アプリケーションエクスペリエンス（AX）では、アプリケーションの健全性をモニタできます。アプリケーションの正常性は、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）に基づいて計算されるスコア値を使用して測定されます。

AX は、ルータ、スイッチ、WLC によってエクスポートされるアプリケーションの可視性レコードに基づいています。アプリケーションクライアントサーバの統計情報、アプリケーション応答時間、およびメディアタイプのモニタを含むアプリケーションパフォーマンスプロファイルのみがサポートされます。

アプリケーションの関連性に基づいて、ビジネス関連、ビジネスと無関係、またはデフォルトとして分類されます。この分類は NBAR 標準規格に基づいて行われます。Cisco Digital Network Architecture Center ユーザガイド [英語] の「Business-Relevance Groups」を参照してください。

AX を表示するには、シスコのネットワークデバイスでアプリケーションの可視性を有効にする必要があります。アプリケーションの可視性の有効化 （162 ページ） を参照してください。

（注） Cisco DNA Center ルータ、スイッチ、および WLC におけるアプリケーションの可視性の設定をサポートします。この ID は、[Device Role] の下の [Inventory] ウィンドウで確認できます。Cisco DNA Center

アプリケーションの可視性の有効化

定性的メトリックと定量的メトリックにより、ネットワークデバイス上で実行されているアプリケーションを表示するには、デバイス上でアプリケーションの可視性を有効にする必要があります。次の手順を実行します。

1. デバイスインターフェイスにキーワード `lan` を含む説明を追加します。これは、デバイスインターフェイス上で手動で設定することも、Cisco DNA Center の [Template Editor] ツールを使用して設定することもできます。
2. ネットワークデバイスを再同期して、このインターフェイスの説明を読み取ります。**ネットワークテレメトリ**ツールは、説明に `lan` が含まれるインターフェイスを検索し、アプリケーションの可視性の設定をそれらのインターフェイスだけに適用します。
3. インターフェイス上で IP アドレスを設定します。このインターフェイスは、管理目的で使用しないでください。
4. **最大可視性**プロファイルをネットワークデバイスに適用します。「デバイスにテレメトリプロファイルを適用 （166 ページ）」を参照してください。

（注）

- **ルータ**：アプリケーションの可視性は、説明に `lan` が含まれていて、IP アドレスがある非管理インターフェイスにのみ適用されます。
- **スイッチ**：アプリケーションの可視性は、説明に `lan` が含まれるインターフェイスにのみ適用されます。
- **ワイヤレスコントローラ**：Cisco AireOS WLC でアプリケーションの可視性を有効にするには、SSID プロファイル名にキーワード `lan` を含める必要があります。

（注）

- ルータおよびスイッチは、NetFlow の標準バージョンである IP Flow Information Export （IPFIX）を使用して、アプリケーションエクスペリエンステレメトリを Cisco DNA Center に送信します。
- シスコ ワイヤレス コントローラは、ワイヤレス サービス アシュアランス（WSA）のストリーミングテレメトリを使用して、Cisco DNA Center にアプリケーション エクスペリエンス テレメトリを送信します。

アプリケーションの可視性がサポートされているデバイス

アプリケーションの可視性をサポートする Cisco Catalyst 9200 シリーズ スイッチを次の表に示します。

（注） アプリケーションの可視性は、説明に `lan` が含まれるインターフェイスにのみ適用されます。

サポート対象の **Cisco Catalyst 9200** シリーズ スイッチ		
デバイス	推奨される **IOS-XE** ソフトウェアバージョン	サポート対象 **IOS-XE** ソフトウェアの最小バージョン
Cisco Catalyst 9200-24P	16.10.1	16.10.1
Cisco Catalyst 9200-24T	16.10.1	16.10.1
Cisco Catalyst 9200-48P	16.10.1	16.10.1
Cisco Catalyst 9200-48T	16.10.1	16.10.1
Cisco Catalyst 9200L-24P-4G	16.10.1	16.9.1
Cisco Catalyst 9200L-24P-4X	16.10.1	16.9.1
Cisco Catalyst 9200L-24T-4G	16.10.1	16.9.1
Cisco Catalyst 9200L-24T-4X	16.10.1	16.9.1
Cisco Catalyst 9200L-48P-4G	16.10.1	16.9.1
Cisco Catalyst 9200L-48P-4X	16.10.1	16.9.1
Cisco Catalyst 9200L-48T-4G	16.10.1	16.9.1
Cisco Catalyst 9200L-48T-4X	16.10.1	16.9.1

アプリケーションの可視性をサポートする Cisco Catalyst 9300 シリーズ スイッチを次の表にを示します。

（注） アプリケーションの可視性は、説明に `lan` が含まれるインターフェイスにのみ適用されます。

サポート対象の Cisco Catalyst 9300 シリーズ スイッチ		
デバイス	推奨される IOS-XE ソフトウェアバージョン	サポート対象 IOS-XE ソフトウェアの最小バージョン
Cisco Catalyst 9300 Stack	16.6.3	16.6.3
Cisco Catalyst 9300-24P	16.6.3	16.6.2
Cisco Catalyst 9300-24T	16.6.3	16.6.2
Cisco Catalyst 9300-24U	16.6.3	16.6.2
Cisco Catalyst 9300-24UX	16.6.3	16.6.2
Cisco Catalyst 9300-48P	16.6.3	16.6.2
Cisco Catalyst 9300-48T	16.6.3	16.6.2
Cisco Catalyst 9300-48U	16.6.3	16.6.2
Cisco Catalyst 9300-48UN	16.6.3	16.6.2
Cisco Catalyst 9300-48UXM	16.6.3	16.6.2

アプリケーションの可視性をサポートする Cisco Catalyst 9400 シリーズ スイッチを次の表に示します。

（注） アプリケーションの可視性は、説明に`lan`が含まれるインターフェイスにのみ適用されます。

サポート対象の Cisco Catalyst 9400 シリーズ スイッチ		
デバイス	推奨される IOS-XE ソフトウェアバージョン	サポート対象 IOS-XE ソフトウェアの最小バージョン
Cisco Catalyst 9400（Sup1E）	16.6.3	16.6.2
Cisco Catalyst 9400-SUP-1	16.6.3	16.6.2
Cisco Catalyst 9400-SUP-1XL	16.6.3	16.6.2
Cisco Catalyst 9407R	16.6.3	16.6.2
Cisco Catalyst 9410R	16.6.3	16.6.2

アプリケーションの可視性をサポートするシスコルータを次の表に示します。

（注） アプリケーションの可視性は、説明に`lan`が含まれていて、IPアドレスがある非管理インターフェイスにのみ適用されます。

サポートされる Cisco ルータ	
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 1000 シリーズ サービス統合型ルータ（ISR1K）	IOS XE Denali リリース 16.3
Cisco 4000 シリーズ サービス統合型ルータ（ISR4K）	IOS XE Denali リリース 16.3
Cisco CSR 1000v シリーズ クラウド サービス ルータ（CSR 1000v）	IOS XE Denali リリース 16.3
Cisco 1000 シリーズ アグリゲーション サービス ルータ（ASR1K）	IOS XE Denali リリース 16.3

アプリケーションの可視性をサポートする Cisco AireOS WLCs を次の表に示します。

（注） Cisco AireOS WLCs でアプリケーションの可視性を有効にするには、SSID プロファイル名にキーワード `lan` を含める必要があります。

サポート対象の Cisco AireOS WLCs	
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 AireOS WLCs	8.8 MR2 - 8.8.114.130 以上のバージョン （注） AireOS 8.9.x は、アプリケーションの可視性をサポートしていません。

関連トピック

Cisco Catalyst 9000 シリーズ スイッチにおけるアプリケーションの可視性の制限事項 （165 ページ）

Cisco Catalyst 9000 シリーズ スイッチにおけるアプリケーションの可視性の制限事項

Catalyst 9000 シリーズ スイッチには、次の制限事項があります。

- サポート対象の Cisco Catalyst 9000 シリーズ スイッチモデル、および IOS-XE ソフトウェアの最小バージョンと推奨バージョンについては、「アプリケーションの可視性がサポートされているデバイス （163 ページ）」を参照してください。
- アプリケーションの可視性は、アクセスロールのスイッチでのみサポートされます。

- 「switchport mode access」ポートのみがサポートされます。
- ポートは ETA に対して有効にできません。
- トランクモードはサポートされません。
- ポートチャネル インターフェイスはサポートされません。
- IPv4 フローのみがモニタされます。
- 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。
- Cisco DNA Advantage ライセンスが必要です。

テレメトリの設定

テレメトリについて

テレメトリ ツールを使用すると、健全性のモニタリングやアクセス用にデバイスのプロファイルを設定および適用できます。

デバイスにテレメトリ プロファイルを適用

テレメトリツールを使用して、テレメトリ アセスメント プロファイルをネットワークデバイスに適用できます。

始める前に

Cisco DNA Centerを使用して、ネットワーク内のデバイスを検出します。

デバイスでアプリケーションの可視性を有効にするには、インターフェイスの説明の下にキーワード `lan` を追加してください。

ステップ 1 Cisco DNA Center のホームページで、[Tools] の [Network Telemetry] をクリックします。

[テレメトリ（Telemetry）] ウィンドウが表示されます。

ステップ 2 [サイトの表示（Site View）] タブをクリックします。

ステップ 3 このタブの [サイト ビュー（Site View）] テーブルを確認します。

次の情報が表示されます。

- [Device Name]：デバイスの名前。
- [Address]：デバイスの IP アドレス。
- [Type]：デバイスの種類。

- [Family]：デバイスのカテゴリ（スイッチ、ルータ、アクセスポイントなど）。
- [Version]：デバイスで現在実行中のソフトウェアバージョン。
- [Profile]：デバイスに適用されたテレメトリプロファイル。
- [Details]：デバイスのテレメトリアセスメント。

ステップ 4 デバイスの [デバイス名（Device Name）] の隣のチェック ボックスをオンにして、そのデバイスにテレメトリ プロファイルを追加します。

ステップ 5 [Actions] ボタンをクリックして、ドロップダウンリストからテレメトリプロファイルを選択します。

アプリケーション エクスペリエンスを有効にするには、デバイスの [Maximal Visibility] プロファイルを選択する必要があります。

次のタスク

Cisco DNA Center この手順で設定されたテレメトリプロファイルは、キャプチャするデータタイプを判別するために Cisco DNA Center で使用されます。これらのデータタイプは、ネットワーク デバイスの状態の監視に使用されます。

ネットワークデバイスの正常性をチェックするために、Cisco DNA Assurance にアクセスして [Health]**アシュアランス** と [Issues]**アシュアランス** の両方を確認します。

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。Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 ページ）を参照してください。
- ネットワークデバイスでのアプリケーションの可視性を有効にします。アプリケーションの可視性の有効化 （162 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時間（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、パケット損失と遅延のメトリックの組み合わせに基づいて計算されます。
- [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。
- [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 9K スイッチまたは Cisco AireOS WLC によってエクスポートされたアプリケーション エクスペリエンス 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を提供します。

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。アプリケーションエクスペリエンスは、ルータ、Cisco Catalyst 9K スイッチ、および Cisco AireOS WLC でサポートされています。

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。Discover Your Network Using an IP Address Range （31 ページ

ジ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 ページ）を参照してください。

- ネットワークデバイスでのアプリケーションの可視性を有効にします。アプリケーションの可視性の有効化 （162 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) 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時間（24 Hours）] です。

b) 適切なフィルタを使用して、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 データをフィルタリングします。フィルタは、[All VRFs] および [All Interfaces] です。

（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、パケット損失と遅延のメトリックの組み合わせに基づいて計算されます。
- [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。
- [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]、および [Application Server Latency] です。

（注） Cisco Catalyst 9K スイッチまたは Cisco AireOS WLC によってエクスポートされたアプリケーション エクスペリエンス 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を提供します。

すべてのアプリケーションの健全性のモニタ

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。Discover Your Network Using an IP Address Range （31 ページ）、CDP を使用したネットワークの検出 （25 ページ）、またはLLDP を使用したネットワークの検出 （37 ページ）を参照してください。
- デバイスでアプリケーションの可視性の収集を有効にします。アプリケーションの可視性の有効化 （162 ページ） を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboard]** > **[Health]** > **[Application Health]** の順に選択します。

[Application Health] ダッシュボードが表示されます。

ステップ 3 次の機能には、[Application Health] タイムラインを使用します。

[Application Health] タイムライン	
項目	**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.** **[開始日付（Start Date）]**と時刻、**[終了日付（End Date）]**と時刻を指定します。 **3.** [Apply] をクリックします。

[Application Health] タイムライン	
項目	説明
Actions	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（256ページ）およびカスタム ダッシュボードの作成（251 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。

ステップ 4 [Location] ペインには、次の機能が用意されています。

[Location] ペイン	
項目	説明
Show Hide	[Location] ペインは、表示または非表示にできます。デフォルトでは、[Location] ペインは非表示になっています。
	この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。

ステップ 5 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	
項目	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 （178 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 6 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	
項目	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	
項目	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。Monitor the Health of an Application （175 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	
項目	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。

Monitor the Health of an Application

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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboard]** > **[Health]** > **[Application Health]** の順に選択します。
[アプリケーションの健全性（Application Health）] ウィンドウが表示されます。

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 正常性タイムラインでは、次の操作を実行できます。

[Application 360 Health] タイムライン	
項目	説明
時間範囲の設定	ダッシュボードの指定された時間範囲内のアプリケーション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.** **[開始日付（Start Date）]**と時刻、**[終了日付（End Date）]**と時刻を指定します。 **3.** [Apply] をクリックします。
[Location] フィルタ	ドロップダウンリストから選択したロケーションのアプリケーション情報を表示します。
[Business Relevance] フィールド [Traffic Class] フィールド [カテゴリ（Category）] フィールド	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。
アプリケーションの正常性タイムラインスライダ	アプリケーションの正常性スコアを、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、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 5 [Issuce] カテゴリの問題に関する情報を確認できます。

a) 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、影響範囲、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。

b) 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. [Status] 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、解決済みの問題の一覧が表示されます。
- 問題を無視するには、次の手順を実行します。
  1. [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。

問題の詳細については、問題の表示と管理 （259 ページ）を参照してください。

ステップ 6 [Application Experience）] カテゴリでアプリケーション エクスペリエンス データを確認できます。

アプリケーション エクスペリエンスのカテゴリ	
カラム	説明
[Source Location]	特定のアプリケーションにアクセスしているクライアントサイト。 ネットワークデバイスのオプションボタンをクリックすると、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。 • メトリック（スループット、パケット損失、ジッター、ネットワーク遅延、クライアントネットワーク遅延、サーバネットワーク遅延、およびアプリケーションネットワークの遅延）のチャートを表示します。 • アプリケーションにアクセスしているクライアントを表示します。各クライアントの詳細情報が示されます。これには、クライアントの正常性スコア、MAC アドレス、IP アドレス、使用率などが含まれます。
ヘルス（**Health**）	正常性スコアはパケット損失と遅延のメトリックの組み合わせに基づいて計算されます。 （注） このメトリックは、Cisco Catalyst 9K スイッチおよび Cisco AireOS WLC では使用できません。
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。
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。
[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、Cisco Catalyst 9K スイッチおよび Cisco AireOS WLC では使用できません。
ネットワーク遅延	ネットワークの遅延時間（最大と平均）（ミリ秒単位）。 （注） このメトリックは、Cisco Catalyst 9K スイッチおよび Cisco AireOS WLC では使用できません。
ジッタ	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、Cisco Catalyst 9K スイッチおよび Cisco AireOS WLC では使用できません。

ステップ 7 （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 8 （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)

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 10 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 サーバと直接通信します。

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

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

サポート対象のセンサーとワイヤレスコントローラ	最小ソフトウェア リリース
シスコ ワイヤレス コントローラ（35xx、55xx、85xx）	8.5.115.0
Cisco Aironet 1800s アクティブ センサー	8.8.263.0

サポート対象の Cisco Aironet 1800s アクティブセンサーリリース

サポート対象の Cisco Aironet 1800s アクティブセンサーと推奨される Cisco DNA Center のソフトウェアリリースを次の表に示します。

注目 この表に記載されている Cisco Aironet 1800s アクティブ センサーの最小ソフトウェアリリースを使用していることを確認します。上位の Cisco Aironet 1800s アクティブ センサーのソフトウェア リリースには互換性がありません。

サポート対象の Cisco Aironet 1800s アクティブセンサーのソフトウェアリリース	推奨される Cisco DNA Center のソフトウェアリリース
1.3.3.0	1.3.3.x 以降
1.3.1.2	1.3.1.2
8.8.263.0	1.3.0.3 以前（1.2.x など）

センサーのプロビジョニング

Provision the Wireless Cisco Aironet 1800s Active Sensor

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。バックホールの設定の管理（198 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（183 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（183 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（198 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（184 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 WebUI 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] エリアで、[Service Status] トグルボタンを [Enabled] に設定します。

b) [Provisioning] エリアで [Provisioning] トグルボタンを [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、実行する必要のあるアクションに関する情報が示されています。

ステップ 6 [CiscoSensorProvisioning] という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] 列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

デバイスを要求すると、デバイスにネットワークプロファイルを割り当て、それをインベントリに追加することで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。

デバイスが要求される場合、Cisco DNA Center からのシステム構成 CLI コマンドの一部はまずデバイスにプッシュされてから、定義した [Onboarding Configuration (Day-0)] テンプレートにプッシュされます。[Onboarding Configuration] テンプレートに同じ CLI コマンドがある場合、

これらは最後に適用されるため、システム設定が上書きされます。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報（CLI および SNMP）
- SSH v2 および SCP サーバの有効化
- HTTP および HTTPS サーバの無効化

（注） デバイスのデバイス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ときに次の設定が追加されます。

- SNMP、NETCONF、Cisco TrustSec（CTS）ログイン情報
- IPDT の有効化
- コントローラ証明書
- SNMP トラップサーバ定義
- Syslog サーバ定義
- NetFlow コレクタ定義
- ワイヤレス ネットワーク アシュアランス

この手順では、メインの [プラグアンドプレイ（Plug and Play）] タブ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、[要求（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、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語]』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。About Network Hierarchy （46 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。
- 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 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

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 デバイステーブルの上にあるメニューバーで、**[アクション（Actions）]** > **[要求（Claim）]** の順に選択します。

[デバイスの要求（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。

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、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 **[次へ (Next)]** をクリックします。
[設定（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 設定するデバイスの名前をクリックし、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、**[RF プロファイル（RF Profile）]** ドロップダウンリストで、デバイスに適用する RF 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) For a Mobility Express device, enter values in the following fields：**Management IP**, **Subnet Mask**, and **Gateway**.

e) ワイヤレスセンサーデバイスの場合、**[センサーの設定（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 プロファイルを選択します。

f) 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。

g) **[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 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 12 **[次へ (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 13 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 プレビューステータス（Day-0 Config Preview Status）]** 列をチェックします。

プレビューでエラーが表示された場合は、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。[設定（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。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 14 [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 15 **[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。センサー主導テストの作成と実行（レガシー）（201 ページ）またはセンサー主導テストの作成と実行（テンプレート）（206 ページ）を参照してください。

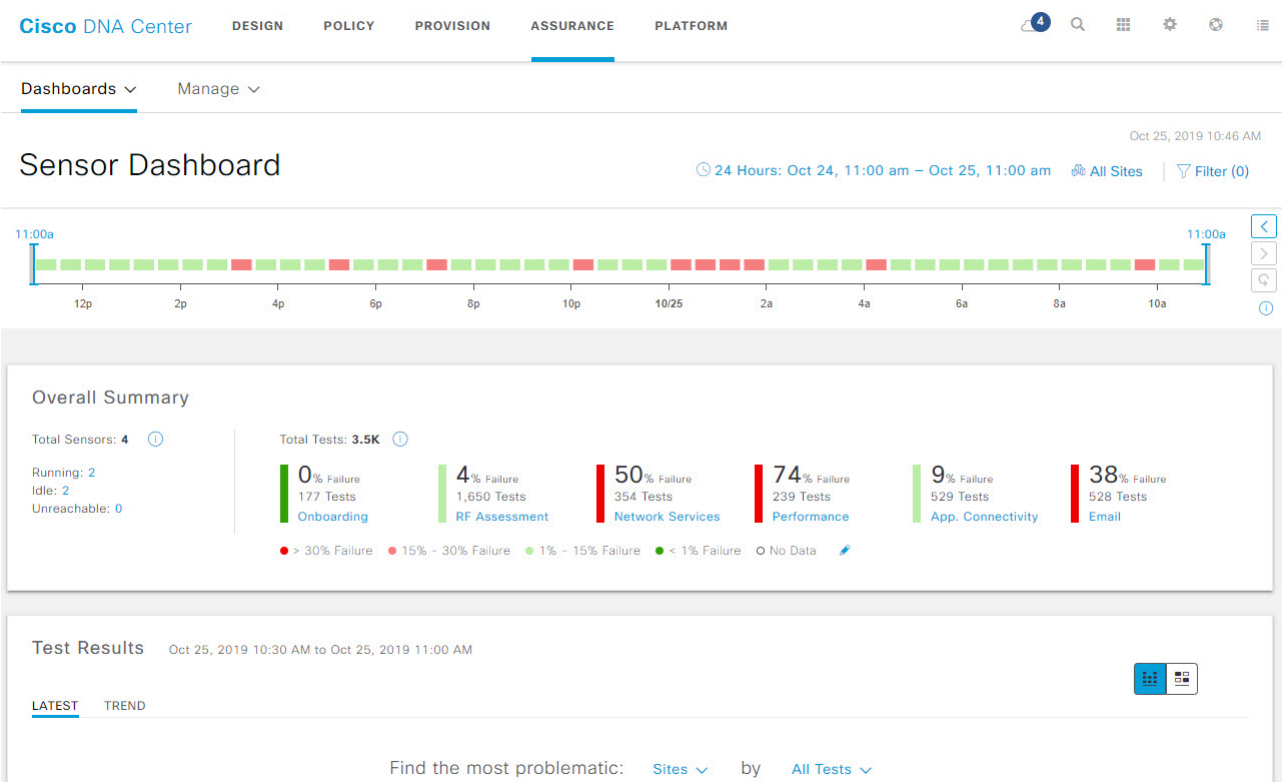
ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Wireless Sensor]** の順に選択します。

[Sensor Dashboard] ダッシュボードが表示されます。

図 *18 : Sensor Dashboard*



ステップ 3 [Sensor Dashboard Timeline] には、次の機能が用意されています。

タイムラインエリア	
項目	**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.** **[開始日付（Start Date）]**と時刻、**[終了日付（End Date）]**と時刻を指定します。 **3.** [Apply] をクリックします。

タイムラインエリア	
項目	**説明**
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。
Filter	このフィルタ処理では、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 をクリックします。 **2.** [Clear Filters] をクリックします。
全体テスト失敗率の**タイムライン**	タイムラインには、時間範囲内の特定の時刻に全体テストが失敗した割合が表示されます。時間範囲は、タイムラインの上にある [Time Range] によって決まります。 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	
項目	**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とトラブルシューティング（194ページ）」を参照してください。

[Overall Health Summary] ダッシュレット	
項目	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。 **オンボーディング** **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** **Email** 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。 ● > 30% Failure ● 15% - 30% Failure ● 1% - 15% Failure ● < 1% Failure 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.** 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	
項目	**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	このトグルにより、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	
項目	説明
カードビュー	カード形式でデータが表示され、高レベルのモニタリングと比較が可能です。 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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Wireless Sensor]** を選択します。

[Sensor Dashboard] が表示されます。

ステップ 3 [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。

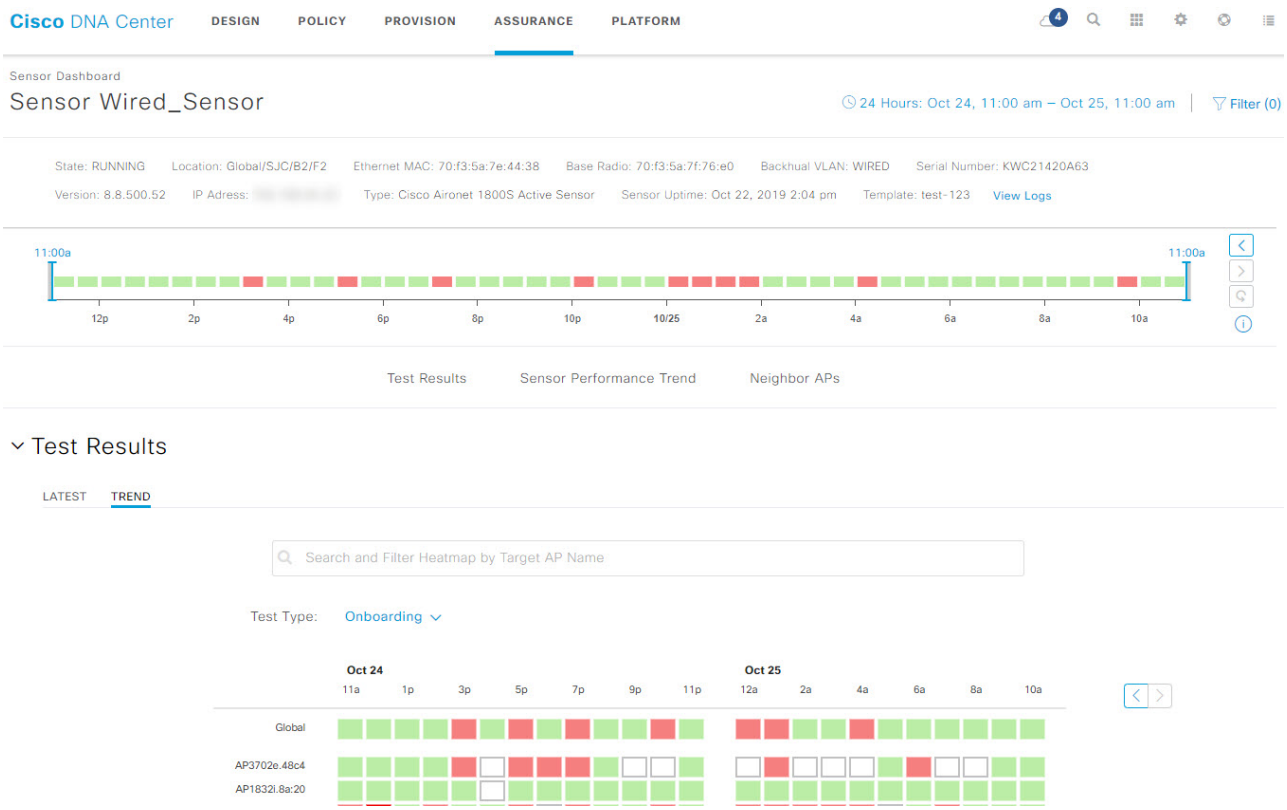
  スライドインペインで、テーブルからセンサーのハイパーリンク名をクリックします。

- [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。

図 *19* : センサーの *360* 度ビュー



ステップ 4 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 5 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 6 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 7 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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Sensors]** > **[Sensor List]** を選択します。

[Sensor List] ウィンドウが開き、ネットワーク内のオンボード済みセンサーが表示されます。

ステップ 3 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 4 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 5 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 6 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 7 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 8 Save をクリックします。

ステップ 9 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にカーソルを合わせて、[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。

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 （199 ページ） を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Sensors]** > **[Backhaul Settings]** の順に選択します。

[Backhaul Settings] ウィンドウが表示されます。

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] ウィンドウが開きます。

b) [Create Sensor Backhaul SSID Assignment] ウィンドウで、次の設定を行います。

- [Settings Name]：バックホール SSID の名前を入力します。

- [Wireless Network Name (SSID)]：このバックホール SSID に使用するワイヤレスネットワーク（SSID）を選択します。
- [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。

セキュリティオプション	説明
WPA2 企業	ユーザ認証に Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）セキュリティを使用します。 ドロップダウンリストから [EAP method] を選択します。 EAP-TLS を選択した場合は、証明書とそのパスワードが必要です。証明書をアップロードするには、[Certificate] ドロップダウンメニューをクリックしてから、Add New Certificate Bundle をクリックします。
WPA2 パーソナル	ユーザ認証に WP2A 暗号化事前共有キー（PSK）を使用します。 [Password] フィールドに使用する PSK を入力します。
オープン（Open）	セキュリティまたは認証は使用されません。

c) **[保存（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、リリース 1.3.3.0 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。

次の表には、Cisco DNA Center、リリース 1.3.1.0 以前のリリースと Cisco DNA Center、リリース 1.3.3.0 の違いとメリットが表示されています。

Cisco DNA Center、リリース 1.3.1.0 以前のリリース	Cisco DNA Center、リリース 1.3.3.0
センサではワイヤレステストとワイヤレスバックホール接続の両方に、単一の MAC アドレス（ベース無線 MAC + 0x11）が使用されます。	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。
センサでは単一の同時無線操作が使用されます。	センサ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。
センサとネットワークとの接続は頻繁に確立・解除されます。	センサには永続的な同時ワイヤレスバックホール接続が備わっており、ワイヤレスのテストアクティビティに関係なく、ワイヤレス接続は「常にオン」になります。 （注） • 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。

センサー主導テスト

センサー主導テストの作成方法 アシュアランス

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

メソッド	説明
レガシー	アシュアランス リリース1.3.1.0 に実装されているメソッドを使用して、センサー主導テストを作成できます。 「センサー主導テストの作成と実行（レガシー）（201 ページ）」を参照してください。 **注目** アシュアランス リリース 1.3.1.0 では、このメソッドは**テストスイート**と呼ばれていました。
テンプレート	テンプレートを使用してセンサー主導テストを作成できます。 このメソッドにより、再利用可能なセンサー主導テストのテンプレートを作成し、ネットワーク内の複数のロケーションに迅速に展開できます。 「センサー主導テストの作成と実行（テンプレート）（206 ページ）」を参照してください。

センサー主導テストの作成と実行（レガシー）

レガシーメソッドでセンサー主導テストを作成して実行するには、次の手順を実行します。このメソッドは、アシュアランス リリース 1.3.1.0 で導入され、**テストスイート**と呼ばれていました。

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、[インベントリ（Inventory）] で表示されるようにしてください。Provision the Wireless Cisco Aironet 1800s Active Sensor （182 ページ）を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

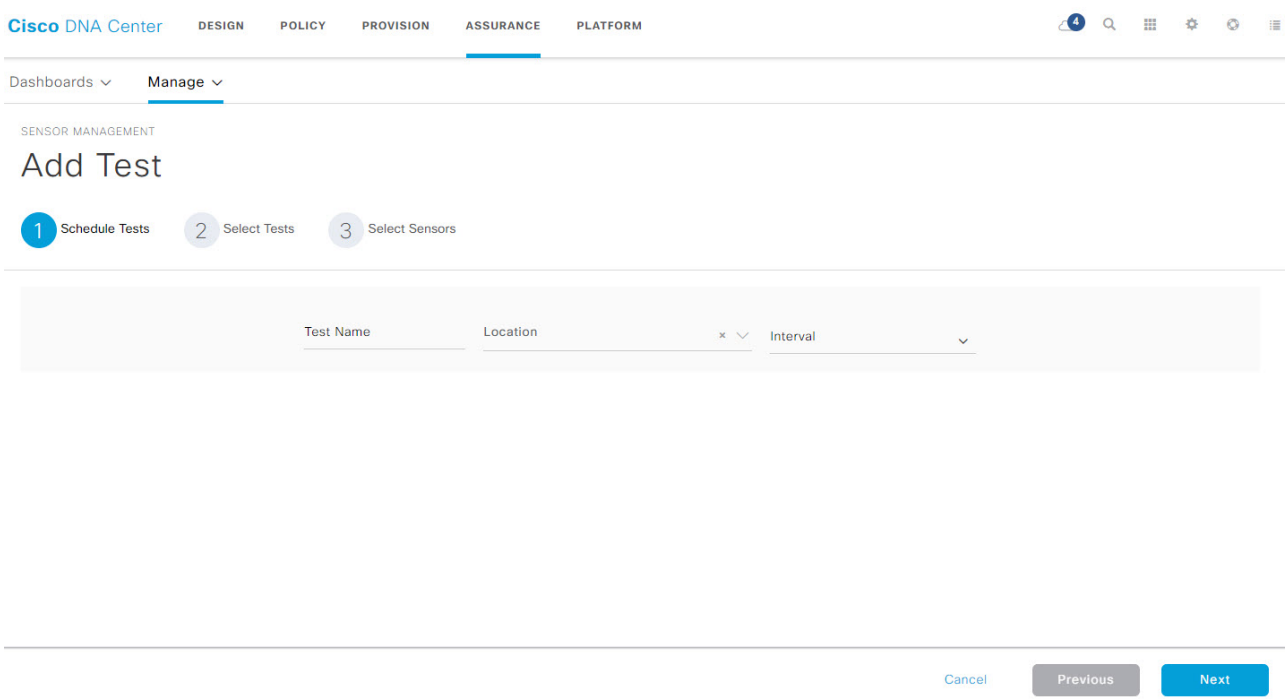
ステップ 2 **[Manage]** > **[Sensors]** > **[Legacy Tests]** の順に選択します。

[Legacy Tests] ウィンドウが表示されます。

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

[Add Test] ウィンドウが表示されます。

図 *20 : [Add Test]* ウィンドウ



ステップ 4 [Schedule Tests] ステップでは、次の設定を行います。

設定	説明
[Test Name] フィールド	テストスイート名を入力します。 （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。

設定	説明
[Location] ドロップダウン リスト	次の手順を実行します。 **1.** ドロップダウンリストからセンサーのロケーションを選択します。 **2.** テストに追加する無線センサーの SSID のチェックボックスをオンにします。 **3.** 必要に応じて、**ログイン情報**を設定します。 **Web 認証対応 SSID に適用** レイヤ 3 セキュリティでは、SSID で **Web 認証**が有効になっている場合、次の機能を使用できます。 • ユーザ認証による **Web 認証**の場合は、必要なログイン情報を入力します。 • **パススルー方式**による **Web 認証**の場合は、メールアドレスの入力を選択できます。 （注） • センサーのテストでは、**内部認証**のみがサポートされています。 • Web 認証は、シスコ ワイヤレス コントローラおよびソフトウェア リリース 8.7 を搭載した Cisco Aironet 1800s アクティブセンサーでサポートされます。 **WPA2 Enterprise 対応 SSID に適用** サポートされるメソッドは、**EAP-FAST**、**PEAP MSCHAPv2**、および **EAP-TLS** です。 EAP-TLS を選択した場合は、証明書とそのパスワードが必要です。証明書をアップロードするには、[Certificate] ドロップダウンメニューをクリックしてから、Add New Certificate Bundle をクリックします。
[Interval] ドロップダウンメニュー	センサーテストのスケジュールを指定します。次のオプションがあります。 • [Daily]：センサーテストは継続的に反復実行されます。デフォルトの間隔は 1 時間です。 • [Once]：センサーテストは、指定された日時に 1 回実行されます。

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

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

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

ネットワークのテスト	
[Test Type]	説明
オンボーディングのテスト	クライアントのオンボーディングテスト（通常、関連付け、AAA、および DHCP を含む）を実行します。 （注） • このオプションはデフォルトで選択されていて、選択解除できません。 • **オンボーディングのテスト**は、Cisco Aironet 1800s アクティブセンサーのソフトウェアリリース 8.8.260.0 以降でサポートされています。
DNS のテスト	ドメイン名の IP アドレスを解決します。
ホストの到達可能性テスト	Internet Control Message Protocol（ICMP）エコー要求を使用して到達可能性を確認します。
RADIUS のテスト	センサーが Dot1x サプリカントとして機能し、ワイヤレスで認証します。Dot1x サプリカントは、Protected Extensible Authentication Protocol（PEAP）と Password Authentication Protocol（PAP） や Microsoft バージョンのチャレンジハンドシェイク認証プロトコル（MS-CHAP）などのプロトコルをサポートしています。

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

パフォーマンステスト	
[Test Type]	説明
速度テスト	ネットワーク診断テスト（NDT）サーバがある場合は、所定のフィールドに NTD サーバの IP アドレスを入力します。NDT サーバがプロキシサーバ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の IP アドレスを入力します。
IPSLA テスト	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。

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

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

電子メールのテスト	
[Test Type]	**説明**
電子メールのテスト	主要な構成は以下のとおりです。 • [POP3]：Post Office Protocol3。POP3 サーバの TCP ポート（110）に接続します。 • [IMAP]：Internet Message Access Protocol。IMAP サーバの TCP ポート（143）に接続します。 • [Outlook Web Server]：Outlook Web サーバ（OWS）にログインします。
Web のテスト	指定された URL へのアクセスと応答データの確認をテストします。
ファイル転送のテスト	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。

ステップ 7 Next をクリックして、**センサーの選択**ステップに進みます。

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

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

     （注）
     - AP は 5 つまで選択できます。
     - センサーのネイバー AP は 30 分ごとに更新されます。

ステップ 9 Next をクリックして、センサーテストを作成します。

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

センサー主導テストの作成と実行（テンプレート）

テンプレートを使用してセンサー主導テストを作成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、テンプレートのコピーを作成して、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

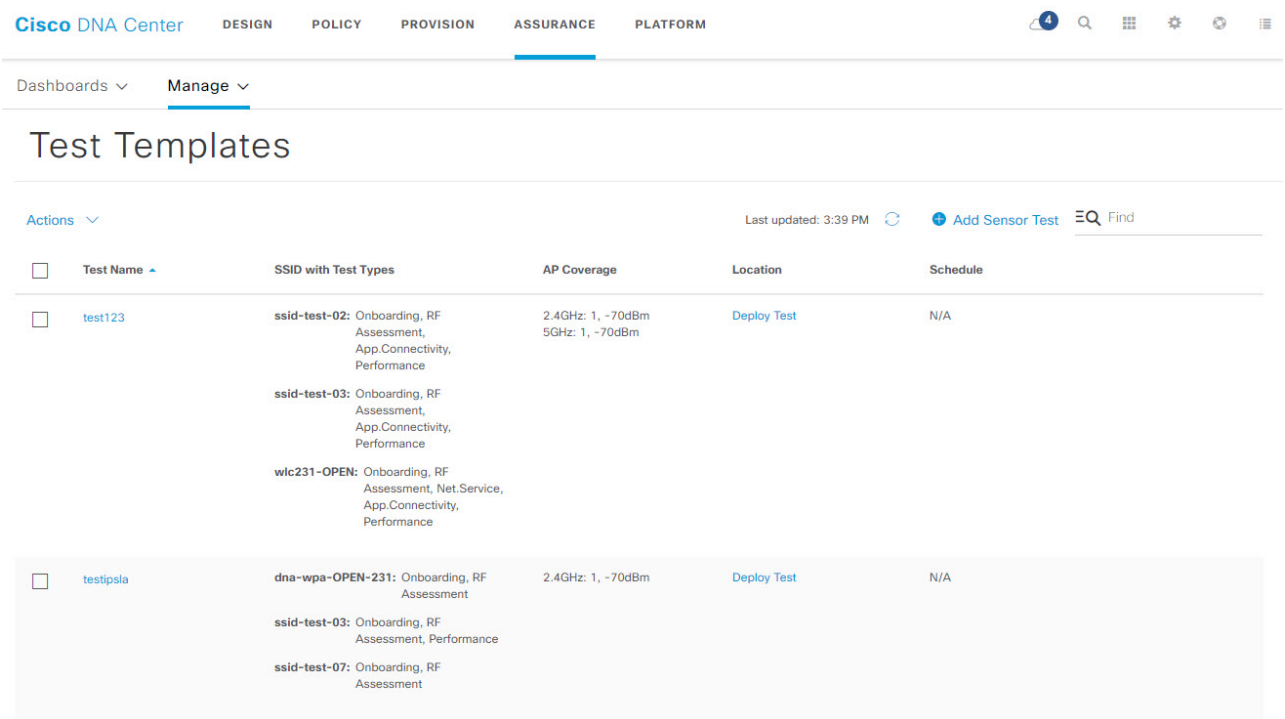
Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[インベントリ（Inventory）] で表示されるようにしてください。Provision the Wireless Cisco Aironet 1800s Active Sensor （182 ページ）を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Sensors]** > **[Test Templates]** を選択します。

[Test Templates ウィンドウが表示されます。



ステップ 3 新しいセンサーテスト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]：テストスイート名を入力します。

  （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、[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、ユーザ名、およびパスワードを入力します。

ステップ 7 Next をクリックします。

ステップ 8 [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）サーバがある場合は、所定のフィールドに NTD サーバの IP アドレスを入力します。NDT サーバがプロキシサーバ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の IP アドレスを入力します。

- [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 サーバの TCP ポート（110）に接続します。
- [IMAP]：Internet Message Access Protocol。IMAP サーバの TCP ポート（143）に接続します。

- [Outlook Web Access]：Outlook Web サーバにログインし、アクセスを検証します。

ステップ 9 Next をクリックします。

ステップ 10 **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） AP は 5 つまで選択できます。

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 11 Next をクリックします。

ステップ 12 [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 13 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 14 [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] をクリックすると、テスト展開の次の手順に進むことができます。

ステップ 15 [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 16 Next をクリックします。

ステップ 17 [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、 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 18 Next をクリックします。

ステップ 19 [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 20 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 21 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テンプレートの実行が開始され、確認のためのダイアログボックスが表示されます。

次のタスク

既存のテストテンプレートを管理します。「センサー主導テストの管理（210ページ）」を参照してください。

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。「センサー主導テストの作成と実行（テンプレート）（206 ページ）」を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Sensors]** > **[Test Templates]** を選択します。
[Test Templates ウィンドウが表示されます。

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]** を選択します。
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]** を選択します。

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]** を選択します。

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 11 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 Connected Mobile Experiences（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 インターフェイス内で、フロア マップ上でのクライアントの正確な場所を把握できます。

CMX の設定は、ユーザの要件に応じて、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 CMX を割り当てることができ、小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 （214 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 ユーザを追加します。Cisco CMX API サーバへのユーザーの追加 （213 ページ）を参照してください。

ステップ 1 Cisco DNA Center のホームページから CMX サーバの詳細を Cisco DNA Center に追加するには、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

[CMX Servers] ウィンドウが表示されます。

ステップ 2 ⊕[Add] をクリックします。

[Add CMX Servers] ウィンドウが表示されます。

ステップ 3 [IP Address] フィールドに、CMX Web GUI の有効な IP アドレスを入力します。

ステップ 4 [User Name] および [Password] フィールドに、CMX Web GUI のユーザ名とパスワードのログイン情報を入力します。

ステップ 5 [SSH User Name] および [SSH Password] フィールドに、CMX 管理者のユーザ名とパスワードの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 6 [Add] をクリックします。

CMX サーバが正常に追加されました。

ステップ 7 サイト、ビル、またはフロアに CMX サーバを割り当てるには、次の手順を実行します。

ステップ 8 **[設計（Design）]** > **[ネットワーク設定（Network Settings）]** > **[ワイヤレス（Wireless）]**を選択します。

ステップ 9 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 10 [CMX Servers] の下で、[CMX Servers] ドロップダウンリストから CMX サーバを選択します。

ステップ 11 **[保存 (Save)]** をクリックします。

[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。

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] の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。[デバイス 360（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ビルディングやフロアの隣にある歯車アイコンをクリックし、[Sync with CMX] を選択して、変更を手動でプッシュします。

ステップ 13 Cisco DNA Center から CMX サーバを編集するには、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

ステップ 14 編集する CMX サーバを選択して変更を加え、[Update] をクリックします。

ステップ 15

ステップ 16 Cisco DNA Center から CMX サーバを削除するには、歯車アイコン（⚙）をクリックし、**[System Settings]** > **[Settings]** > **[CMX Servers]** を選択します。

ステップ 17 削除する CMX サーバを選択し、[Delete] をクリックします。

ステップ 18 [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 12 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。

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
Cisco 5520 ワイヤレス コントローラ	AireOS 8.8

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 8540 ワイヤレス コントローラ	AireOS 8.8

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 16.10.1

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	8.10.105.0	16.12.1 s
Aironet 1560 AP	8.10.105.0	16.12.1 s
Aironet 1815 AP	8.10.105.0	16.12.1 s
Aironet 1830 AP	8.10.105.0	16.12.1 s
Aironet 1840 AP	8.10.105.0	16.12.1 s
Aironet 1850 AP	8.10.105.0	16.12.1 s
Aironet 2800 シリーズ AP	8.8.125.0	16.12.1s
Aironet 3800 シリーズ AP	8.8.125.0	16.12.1s
Aironet 4800 シリーズ AP	8.8.125.0	16.12.1s
Catalyst 9115 AP	8.10.105.0	16.12.1 s
Catalyst 9120 AP	8.10.105.0	16.12.1s

（注）

- 現在、データパケットキャプチャは、Aironet 4800 AP でのみサポートされます。
- 現在、スペクトル解析は、Aironet 1560 AP、Aironet 2800 シリーズ AP、Aironet 3800 シリーズ AP、および Aironet 4800 シリーズ AP でのみサポートされています。スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、Catalyst 9115 AP、および Catalyst 9120 AP ではサポートされていません。Catalyst 9120 AP では、すべてのスペクトル解析が今後のリリースでサポートされる予定です。

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、そのワイヤレスコントローラによって管理されている AP の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 2 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 （221 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 （227 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。「クライアントデバイス向けライブキャプチャセッションの有効化」を参照してください。

クライアント キャプチャ セッションの制限事項

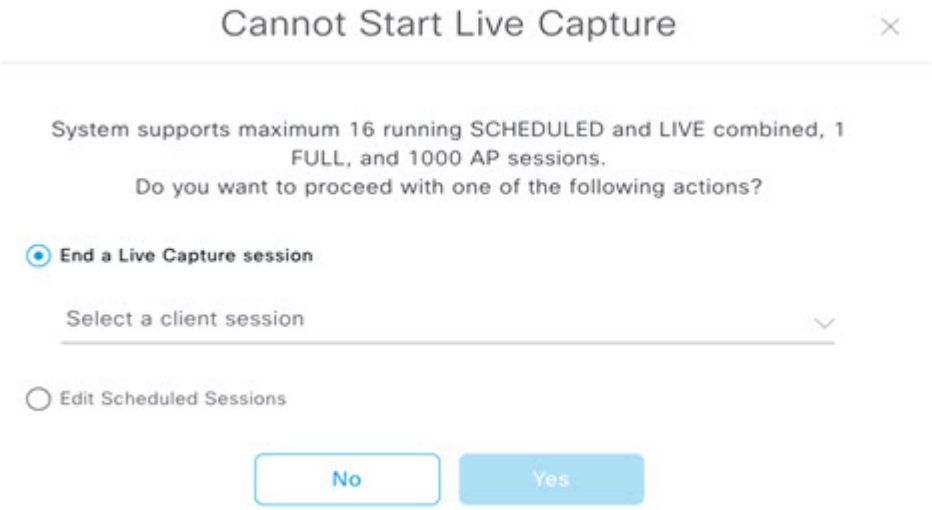
クライアント キャプチャ セッションの制限事項は次のとおりです。

- 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、AP コントローラによって適用されます。16 個のキャプチャセッションを AP コントローラで直接設定した場合、Cisco DNA Center では最大キャプチャセッション数の制限に達していることが認識されないため、Cisco DNA Center ではキャプチャセッションの追加が引き続き許可されます。このような場合、キャプチャセッションが AP コントローラにプッシュされるときにエラーが発生します。

- 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、最も古いパケットファイルから順に、合計サイズが 3.5 GB の制限を下回るまで削除されます。

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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Health]** > **[Client Health]** を選択します。

[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て、特定のクライアントの [Client 360] ウィンドウを開きます。

- [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。
- [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 （246 ページ） で詳細を確認してください。

図 *21* : 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	
項目	**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 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	
項目	**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、「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、「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.** Download PCAP をクリックして、ダウンロードを開始します。 （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。

[Onboarding Events] ダッシュレット	
項目	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	
項目	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 （213 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。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 （230 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 （221 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 （240 ページ） を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Intelligent Capture Settings]** > **[Client Schedule Capture]** を選択します。

[Intelligent Capture Settings - Client Schedule Capture] ウィンドウが表示されます。

ステップ 3 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 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 （219 ページ） を参照してください。

d) **[保存 (Save)]** をクリックします。

ステップ 4 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 5 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 6 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、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。「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（230 ページ）」を参照してください。

このデータを表示するには、Network Analysis Module（NAM）サーバと Cisco DNA Center の統合が必要です。「NAM 統合について （228 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 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 Cisco Aironet 4800 AP 以外の AP にローミングする場合、クライアントが Cisco Aironet 4800 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）サーバに接続されていることを確認します。
- 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。

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 NAM（ネットワーク解析モジュール）または vNAM サーバを使用している場合は、NAM サーバを 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。

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（ネットワーク分析モジュール）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 ユーザインターフェイスから時刻を同期できます。 **[Administration]** > **[System]** > **[System Time]** の順に選択します。

次のタスク

gRPC コレクタを設定します。「gRPC コレクタの設定（230 ページ）」を参照してください。

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（229 ページ）」を参照してください。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Data Platform]** > **[Collectors]** の順に選択します。

[コレクタ（Collectors）] ウィンドウが表示されます。

ステップ 2 [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 3 ⊕ 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 4 [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（229 ページ）の ステップ 5（229 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

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ための手順を紹介します。これには、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、ジッターに関する情報が含まれます。

始める前に

Cisco DNA Center と Network Analysis Module（NAM）サーバを統合します。NAM 統合について（228 ページ）を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Dashboards]** > **[Health]** > **[Client Health]** を選択します。

[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て、特定のクライアントの [Client 360] ウィンドウを開きます。

- [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。
- [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 （246 ページ） で詳細を確認してください。

図 *22 : 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	
項目	**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	
項目	説明
Run Data Packet Capture	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。 （注） データパケットキャプチャは、Cisco Aironet 4800 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 Cisco Aironet 4800 AP 以外の AP にローミングする場合、クライアントが Cisco Aironet 4800 AP に再接続するまで、パケットキャプチャは停止します。 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。 （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	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、Network Analysis Module（NAM）の統合を設定する必要があります。「NAM 統合について （228 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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Intelligent Capture Settings]** > **[Client Data Packet Capture]** の順に選択します。

[Intelligent Capture Settings - Client Data Packet Capture] 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 ID またはホスト名が表示されます。ユーザ 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 アドレス	クライアントデバイスの MAC アドレスが表示されます。
最初のパケット時間	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、最も古いパケットファイルから順に、合計サイズが 1.05 GB の制限を下回るまで削除されます。

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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Manage] > [Intelligent Capture Settings] > [Access Point] を選択します。 > >

[Intelligent Capture Settings - 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。[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 - no APs are enabled	有効になっている AP がない場合は、「None - no APs are enabled」と表示されます。 すべての AP で統計情報キャプチャを有効にできます。
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。

オプション	説明
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 - no APs are enabled	有効になっている AP がない場合は、「None - no APs are enabled」と表示されます。 すべての AP で 異常キャプチャを有効にできます。
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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Health] > [Network] 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。

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。
- [検索（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（246 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（235 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	
項目	**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。

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。
[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。

ダッシュレット	説明
[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 をクリックすると、スペクトル解析セッションが開始されます。

（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	
項目	**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	
項目	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） [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は、その AP には選択されたバンド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 （245 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	
項目	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。 カート内の色は、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。
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。カートは、パーシステント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、Catalyst 9115 AP、および Catalyst 9120 AP ではサポートされていません。Catalyst 9120 AP では、すべてのスペクトル解析が今後のリリースでサポートされる予定です。

（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 （217 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。

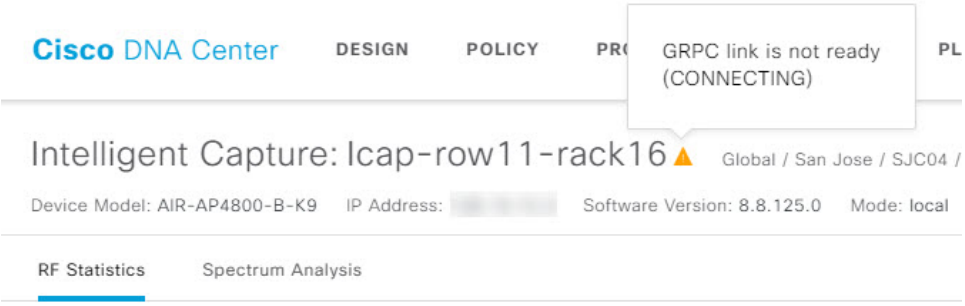
スペクトル解析のための無線スロットの割り当ては次のとおりです。

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**	無線スロット 0 および 1 が有効になっています。
Aironet 4800 シリーズ 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。

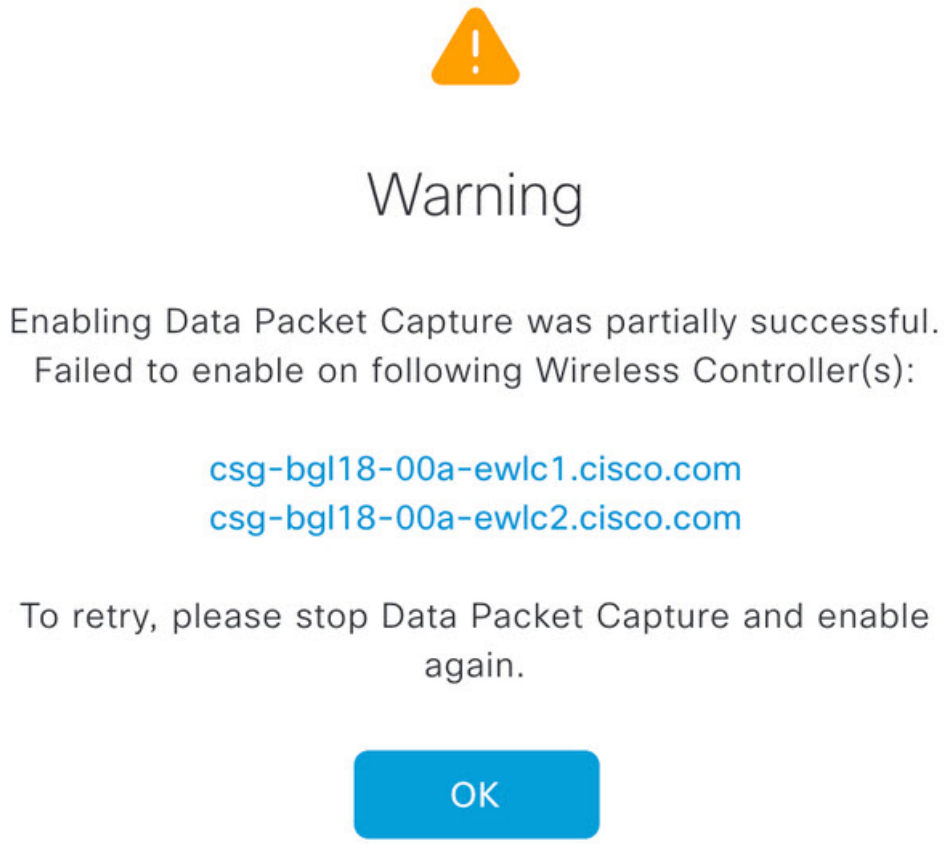
ただし、Cisco DNA Center のアップグレードパスによっては、ポート番号が適切に設定されない場合があります。

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。

データパケットキャプチャを開始すると設定エラーが発生する

問題：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しようとすると、データパケットキャプチャの有効化で問題が発生したことを示す警告メッセージが表示されます。次に示すように、警告メッセージには問題を報告したコントローラ名も含まれています。



（注） 警告メッセージで [OK] をクリックすると、メッセージが閉じ、[Intelligent Capture: Client Device] ウィンドウに警告（⚠）アイコンが表示されます。警告（⚠）アイコンをクリックすると、次に示すように、問題を報告したコントローラ名が表示されます。

Enabling Data Packet Capture was partially successful. Failed to enable on following Wireless Controller(s):

csg-bgl18-00a-ewlc1.cisco.com:
% switch-2:dbm:wireless:Cannot create more than 1 client MAC entries.

csg-bgl18-00a-ewlc2.cisco.com:
% switch-1:dbm:wireless:Cannot create more than 1 client MAC entries.

To retry, please stop Data Packet Capture and enable again.

考えられる原因：

次のいずれかの理由で、コントローラに外部 MAC アドレスが設定されている場合に、この問題が発生します。

- データパケットキャプチャの MAC アドレスが、Cisco DNA Center クラスタに接続されたコントローラ上で手動で設定された。

- データパケットキャプチャ用に事前に設定された MAC アドレスを持つコントローラが、別の Cisco DNA Center クラスタに移動された。
- 最初にデータパケットキャプチャを無効にせずに、Cisco DNA Center が再イメージ化された。

解決策：

この問題を解決するには、ワイヤレスコントローラまたは eWLC から外部 MAC アドレスを削除する必要があります。

ワイヤレス コントローラ

ワイヤレスコントローラから外部 MAC アドレスを削除するには、次の手順を実行します。

1. ワイヤレスコントローラにログインします。
2. 次のコマンドを入力して、クライアントの MAC アドレスが設定されているかどうかを確認します。

   show icap global detail full-packet-trace

3. コマンド出力でクライアントの MAC アドレスが設定されていると表示された場合は、次のコマンドを実行して、データパケットキャプチャを無効にします。

   config icap global subscription client packet-trace full disable

4. 次のコマンドを実行して、MAC アドレスを削除します。

   config icap global subscription client packet-trace full filter remove *Client_MAC_listed_in_the_output_of_step_2*

eWLC

eWLC から MAC アドレスを削除するには、次の手順を実行します。

1. eWLC にログインします。
2. 次のコマンドを入力して、クライアントの MAC アドレスが設定されているかどうかを確認します。

   show run | sec ap profile

3. コマンド出力で **cap subscription client packet-trace full enable** と表示された場合は、次のコマンドを実行してデータパケットキャプチャを無効にします。

   no icap subscription client packet-trace full enable

4. 次のコマンドを実行して、MAC アドレスを削除します。

   no icap subscription client packet-trace full filter *Client_MAC_listed_in_the_output_of_step_2*

第 13 章

セキュリティ脅威の管理

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 14 章

ダッシュボードの管理

ダッシュボードについて

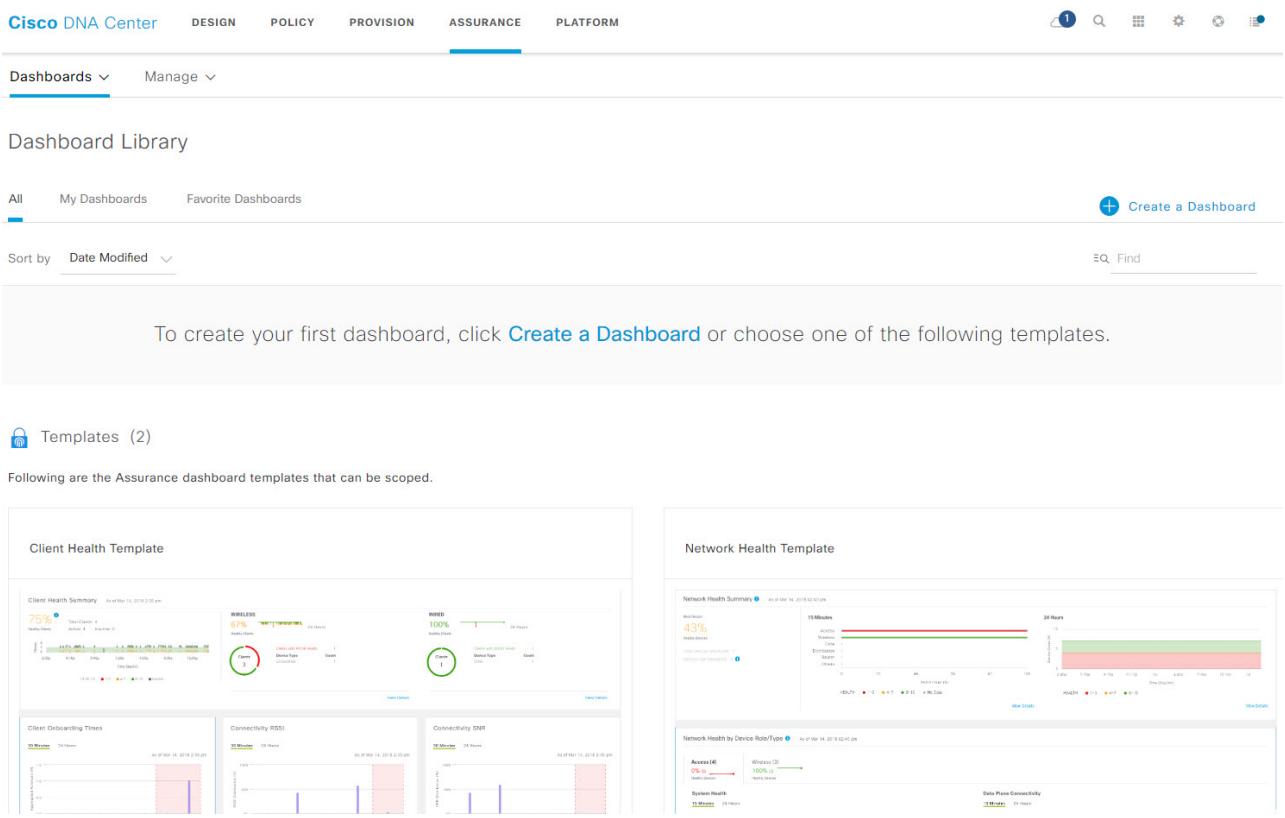
ネットワーク監視用のカスタムダッシュボードを作成できます。ダッシュボードには、1 つまたは複数のダッシュレット（チャート、表、地理マップなどの情報）で構成されます。

カスタム ダッシュボードの作成

ステップ 1 Cisco DNA Center のホームページで、**アシュアランス** > **[ダッシュボード（Dashboards）]** > **[ダッシュボード ライブラリ（Dashboard Library）]** の順に選択します。

[ダッシュボード ライブラリ（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。

図 *23* : ダッシュボード ライブラリ ウィンドウ



ステップ 2 右上隅にある Create a Dashboard をクリックします。

ステップ 3 **[ダッシュボードの作成（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 **[保存（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 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 **[保存（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。

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リングできます。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リングします。

ステップ 1 Cisco DNA Center のホームページで、[Dashboards] > [Dashboard Library]**アシュアランス** > > 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 **[ダッシュボードの作成（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 **[保存（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には、 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。
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 **[次へ (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 **[次へ (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。

確認のダイアログが表示されます。

（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 Cisco DNA Centerのホームページで、[Dashboards] > [Dashboard Library]**アシュアランス** > > の順に選択します。

[ダッシュボードライブラリ（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。[並べ替え（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、[検索（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 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 Cisco DNA Center のホームページで、[Dashboards] > [Dashboard Library]**アシュアランス** > > の順に選択します。

[ダッシュボードライブラリ（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。[並べ替え（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、[検索（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 [削除（Delete）] をクリックします。

ダッシュボードの複製

ステップ 1 Cisco DNA Center のホームページで、[Dashboards] > [Dashboard Library]**アシュアランス** > > の順に選択します。

[ダッシュボードライブラリ（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。[並べ替え（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、[検索（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 **[保存 (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 **[保存（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 Cisco DNA Center のホームページで、[Dashboards] > [Dashboard Library]**アシュアランス** > > の順に選択します。

[ダッシュボードライブラリ（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。[並べ替え（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、[検索（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 のホームページで、**アシュアランス** > **[Dashboards]** > **[Health]** > **[Overall Health]** の順に選択します。

  [Overall Health] ダッシュボードが表示されます。

- Cisco DNA Center のホームページで、**アシュアランス** > **[Dashboards** > **[Health]** > **[Network Health]** の順に選択します。

  [Network Health] ダッシュボードが表示されます。

- Cisco DNA Center のホームページで、**アシュアランス** > **[Dashboards]** > **[Health]** > **Client Health]** の順に選択します。

  [Client Health] ダッシュボードが表示されます。

- Cisco DNA Center のホームページで **アシュアランス** > **[Dashboards]** > **[Health]** > **[Application Health]** の順に選択します。

  [Application Health] ダッシュボードが表示されます。

ステップ 2 Actions （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 **[保存 (Save)]** をクリックします。

第 15 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、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。

機械推論エンジンとレイヤ 2 のループ問題について

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。

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。

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 リリース 1.3.1.0 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 ベースの AI 駆動型の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、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。

（注） Cisco DNA Center リリース 1.3.0 では、過剰なオンボーディング時間に対応するため、制限付きのオンアプライアンス Cisco AI Network Analytics 機能が導入されました。したがって、Cisco DNA Center リリース 1.3.1.0 に Cisco AI Network Analytics アプリケーションをインストールしていない場合でも、Cisco DNA Center リリース 1.3.0 以降に発生した AI 駆動型のオンプレミスの問題の一部を確認できます。

- **レイヤ 2 ループの問題**：機械推論エンジン（MRE）によって実行される根本原因の分析。機械推論エンジンとレイヤ 2 のループ問題について （260 ページ）を参照してください。

始める前に

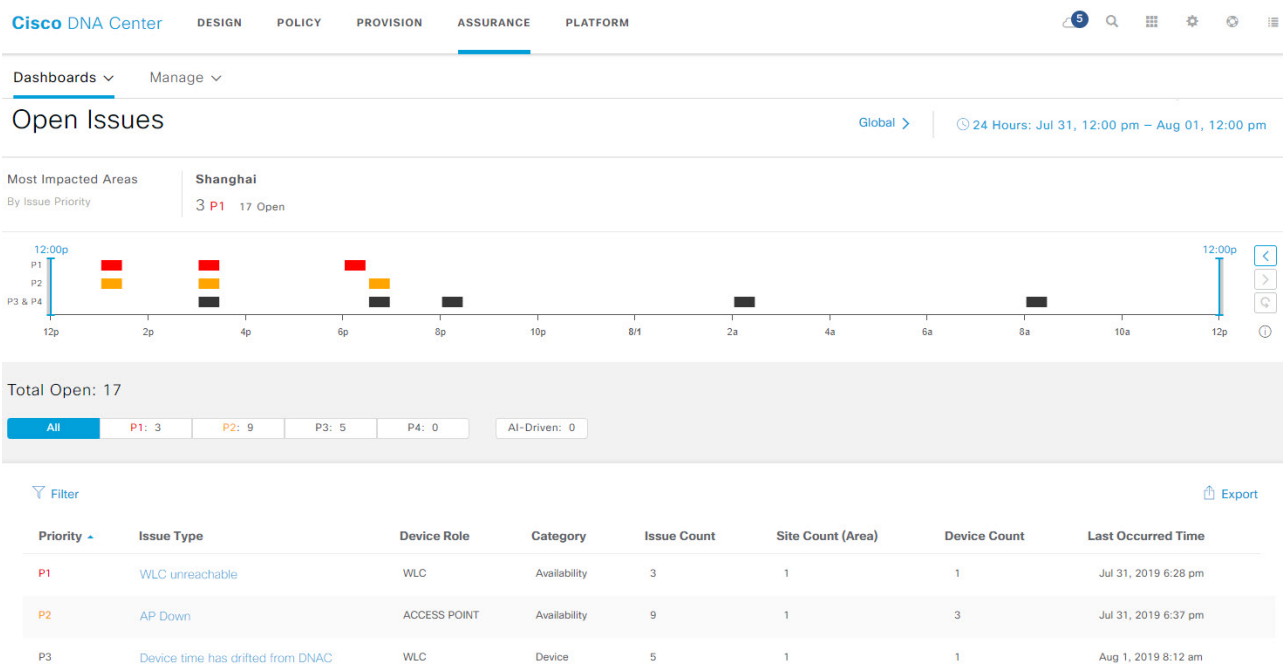
- 人工知能（AI）および機械学習（ML）テクノロジーを使用してインテリジェントな問題の検出と分析を行う AI 駆動型クラウドベースの問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認します。Cisco AI Network Analytics データ収集の設定 （89 ページ） を参照してください。
- syslog メッセージを表示するには、デバイスで**最適な可視性**と**最大可視性**のテレメトリプロファイルが設定されていることを確認してください。 Cisco Digital Network Architecture Center ユーザ ガイド の「テレメトリプロファイルの設定」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 [Summary] > [Critical Issues]**アシュアランス** エリアで、[View Details] を選択します。
- Cisco DNA Center のホームページで、**アシュアランス** > **[Dashboard]** > **[Issues]** > **[Open]** の順に選択します。

[All Issues] ウィンドウに次の情報が表示されます。

図 *24 : [Open Issues]* ウィンドウ



[Open Issues] ウィンドウ	
項目	**説明**
Global	選択したロケーション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 [Global] です。ロケーションを変更するには、次の手順を実行します。 **1.** [Global] をクリックします。サイト/ビル/フロア テーブルが表示されます。 **2.** 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。 **3.** 特定のサイト、建物またはフロアに関する情報を表示するには、適切な行で [Apply] をクリックすると、選択した内容に基づいて [Open Issues] ウィンドウ内の情報が更新されます。

[Open Issues] ウィンドウ	
項目	説明
[24時間（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時間（24 Hours）] です。次の手順を実行します。 **1.** [24 時間（24 Hours）] ドロップダウン リストで、時間範囲（[3 時間（3 hours）]、[24 時間（24 Hours）]、または [7 日間（7 days）]）を選択します。 **2.** **[開始日付（Start Date）]**と時刻、**[終了日付（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、問題が発生したビル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。
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]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。デフォルトは [All] です。

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	
項目	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。

[Open Issue] ウィンドウの [Issue Type] 表	
項目	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。アクセス、コア、分散、境界ルータ、または不明のいずれかを指定できます。
Category	問題のタイプが属するカテゴリ。たとえば、接続、可用性、オンボーディング、使用率などがあります。
問題数	このタイプ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] が開き、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）	
項目	説明
未解決の問題	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 （275 ページ） を参照してください。
問題	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] が開き、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 （265 ページ） を参照してください。

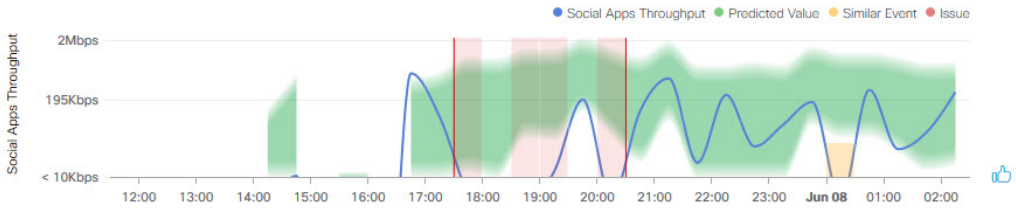
機械推論をサポートするレイヤ 2 ループの問題については、[Issue Instance Details] スライドインペインに特定の情報が表示されます。「レイヤ 2 のループ問題に関与するインスタンスの詳細 （268 ページ）」を参照してください。

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 （260 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）	
項目	**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、[ステータス（Status）] ドロップダウン メニューで [解決する（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。

[Issue Instance Details]（2 番目のスライドインペイン）	
項目	説明
[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。
[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 *25 :* 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。 [Connected Clients]、[Impacted APs]、[Device Breakout]、 [Applications by TX/RX] などのタブがあります。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）	
項目	説明
根本原因の分析	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 *26* : 根本原因の分析チャート  [Network Causes]、[Failed Distribution]、[Failed Percentage]、[Failed Count] などのタブがあります。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。
推奨されるアクション（Suggested Actions）	この問題を解決するために実行できるアクションについて説明します。

レイヤ 2 のループ問題に関与するインスタンスの詳細

（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 （260 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、「機械推論エンジンとレイヤ 2 のループ問題について （260 ページ）」を参照してください。

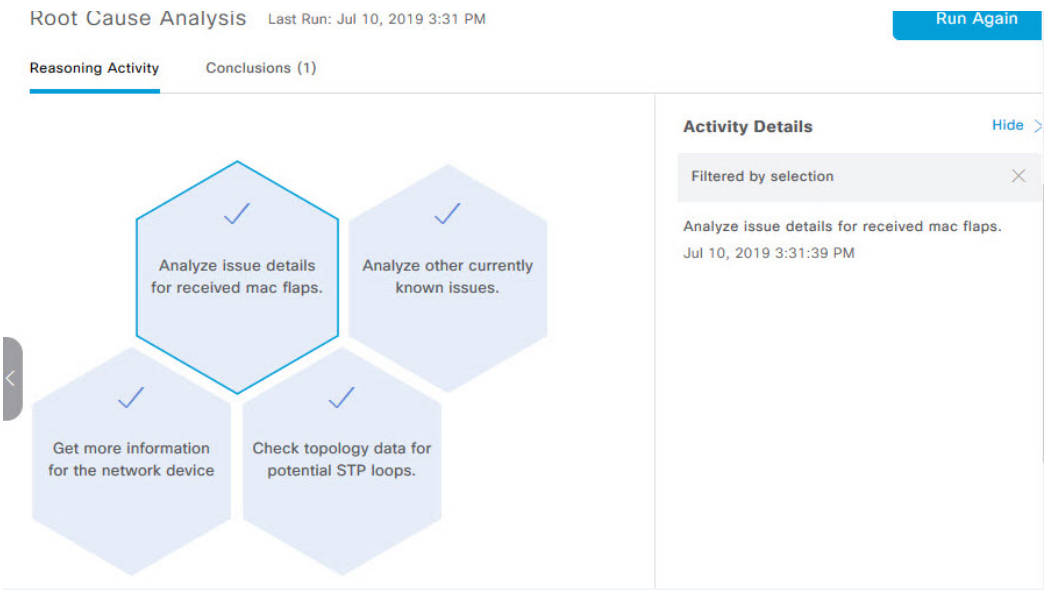
（注） レイヤ 2 ループのスケールに関する制約事項は、次のとおりです。

- VLAN 数は 10 です。
- VLAN ごとのデバイス数は 30 です。

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）	
項目	**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、[ステータス（Status）] ドロップダウン メニューで [解決する（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。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]	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）	
項目	説明
[Root Cause Analysis]	

[Issue Instance Details]（2 番目のスライドインペイン）	
項目	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、[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 *27*：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）	
項目	説明
	6. MRE を再実行する場合は、[Run Again] をクリックします。
[トポロジ] アイコン	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。

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 （89 ページ）を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**アシュアランス** > **[Dashboard]** > **[Issues]** > **[Resolved]** を選択します。

[Resolved Issues] ウィンドウが表示されます。

ステップ 2 [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	
項目	説明
Global	選択したロケーション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 [Global] です。ロケーションを変更するには、次の手順を実行します。 **1.** [Global] をクリックします。サイト/ビル/フロア テーブルが表示されます。 **2.** 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。 **3.** 特定のサイト、建物またはフロアに関する情報を表示するには、適切な行で [Apply] をクリックすると、選択した内容に基づいて [Open Issues] ウィンドウ内の情報が更新されます。

[Resolved Issues] ウィンドウ	
項目	説明
[24時間（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時間（24 Hours）] です。次の手順を実行します。 **1.** [24 時間（24 Hours）] ドロップダウンリストで、時間範囲（[3 時間（3 hours）]、[24 時間（24 Hours）]、または [7 日間（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]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。デフォルトは [All] です。

ステップ 3 [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	
項目	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。アクセス、コア、分散、境界ルータ、または不明のいずれかを指定できます。
Category	問題のタイプが属するカテゴリ。たとえば、接続、可用性、オンボーディング、使用率などがあります。
問題数	このタイプ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 4 [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 （277 ページ） を参照してください。

ステップ 5 [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] が開き、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。表示される無視された問題のリストは、次の 2 つ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 （89 ページ） を参照してください。

ステップ 1 Cisco DNA Centerホーム ページで、**アシュアランス** > **[Dashboard]** > **[Issues]** > **[Ignored]** を選択します。

[Ignored Issues] ウィンドウが表示されます。

ステップ 2 [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	
項目	説明
Global	選択したロケーション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 [Global] です。ロケーションを変更するには、次の手順を実行します。 **1.** [Global] をクリックします。サイト/ビル/フロア テーブルが表示されます。 **2.** 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。 **3.** 特定のサイト、建物またはフロアに関する情報を表示するには、適切な行で [Apply] をクリックすると、選択した内容に基づいて [Ignored Issues] ウィンドウ内の情報が更新されます。
[24時間（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時間（24 Hours）] です。次の手順を実行します。 **1.** [24 時間（24 Hours）] ドロップダウン リストで、時間範囲（[3 時間（3 hours）]、[24 時間（24 Hours）]、または [7 日間（7 days）]）を選択します。 **2.** **[開始日付（Start Date）]**と時刻、**[終了日付（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]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。デフォルトは [All] です。

ステップ 3 [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	
項目	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。アクセス、コア、分散、境界ルータ、または不明のいずれかを指定できます。

[Ignored Issues] ウィンドウの [Issue Type] 表	
項目	説明
Category	問題のタイプが属するカテゴリ。たとえば、接続、可用性、オンボーディング、使用率などがあります。
問題数	このタイプ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 4 [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 5 [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] が開き、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 Cisco DNA Center のホームページで、**アシュアランス** > **[Dashboard]** > **[Issues]** > **[Open]** の順に選択します。

[Open Issues] ウィンドウが表示されます。

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 issue] ウィンドウの [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、[ステータス（Status）] ドロップダウン メニューで [解決する（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。

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。
- AP が停止した。

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 （271 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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Issue Settings]** を選択します。

[Issue Settings] ウィンドウが表示されます。

ステップ 3 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 4 [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、ⓘ の上にカーソルを置くと、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。

トリガー条件の例：

```
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 5 Manage Subscription 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の外部通知を登録できます。「問題の通知の有効化 （278 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 Cisco DNA Centerのホームページで、**アシュアランス** タブをクリックします。

[Overall Health] ダッシュボードが表示されます。

ステップ 2 **[Manage]** > **[Issue Settings]** を選択します。

[Issue Settings] ウィンドウが表示されます。

ステップ 3 [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 4 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 5 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 6 [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（Details）
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。
電子メール	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, Release 1.3.1.0 [英語]*』の「*Working with Events*」を参照してください。

アシュアランス および Cisco AI Network Analytics 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	要約
接続性	BGP トンネル接続	AS（自律システム）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 ISIS（Intermediate System Intermediate System）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 OSPF（Open Shortest Path First）隣接関係に障害が発生しました。
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	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。
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。

ルータの問題		
カテゴリ	問題の名称	要約
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	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	要約
接続性	BGP トンネル接続	AS（自律システム）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。

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	要約
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 ISIS（Intermediate System Intermediate System）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 OSPF（Open Shortest Path First）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。
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。

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	要約
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	ファブリックエッジが物理ネットワーク内の ISE サーバ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。
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	デバイスと DNAC 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	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	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。

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	要約
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。
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	要約
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	デバイスと DNAC 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。
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	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。

コントローラの問題		
カテゴリ	問題の名称	要約
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	要約
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	AP の停止	AP が停止しました。
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。
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 で 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 で 5 GHz 無線の使用率が高くなっています。
AP 異常	AP 異常	AP で異常が発生しました。

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	要約
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	クライアントの DNS 到達可能性の問題	クライアントが DNS サーバから応答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 を使用するユーザデバイス認証のエラーです。 （注） この問題は、単独の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	要約
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	クライアントの DNS 到達可能性の問題	クライアントが DNS サーバから応答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。

ワイヤレスクライアントの問題		
カテゴリ	問題の名称	要約
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。
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 サーバでタイムアウトが発生しました。

ワイヤレスクライアントの問題		
カテゴリ	問題の名称	要約
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。
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。

ワイヤレスクライアントの問題		
カテゴリ	問題の名称	要約
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。
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。

ワイヤレスクライアントの問題		
カテゴリ	問題の名称	要約
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。
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	要約
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。

センサーの問題		
カテゴリ	問題の名称	要約
センサーテスト	センサー - オンボーディング時の認証の遅延	802.1x 認証フェーズでの遅延により、センサーのオンボーディングが低速です。
センサーテスト	センサー - RADIUS 到達可能性の遅延	複数のセンサーが RADIUS サーバからの ping 応答の遅延を報告しています。
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 - デフォルトゲートウェイ障害の発生	複数のセンサーがローカルゲートウェイ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 - 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 - DNS サーバの到達可能性エラー	複数のセンサーが到達不能な DNS サーバを報告しています。ping が失敗しています。
センサーテスト	センサー - DNS サーバ応答の遅延	複数のセンサーで ping を介した DNS サーバ ホストからの応答が遅れています。
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 - ファーストホップの応答遅延	複数のセンサーがローカルゲートウェイからの ping 応答の遅延を報告しています。
センサーテスト	センサー - FTP 到達可能性の遅延	複数のセンサーが FTP サーバホストからの応答の遅延を報告しています。
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 サーバに接続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 - FTP 転送の失敗	複数のセンサーが FTP サーバ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 転送の遅延	複数のセンサーが FTP サーバとの FTP 転送時間の遅延を報告しています。
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 - IPSLA IP アドレスなし	複数のセンサーが DNAC 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。

センサーの問題		
カテゴリ	問題の名称	要約
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 - メールサーバ到達可能性の遅延	複数のセンサーがメールサーバからの ping 応答の遅延を報告しています。
センサーテスト	センサー - メールサーバ応答の遅延	複数のセンサーがメールサーバへの接続時間の遅延を報告しています。
センサーテスト	センサー - メールサーバのテスト失敗	複数のセンサーがメールサーバ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 - メールサーバに到達不能	複数のセンサーがメールサーバ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 サーバなし	複数のセンサーが速度テスト NDT サーバ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 サーバのファーストホップ遅延	複数のセンサーが Outlook Web アクセスのファースト ホップゲートウェイからの応答遅延を報告しています。
センサーテスト	センサー - Outlook サーバ応答の遅延	複数のセンサーが、Outlook Web アクセスへのメール接続時間の遅延を報告しています。
センサーテスト	センサー - Outlook サーバの遅延	複数のセンサーが Outlook Web アクセスホストからの ping 応答の遅延を報告しています。
センサーテスト	センサー - Outlook サーバのテスト失敗	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。
センサーテスト	センサー - Outlook サーバに到達不能	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のタイムアウトを報告しています。

センサーの問題		
カテゴリ	問題の名称	要約
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 - RADIUS 認証の遅延	複数のセンサーが RADIUS サーバからの認証時間の遅延を報告しています。
センサーテスト	センサー - オンボーディング時の関連付けの遅延	関連付けフェーズでの遅延により、センサーのオンボーディングが低速です。
センサーテスト	センサー - DNS 名前解決の遅延	複数のセンサーで DNS サーバからの名前解決が遅れています。
センサーテスト	センサー - オンボーディング時の IPv4 アドレッシングの遅延	複数のセンサーで IPv4 アドレスの取得が遅延しています。
センサーテスト	センサー - ホストからの応答遅延	複数のセンサーがホストからの ping 応答の遅延を報告しています。
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 認証設定の失敗	複数のセンサーが無効な Web 認証設定を報告しています。
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 認証 HTTP の失敗	複数のセンサーが Web 認証の HTTP エラーを報告しています。
センサーテスト	センサー - Web 認証の遅延	複数のセンサーが Web 認証の遅延を報告しています。
センサーテスト	センサー - Web サーバのファーストホップ遅延	複数のセンサーが Web サーバのファースト ホップ ゲートウェイからの応答遅延を報告しています。

センサーの問題		
カテゴリ	問題の名称	要約
センサーテスト	センサー - Web サーバ到達可能性の遅延	複数のセンサーが Web サーバからの ping 応答の遅延を報告しています。
センサーテスト	センサー - Web サーバ応答の遅延	複数のセンサーが Web サーバからの Web 応答時間の遅延を報告しています。
センサーテスト	センサー - Web サーバのテスト失敗	複数のセンサーが Web サーバ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 サーバに到達不能	複数のセンサーが Web サーバ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	要約
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。

AI 駆動型の問題		
カテゴリ	問題の名称	要約
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。
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。

第 16 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。

（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。

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 次のいずれかを実行します。

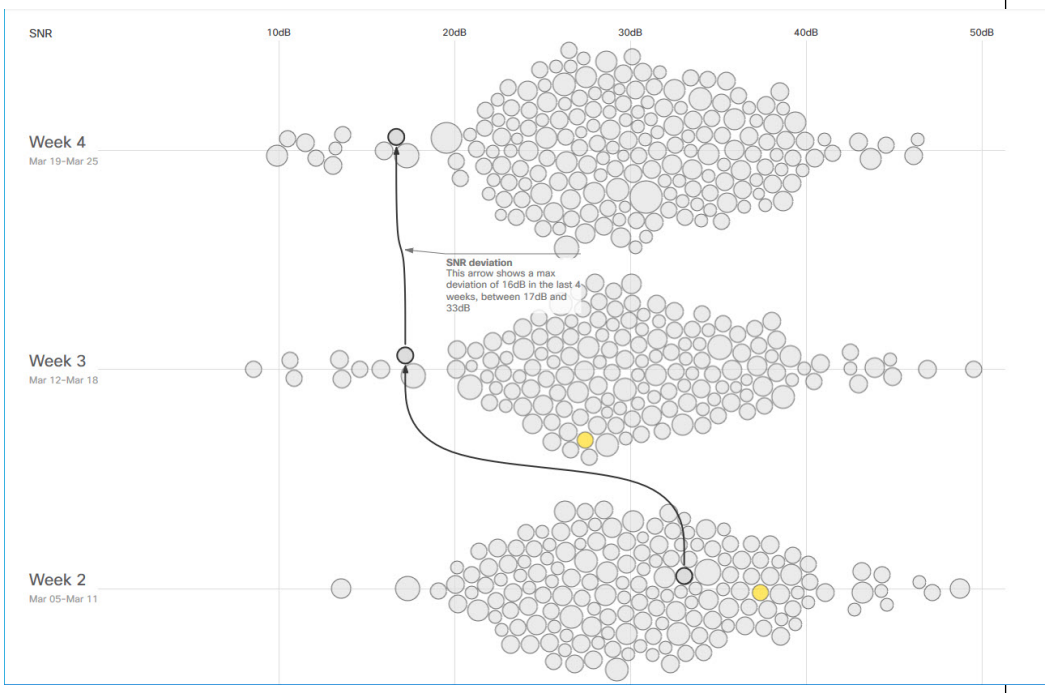
- Cisco DNA Center ホーム ページの [Summary] > [Trends and Insights]**アシュアランス** エリアで、[View Details] を選択します。
- Cisco DNA Center ホームページから、 **アシュアランス** > **[Trends and Insights]** > **[Network Insights]** を選択します。

[Network Insights] ウィンドウに、[Capacity]、[Coverage]、[Throughput] の 3 つのタブが表示されます。デフォルトでは、[Capacity] タブが選択されており、次の情報が表示されています。

インサイトテーブル	
項目	説明
Occurrence	このトレンドが観測された期間。たとえば、2019 年 5 月 27 日 ～ 6 月 3 日など。
Insight	特定の期間に観測されたすべての AI 駆動型のすべて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。[Capacity]、[Coverage]、[Throughput] のいずれかを選択できます。
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。[2.4 GHz]、 [5 GHz]、またはその両方の周波数帯を使用できます。
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	
項目	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。
Insight Summary	下の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。
トラブルシューティング	[Network Heatmap] ページと [AP 360] ページにリンクしています。これらのページでは、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できます。
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	
項目	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 *28*：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などの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

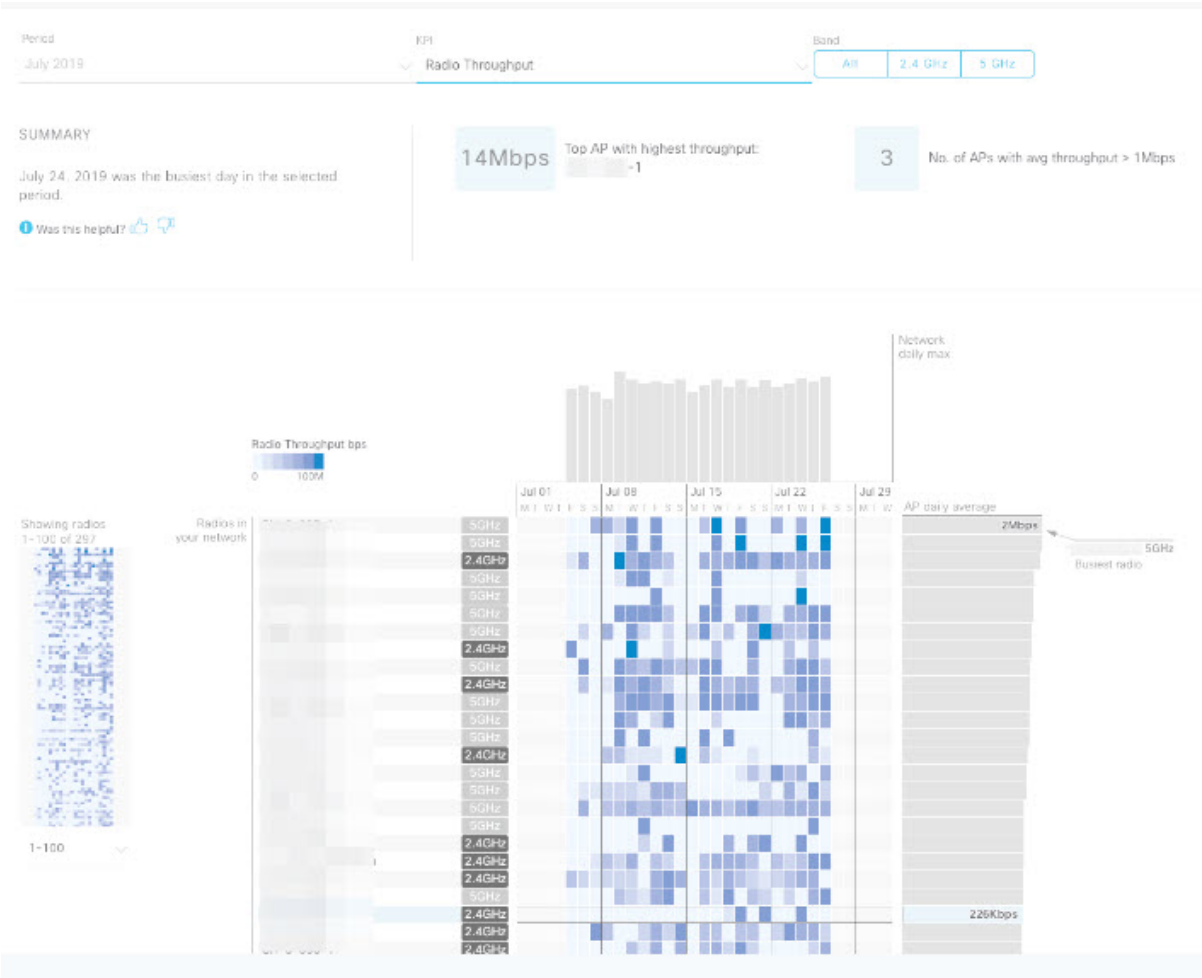
ヒートマップ内の特定の月にネットワーク内のすべての AP を視覚的に比較して、トレンドを把握し、インサイトを取得するには、次の手順を実行します。異なる KPI と帯域周波数で AP を比較することを選択できます。取得したインサイトにより、最も輻輳が多い KPI、最も輻輳のある AP、および それらの AP のうち使用中の AP に関する情報が得られます。この情報により、トレンドが観察されたサイトまたはビルにさらにドリルダウンすることができます。AP または AP のグループを特定したら、それらの AP の動作履歴（1 日、1 週間、および月全体）を判断できます。

ステップ 1 Cisco DNA Center のホームページで [Trends and Insights]**アシュアランス** > を選択します。

ステップ 2 [Trends and Insights] ドロップダウン リストから、[Network Heatmap] を選択します。

[Network Heatmap] ウィンドウに次の情報が表示されます。

図 *29 : [Network Heatmap]* ウィンドウ



[Network Heatmap] ウィンドウ	
項目	**説明**
期間	ヒートマップが表示されている月が表示されます。
[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。
[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。
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。
[Network Daily Max] グラフ	特定の日におけるすべての AP について、ネットワークの日次平均割合を示すグラフが表示されます。日次平均スコアが最も高い（最もビジーな）AP が強調表示されます。
[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]：[Band] のオプションから選択した帯域周波数に応じて、この領域には、クライアントによって使用された帯域周波数がリストされます。 • [AP Heatmap]：AP の動作履歴（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。 • [AP Daily Average]：その AP の平均 KPI スコア。

ステップ 3 各日の KPI 値を表示するには、[Network Daily Max] グラフのバーにカーソルを合わせます。

ステップ 4 [Heatmap] 内のカラーブロックにカーソルを合わせると、AP の名前と MAC アドレス、帯域周波数、AP グループ、AP の場所、日次平均 KPI スコアなどの情報が表示されます。

ステップ 5 [AP Daily Average] 領域にカーソルを合わせると、その期間中の AP の平均 KPI 値を確認できます。

ステップ 6 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

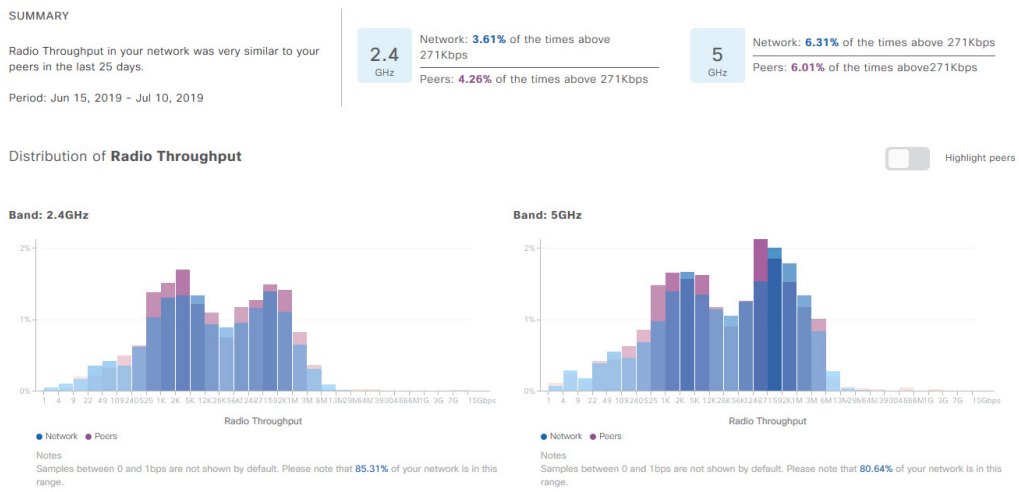
選択した重要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。

ステップ 1 Cisco DNA Center のホームページで [Trends and Insights]**アシュアランス** > を選択します。

ステップ 2 [Trends and Insights] ドロップダウンリストから、[Peer Comparison] を選択します。

[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	
項目	**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 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。次の情報を提供します。 • [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。
[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。

[Peer Comparison] ウィンドウ	
項目	説明
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 *30 :* 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 3 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。

ネットワーク内のサイト間の比較

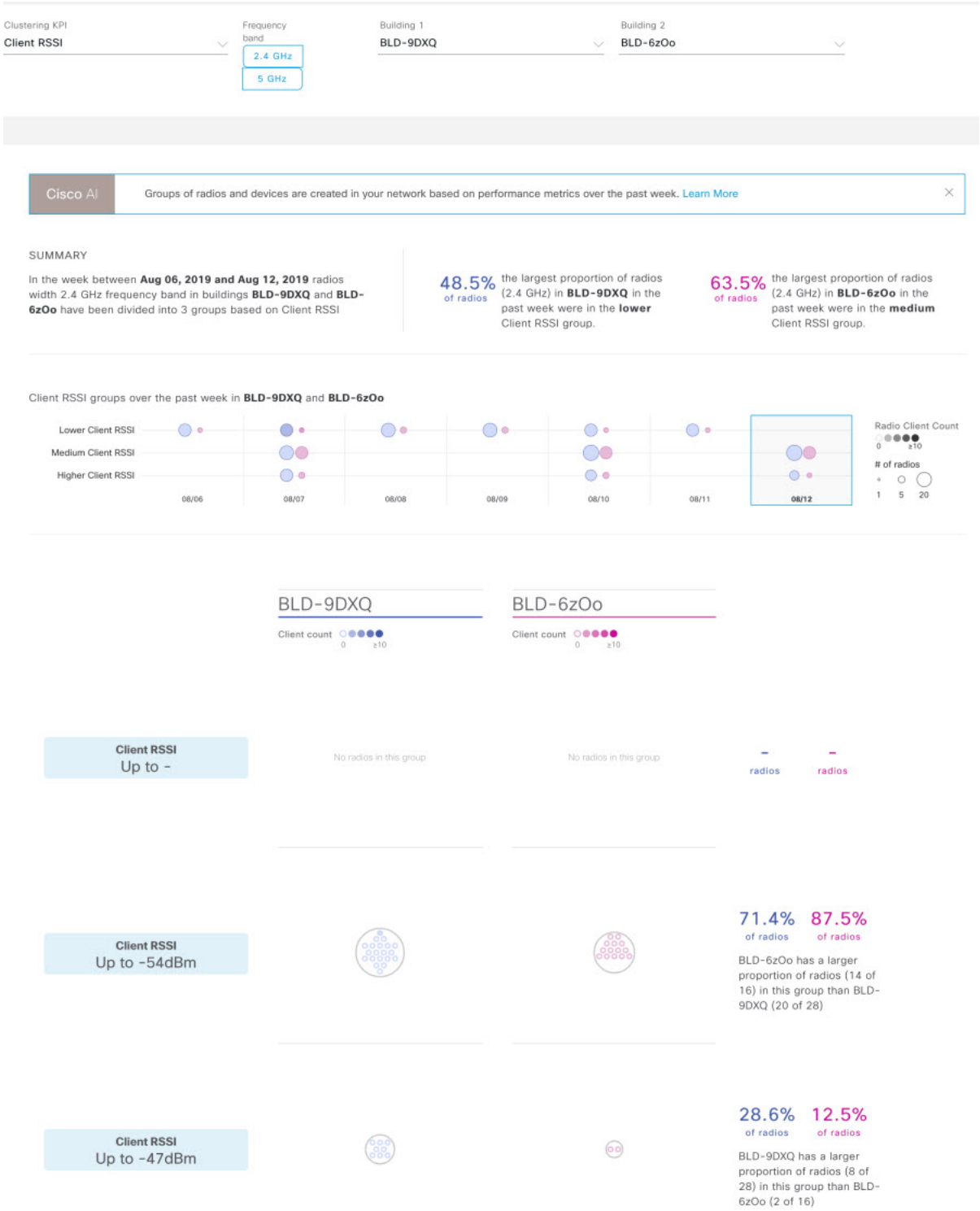
選択した重要業績評価指標（KPI）について、ネットワーク内のサイト（ビル）間でパフォーマンスを比較するには、次の手順を実行します。2 つのサイト間のパフォーマンスの比較に使用できる KPI として、無線スループット、クライアント RSSI、および平均オンボーディング時間があります。この手順では、パフォーマンスが、高、中、低のサイト内の AP の数を判断できます。

ステップ 1 Cisco DNA Center のホームページで [Trends and Insights]**アシュアランス** > を選択します。

ステップ 2 [Trends and Insights] ドロップダウンリストから、[Site Comparison] を選択します。

[Site Comparison] ウィンドウが開き、次の情報が表示されます。

図 *31 : [Site Comparison]* ウィンドウ



[Site Comparison] ウィンドウ	
項目	**説明**
[Clustering 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]、[Client RSSI]、[Average Onboarding Time] のいずれかを選択できます。デフォルトは [Radio Throughput] です。
周波数帯域	帯域周波数を選択できます。[Band 2.4 GHz] または [Band 5 GHz] を選択できます。
[Building 1] ドロップダウンリスト	KPI 値を比較する最初のサイトを選択します。
[Building 2] ドロップダウンリスト	最初のサイトの KPI 値と比較する 2 番目のサイトを選択します。
タイムライン	各曜日の AP クラスタのパフォーマンスが表示されます。
[クライアント カウント（Client Count）] または Device Count	[Radio Throughput] と [Client RSSI] KPI の場合、このエリアには各サイトの無線ごとのクライアント数が表示されます。 [Average Onboarding Time] KPI の場合、このエリアには各サイトのデバイスの数が表示されます。

AP クラスタ
または
デバイスタイプクラスタ
	• [Radio Throughput] と [Client RSSI] KPI の場合、このエリアには各サイトに 1 つずつ、2 つの AP クラスタが表示されます。このエリアでは、2 つのサイ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。
	  • 各サイトでの AP のクラスタ化の程度。
	  • 低、中、高の KPI 値を示している AP の数。
	  • KPI のパフォーマンス（パーセンテージ）（AP クラスタ上で提供）
	• [Average Onboarding Time] KPI の場合、このエリアには以下が表示されます。
	  • 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。

ステップ 3 [Radio Throughput] と [Client RSSI] KPI の場合は、AP クラスタ領域内の AP にカーソルを合わせると、その AP の名前とクライアント数が表示されます。

第 17 章

定期レポート

Cisco DNA Center プラットフォーム を使用して、レポートのサンプル化およびスケジュール設定を行います。詳細については、Cisco DNA Center プラットフォームユーザガイドを参照してください。

データとレポートの操作

データおよびレポート機能は、次の使用例をサポートしています。

- キャパシティプランニング：ネットワーク内のデバイスがどのように利用されているのかを理解できます。
- パターンの変更：ネットワークでの使用パターンの傾向の変化を追跡します。使用パターンの傾向には、クライアント、デバイス、バンド、またはアプリケーションが含まれる場合があります。
- 運用レポート：アップグレード完了やプロビジョニング障害などのネットワーク運用に関するレポートを確認できます。
- ネットワークの正常性：レポートによってネットワークの全体的な正常性を判断できます。

（注） データおよびレポート機能の新しい使用例は、将来のリリースで追加される予定です。これらの情報については、今後の Cisco DNA Center プラットフォーム のリリースノートで確認してください。

レポートのサンプルとスケジュール

ネットワークに関する専門的なデータレポートを設定するには、この手順を実行します。Cisco DNA Center GUI の [Data and Reports] ウィンドウを使用では、データレポートを設定できます。

始める前に

- Cisco DNA Center で **ディスカバリ**ジョブを正常に実行し、デバイスとネットワークデータに関するレポートを設定およびスケジュールします。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。[Home] ページで、[Provision] > [Device Inventory] > [Inventory] の順に選択して、検出結果を表示します。

ステップ 1 [Catalog] ウィンドウを確認します。

[Catalog] ウィンドウに、カタログ品目と呼ばれるサポート対象のレポートカテゴリが表示されます。各カタログ品目はタイルで表示され、サンプルレポートとレポートの設定（スケジュール）の両方へのリンクが含まれています。

ステップ 2 [Catalog] ウィンドウで、レポートを作成するカタログ品目を指定します。

ステップ 3 サンプルレポートを表示するには、カタログ品目のタイルで [Sample] をクリックします。

そのサンプルレポートの [Preview] ウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注） [Preview] ウィンドウのサンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、カタログ品目のタイルで [Schedule] をクリックします。

[Schedule] ウィンドウが開きます。ここで、レポートのフォーマットタイプを選択、データのフィルタを適用、および実際のレポート生成スケジュールを設定できます。

ステップ 6 [Schedule] ウィンドウでは、レポートを作成するためのパラメータを設定します。

[Schedule] ウィンドウは次のフィールドに分かれています。

- [Format]：デフォルトのレポート名を承認するか、新しいレポート名を作成します。また、データタイプやファイルタイプを選択します（複数のオプションがある場合）。

- [Filters]：レポートのデータのフィルタを選択します。
- [Schedule]：レポート生成の日時を選択します。
- [Send to]：レポートのダウンロードリンクが記載された電子メールの送信先となる電子メールアドレスを入力します。

ステップ 7 [Report Name] フィールドで、デフォルトのレポート名を受け入れるか、新しいレポート名を入力します。

ステップ 8 [Type] フィールドで、データタイプをクリックします。

SWIM およびインベントリレポートの場合は、データタイプの選択肢はありません。デフォルトのデータタイプは、[All Data] です。エグゼクティブサマリーの場合、データの選択肢はありません。[Executive Summary] がデフォルトになります。

（注） エグゼクティブサマリーレポートの日付と時刻の値は、協定世界時（UTC）標準に基づきます。

クライアントレポートの場合は、次のいずれかを選択できます。

- **Client Summary**
- **Top N Summary**
- **クライアントの詳細**

ステップ 9 [File Type] フィールドでは、完成レポートのファイルタイプを選択します。

[File Type] では、作成するレポートに応じて次のオプションを選択できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [CSV]、[JSON]、[Tableau Data Extract] の場合、[Fields] オプションが表示され、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

ステップ 10 （任意）レポートの属性（フィールド）を選択します。

（注） SWIM データとレポートの場合は、 [CSV] と [Tableau Data Extract] の両方のファイルタイプについて、個々のフィールドを選択できます。クライアントデータとレポートの場合は、[Client Detail] を選択してから、 [CSV]、[Tableau Data Extract]、[JSON] の各ファイル タイプについて、個々のフィールドを選択できます。インベントリデータとレポートの場合は、[CSV] と [Tableau Data Extract] の両方のファイルタイプについて、個々のフィールドを選択できます。

ステップ 11 必要に応じて、レポートの [Data Filters] を選択します。

[Data Filter] は、設定するレポートのタイプによって異なります。たとえば、SWIM データフィルタは、[Location]、[Device Family]、および [Device Role] で構成されます。対照的に、エグゼクティブサマリーのデータフィルタは、特定の時間範囲です（追加の [Custom] 時間範囲オプションがあります）。

ステップ 12 [Schedule] フィールドで、レポートのスケジュールを設定します。

[Schedule] には、次のオプションがあります。

- **Schedule Now**
- **Schedule for Later**
- **Reoccurring Schedule**

ステップ 13 レポートの電子メール通知を送信するには、[Send to] フィールドに電子メールアドレスを入力します。

Cisco DNA Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Data and Reports] の [My Downloads] ページへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

（注） 電子メールからレポートを表示してダウンロードするには、適切な Cisco DNA Center ユーザ権限が必要です。

ステップ 14 [Schedule] ボタンをクリックします。

[My Downloads] ウィンドウが開き、スケジュールされたレポートのインスタンスの詳細が表示されます。

次のタスク

[My Downloads] ウィンドウで、レポートインスタンスを確認します。

（注） [My Downloads] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除することができます。

マイダウンロードの確認

以前生成したレポートをダウンロード、確認、編集、複製、または削除するには、この手順を実行します。

始める前に

- Cisco DNA Center で **ディスカバリ**ジョブを正常に実行し、デバイスとネットワークデータに関するレポートを設定およびスケジュールします。[Device Inventory] で**ディスカバリ**

ジョブが成功しているかどうか確認できます。[Home] ページで、 [Provision] > [Device Inventory] > [Inventory] の順にクリックして、検出結果を表示します。

- [Catalog] の [Schedule] 機能を使って、レポートを作成します。

ステップ 1 [My Downloads] タブをクリックします。

次の情報が表示されます。

- [Name]：レポートの名前。

  レポート名を指定しなかった場合は、レポートの日付と時刻とともにレポートタイプを含むデフォルト名がレポートに設定されます。

- [Report Type]：カタログオプション（クライアント、SWIM、インベントリ）に基づくレポートのタイプ。
- [File Type]：ファイル形式タイプ（PDF または CSV ファイル形式など）。
- [Schedule]：レポートを生成したスケジュールの説明。
- [Last Execution Status]：レポートの実行ステータスと詳細が表示されます。次のレポート実行ステータスタイプが表示される場合があります。
  - [Not Initiated]：スケジュールされたが、まだ開始されていないレポート。
  - [In Queue]：スケジュールされ、実行する処理キュー内にあるレポート。
  - [In Progress]：現在実行中のレポート。
  - [Completed]：レポートの実行が完了しました。

    [Completed] の横にあるアイコン（下矢印）をクリックすると、最後に生成されたレポートがダウンロードされます。

  - [Expired]：期限切れになり、Cisco DNA Center で使用できなくなっているレポート。
  - [Error]：レポートの実行に失敗しました。

- [Reports]：合計で最大 7 個のレポート数。

  表示されたレポート数にマウスのカーソルを合わせると、[View Report List] が表示されます。レポートダイアログボックスを表示するには、[View Report List] をクリックします。レポートダイアログボックスには、すべてのレポート実行とそのステータス（[Not Initiated]、[In Queue]、[In Progress]、[Completed]、[Expired]、[Error]）、およびコピーをダウンロードするための [Download] ボタンが表示されます。[Error] をクリックすると、レポートの実行に関するエラーと警告が表示されます。

重要 Cisco DNA Center プラットフォーム 合計 7 個のレポートを保持します。具体的には、Cisco DNA Center プラットフォームは実行された最後の 7 個のレポートと、過去 7 日間（週）に実行された最後の 7 個のレポートを保持します。たとえば、1 日に 8 個のレポートを実行した場合、Cisco DNA Center プラットフォーム は最後の 7 個のレポートのみを保持します。毎日 1 つのレポートをスケジュールすると、Cisco DNA Center プラットフォーム は過去 7 日間（週）にわたる最新の 7 個のレポートのみを保持します。また、Cisco DNA Center プラットフォーム からさまざまな形式でレポートをエクスポートし、それらを安全な場所にアーカイブすることもできます。

- [Actions]：レポートで実行できるタスクのリスト。

[Filter] アイコンをクリックしてフィルタを使用するか、[Find] フィールドにキーワードを入力することで、GUI に表示されるダウンロードを調整することができます。

ステップ 2 次の 1 つ以上のタスクを実行するには、[Actions] をクリックします。

- [Edit]：レポートに設定されたパラメータ（スケジュールを含む）が表示されるウィンドウを開きます。このウィンドウでは、設定されているレポートパラメータを確認できます。ただし、このウィンドウでは、レポート設定を変更できません。これは、読み取り専用ビューです。設定を編集する必要がある場合は、[Actions] > [Edit] をクリックします。[Edit] をクリックすると、レポート設定を表示および編集できます。

- [Edit]：レポートに設定されたパラメータ（スケジュールを含む）が表示されるウィンドウを開きます。このウィンドウでは、パラメータの確認および編集もできます。レポートを編集した後、[Update Schedule] をクリックします。

  重要 レポート設定を編集して更新すると、以降のレポート実行にはこの新しい設定が反映されます。このことは、繰り返しのスケジュールでレポートが生成されている場合に重要です。さらに、レポート設定を編集して更新すると、 Cisco DNA Center プラットフォーム の以前のレポートはすべて削除されます。このウィンドウで、[Update Schedule] ボタンをクリックすると、削除に関する警告が GUI に表示されます。[Update Schedule] ボタンをクリックして以前のすべてのレポートを削除するために設定で編集を行う必要はありません。

- [Duplicate]：レポートのパラメータを表示または設定できる [Schedule] ウィンドウが開きます。レポートを再度実行するには、[Schedule] をクリックします。

  （注） 既存のレポートとその設定に基づいて新しいレポートを作成する場合は、[Duplicate] オプションを使用し、設定を変更します。これにより、既存のレポートとその設定を保持したまま、既存のレポートと同様の新しいレポートを作成できます。既存のレポートを廃棄して新しいレポートに完全に置き換える場合は、前述のように [Edit] オプションを使用します。

- [Run Now]：レポートを実行するプロセスを開始します。レポートの実行が成功すると、成功メッセージが表示されます。

  （注） レポートを実行しようとしたときに以前のレポートが 7 個ある場合、最後の 7 つのレポートのみが保存されることを示す警告が GUI に表示されます。レポートの既存のスケジュール以外でレポートを生成する必要がある場合は、[Run Now] オプションを使用します。

- [Delete]：レポートを削除します。レポートを削除する前に、このアクションを確認するよう求められます。

第 18 章

データ プラットフォームを使用した Cisco DNA Center のトラブルシューティング

データ プラットフォームについて

データ プラットフォームには、Cisco DNA Center アプリケーションのモニタとトラブルシューティングに役立つツールがあります。[データ プラットフォーム（Data Platform）] には、ネットワークのパターン、トレンド、問題領域を特定するのに役立つ、さまざまな入力から合成されたデータが表示されます。たとえば、ネットワークに問題が発生した場合、パイプラインがエラー状態になっているかどうか、特定のエリアにおけるリアルタイム トラフィック フローが何かなど、問題に対する回答を迅速に得ることができます。データ プラットフォームの主なエリアは次のとおりです。

- [Analytics Ops Center]：データがコレクタとパイプラインを経由してどのように流れているかをグラフィカルに表示します。また、ネットワーク内のパターン、傾向、および問題領域を特定できる Grafana ダッシュボードも用意されています。「分析 Ops センターを使用したトラブルシューティング （318 ページ）」を参照してください。

- [Collectors]：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。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。「コレクタの設定情報の表示または更新 （320 ページ）」を参照してください。

- [Store Settings]：アプリケーションデータの保存期間を指定できます。「データ保持設定の表示 （321 ページ）」を参照してください。

- [Pipelines]：Cisco DNA Center アプリケーションが、ストリーミングデータを処理できるようにします。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な

情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。「パイプライン ステータスの表示 （321 ページ）」を参照してください。

分析 Ops センターを使用したトラブルシューティング

分析 Ops センターは、データがコレクタとパイプラインを経由してどのように流れているかに関するグラフィカル表示を提供します。また、ネットワーク内のパターン、傾向、次のような問題領域を特定するために役立つ Grafana ダッシュ ボードを提供します。

- アシュアランス の見つからないデータ。
- 不正確な正常性スコア。
- デバイスがインベントリではモニタ対象として表示され、アシュアランス ではモニタ対象外として表示される。

ステップ 1 Cisco DNA Centerのホームページで、歯車のアイコン ⚙ をクリックして、**[システムの設定（System Settings）]** > **[データ プラットフォーム（Data Platform）]** の順に選択します。

ステップ 2 [分析 Ops センター（Analytics Ops Center）] をクリックします。
アプリケーションのリストが表示されます。

ステップ 3 メトリックを表示するアプリケーション名、たとえば、[Assurance] をクリックします。

アプリケーション内のすべての既存のコレクタとパイプラインのグラフィカル表示が現れます。また、各パイプラインに対応する CPU またはスループット値も提供されます。

各コンポーネントの現在のヘルス ステータスは、色によって示されます。

- 赤色：エラー
- 黄色：警告
- 灰色：通常動作

ステップ 4 パイプラインの履歴データを表示するには、[タイムライン&イベント（Timeline & Events）] をクリックします。

時間間隔のデータを提供するタイムライン バーが表示されます。次のことも実行できます。

- スライダを移動して、特定の時間のデータを表示する
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- イベントをクリックして、その特定の時点での分析 Ops センターの可視化を表示する

ステップ 5 問題のトラブルシューティングに役立つ追加の詳細を表示し、エラーまたは警告の原因を特定するには、コレクタ名をクリックします。

スライドインペインに次のタブが表示されます。

- [Metrics]：直近 30 分間に収集された使用可能なメトリックの選択肢が提示されます。コンポーネントのステータス、開始時間と停止時間、およびエラーの例外を示す概要情報が表示されます。別の時間間隔を選択することもできます。
- [Grafana]：より詳細にデバッグするために各コンポーネントに関連付けられているダッシュボードが表示されます。

ステップ 6 データが特定のパイプラインを経由して流れているかどうかを表示するには、パイプラインストリームをクリックします。

スライドインペインが表示され、内部にグラフが表示されます。グラフは、アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示します。グラフの情報は、スライドインペインでドロップダウンリストから選択する時間間隔に基づきます。オプションは、[直近30分間（Last 30 Min）]、[直近1時間（Last Hour）]、[直近2時間（Last 2 Hours）]、および [直近6時間（Last 6 Hours）] です。デフォルトは、[Last 30 Min] です。

ステップ 7 パイプラインが通常レベルで流れていない場合は、カーソルをストリームに合わせると、遅延メトリックが表示されます。

ステップ 8 特定のパイプラインの詳細情報を表示するには、パイプライン名をクリックします。

適切な [パイプライン（Pipeline）] ページが、次のタブとともに表示されます。

（注） [Exceptions] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

ステップ 9 [Analytics Ops Center] ページに表示されるメトリックを変更するには、[Key Metrics] をクリックして、最大 2 つのメトリックを選択し、[Apply] をクリックします。

デフォルトでは、Cisco DNA Center は CPU とスループットのメトリックを表示します。

ステップ 10 特定のフローのメトリックを表示するには、次を実行します。

a) [フローの詳細を表示（View Flow Details）] をクリックします。
b) コンポーネントの左上隅にあるチルダ（～）をクリックして、3 つの接続されたコンポーネント（コレクタ、パイプライン、ストア）を選択します。
c) [フローを表示（View Flow）] をクリックします。
Cisco DNA Center は、その特定のフローに関連付けられたメトリックを表示します。

コレクタの設定情報の表示または更新

コレクタは、さまざまなネットワークテレメトリおよびコンテクスチュアルデータをリアルタイムで収集します。データが取り込まれると、Cisco DNA Center はデータを関連付けて分析します。コレクタのステータスを表示し、問題領域をすばやく見分けることができます。

ステップ 1 Cisco DNA Centerのホームページで、歯車のアイコン をクリックして、**[システムの設定（System Settings）]** > **[データ プラットフォーム（Data Platform）]** の順に選択します。

ステップ 2 [コレクタ（Collectors）] をクリックします。各コレクタの横にある色付きの点は、全体的なステータスを示しています。

ステップ 3 追加の詳細を表示するには、コレクタ名をクリックします。

適切な *[コレクタ（Collector）]* ページが表示されます。デフォルトでは、Cisco DNA Center に **[設定（Configuration）]** タブが表示され、現在の設定リストを確認できます。

ステップ 4 構成を表示、更新、または削除するには、特定の構成名をクリックします。

ステップ 5 新規の設定を追加するには、**[設定（Configuration）]** タブで **[追加（+ Add）]** をクリックします。

スライドインペインが表示されます。

（注） [コレクタISE（COLLECTOR-ISE）] の設定については、Cisco ISE 版 Cisco DNA Center の統合の設定 （78 ページ）項を参照してください。

ステップ 6 設定に必要な情報をスライドインペインに入力します。

ステップ 7 （任意） **[匿名化（Anonymize）]** チェックボックスをオンにすると、**[WIRELESSCOLLECTOR]** などの一部コレクタのデータを匿名化できます。

（注） **[匿名化（Anonymize）]** チェックボックスをオンにすると、**[クライアントの健全性（Client Health）]** ウィンドウに表示されるホスト名とユーザ ID は、復号化できない一方向ハッシュを用いてスクランブル処理されます。

重要 データを匿名化する場合は、**[ディスカバリ（Discovery）]** ツールを使用してデバイスを検出する前に、**[匿名化（Anonymize）]** チェックボックスをオンにしてください。デバイスを検出した後にデータを匿名化した場合、システムに入ってくる新しいデータは匿名化されますが、既存のデータは匿名化されません。

ステップ 8 [Save Configuration] をクリックします。

ステップ 9 設定されているインスタンスを表示するには、[インスタンス（Instances）] タブをクリックします。

ステップ 10 概要情報とメトリックを表示するには、リストからインスタンスを選択します。

ステップ 11 （任意） Cisco DNA Center を Cisco Connected Mobile Experience（CMX）と統合する場合は、CMX 側でデータの匿名化を選択できます。次の手順を実行します。

a) SSH クライアントを使用して、cmxadmin CLI ユーザとして Cisco CMX にログインします。

b) ルートユーザに変更します。

c) `/opt/cmx/etc/node.conf` に移動し、`[location]` の下に **`user_options`** を追加します。次に例を示します。

```
[location]
…
user_options=-Dhideusername=true
```

d) Cisco CMX CLI で、次のコマンドを入力します。

```
cmxctl agent restart
cmxctl location restart
```

データ保持設定の表示

アプリケーションのデータの保存期間を表示できます。

ステップ 1 Cisco DNA Centerのホームページで、歯車のアイコン をクリックして、**[システムの設定（System Settings）]** > **[データ プラットフォーム（Data Platform）]** の順に選択します。

ステップ 2 [ストア設定（Store Settings）] をクリックします。

ステップ 3 完了した履歴消去ジョブのリストを表示するには、[データ消去スケジュール（Data Purge Schedule）] をクリックします。

[HISTORY] テーブルには、消去ジョブの名前、結果、時刻、その他のデータが表示されます。テーブル内のデータをソート、フィルタリング、エクスポートすることができます。

ステップ 4 現在のデータの保持または消去の設定を表示するには、[Data Retention & Purge Configuration] をクリックします。次の出力が表示されます。

- [Document Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのデータの設定。
- [Metric Graph Store]：最大サイズ、ウォーターマークの下限および上限しきい値など、すべての時間ベースのグラフィカルデータの設定。

パイプライン ステータスの表示

データ パイプラインによって、Cisco DNA Center アプリケーションは、ストリーミング データを処理できます。データ パイプラインでは、外部ソースからの入力データを受け入れ、有用な情報を提供するためにそのデータを変換し、出力データを生成する一連の計算をカプセル化します。パイプラインのステータスを表示し、問題領域をすばやく見分けることができます。

ステップ 1 Cisco DNA Centerのホームページで、歯車のアイコン をクリックして、**[システムの設定（System Settings）]** ＞ **[データ プラットフォーム（Data Platform）]** の順に選択します。

ステップ 2 [パイプライン（Pipelines）] をクリックします。

ステップ 3 アプリケーションが基盤となるパイプラインからデータを受信しているかどうかを表示するには、パイプライン名をクリックします。

適切な [パイプライン（Pipeline）] ページが、次のタブとともに表示されます。

（注） [例外（Exceptions）] タブをクリックして、パイプラインで例外が発生していないかどうかを確認してください。通常の動作状況では、このタブは **null** を表示します。

- **メトリック**：グラフ中で 30 分ごとに更新されるメトリックを表示します。
- **サマリ**：統計、ランタイム、マニフェストなどのサマリ情報を表示します。
- **例外**：パイプラインで発生した例外を表示します。
- **ステージ**：パイプラインのステージを表示します。

第 19 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。

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
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 Assurance 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

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...
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 Assurance 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