

Cisco Catalyst Assurance リリース 3.2.x ユーザーガイド

最終更新：2026 年 10 月 15 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

© 2026 Cisco Systems, Inc. All rights reserved.



目 次

第 1 章 新機能および変更された機能に関する情報 1

Cisco Catalyst Assurance の新機能および変更された機能 1

第 2 章 Cisco Catalyst Assurance の概要 3

Assurance の概要 3

Assurance のアーキテクチャ 4

IPv6 アドレスのサポート 5

ユーザープロファイルのロールおよび権限 5

Assuranceの開始 6

第 3 章 Cisco AI Network Analytics の概要 7

About Cisco AI Network Analytics 7

Cisco AI Network Analytics の利点 10

Cisco AI Network Analytics のライセンスと導入 11

第 4 章 Assurance を使用するための Catalyst Center の設定 13

Assurance での制限事項と制約事項 13

基本的な設定のワークフロー 13

デバイスの検出 16

検出の概要 16

ディスカバリの前提条件 17

優先管理 IP アドレス 18

検出設定のガイドラインと制限事項 19

ディスカバリクレデンシャル 20

CDP を使用したネットワークの検出 26
IP アドレス範囲または CIDR を使用したネットワークの検出 29
LLDP を使用したネットワークの検出 32
ディスカバリジョブの管理 35
ディスカバリ ジョブの停止および開始 35
ディスカバリジョブの複製 35
ディスカバリ ジョブの削除 36
ディスカバリ ジョブ情報の表示 36
ネットワーク階層 37
ネットワーク階層の作成 39
サイトの作成、編集、削除 39
ビルディングの追加、編集、および削除 41
フロアの追加、編集、および削除 42
既存のシスコのネットワーク階層 44
Cisco Prime Infrastructure からのサイト階層のエクスポート 45
Cisco Prime Infrastructure からのマップアーカイブのエクスポート 45
Catalyst Center へのサイト階層のインポート 46
Catalyst Center へのマップアーカイブのインポート 47
既存の Ekahau ネットワーク階層の使用 48
Catalyst Center からの Ekahau プロジェクトのエクスポート 48
Ekahau プロジェクトを Catalyst Center にインポートします。 48
Ekahau サイト調査の Catalyst Center へのインポート 50
2D フロアマップのデバイスとオーバーレイオブジェクトの設定 52
AP の追加、配置、編集、削除 53
センサーの追加、配置、削除 55
カバレッジエリアの追加、編集、削除 56
吹き抜けの追加、編集、コピー、および削除 57
ロケーションリージョンの追加、編集、および削除 58
壁の追加、編集、および削除 60
シェルフユニットの追加、コピー、編集、および削除 61
マーカーの追加、編集、および削除 62

GPS マーカーの追加、編集、および削除 63
位置合わせポイントの追加、編集、および削除 64
インベントリの管理 64
インベントリについて 64
デバイスポーリング間隔の更新 66
インベントリに関する情報の表示 66
SSH キー検証エラーへの対処 76
SSH キー変更の自動承認の設定 77
ネットワークデバイスの削除 77
デバイス構成を今すぐまたは後で展開する 78
デバイス設定のプレビューと展開 79
プロビジョニングされていないデバイスのサイトへの割り当て 81
マップへの AP の追加 83
AP をマップ上に配置する 84
Cisco ISE の Catalyst Center 設定について 88
認証サーバーとポリシーサーバーの設定 88
テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 93
Cisco AI Network Analytics の設定 95
Cisco AI Network Analytics の無効化 97
機械推論ナレッジベースの更新 98
ローカリゼーションの有効化 99

第 5 章 企業全体の健全性のモニターとトラブルシューティング 101
エンタープライズ 101
企業全体の健全性のモニターとトラブルシューティング 101

第 6 章 ネットワーク正常性のモニターとトラブルシューティング 107
ネットワークの正常性のモニターとトラブルシューティング 107
デバイスの正常性のモニターとトラブルシューティング 117
Cisco StackWise Virtual と制限事項について 138

Cisco StackWise と制限事項について 139
ネットワークデバイスの正常性スコアの設定 139
ファブリックデバイスの SNMP コレクタメトリックの有効化 141
ネットワークの正常性スコアと KPI メトリックについて 143
ネットワークの正常性スコア 143
デバイスカテゴリの正常性スコア 143
個別のデバイス正常性スコア 143
スイッチの正常性スコア 145
ルータの正常性スコア 146
AP の正常性スコア 148
ワイヤレスコントローラの正常性スコア 149
ネットワークの正常性スコアと KPI メトリックに対するメンテナンス モードの影響 151
RF の計算について 152

第 7 章 クライアント正常性のモニターとトラブルシューティング 155
リモート LAN サポート 155
ワークグループ ブリッジ クライアントのサポート 155
すべてのクライアントデバイスの正常性のモニターとトラブルシューティング 156
クライアントデバイスの正常性のモニターとトラブルシューティング 173
クライアント追跡 186
既知のクライアントの追跡 187
新しいクライアントの追跡 188
クライアントの追跡の停止 190
除外クライアントの設定 191
クライアントの正常性スコアと KPI メトリックについて 192
クライアントの正常性スコア 192
クライアント オンボーディング スコア 193
クライアントの接続スコア 193
個別のクライアント正常性スコア 195

第 8 章 アプリケーション健全性のモニター 197

アプリケーション エクスペリエンスとアプリケーションの可視性について 197
サポートされるプラットフォーム 199
デバイスでのアプリケーションテレメトリ有効化の基準 200
アプリケーションの正常性の前提条件 203
アプリケーションテレメトリ設定のプロビジョニング 205
ホストのアプリケーション エクスペリエンスの表示 206
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 208
すべてのアプリケーションの正常性のモニター 210
ThousandEyes Enterprise Agent のインストール 221
企業エージェントとテストの管理 224
アプリケーションの正常性をモニター 226
Webex アプリケーション正常性のモニターとトラブルシューティング 231
Microsoft Teams アプリケーションの正常性のモニターとトラブルシューティング 235
アプリケーションの正常性スコアの設定 239
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 240
全体的なアプリケーション正常性スコア 240
個別アプリケーションの正常性スコア 240

第 9 章 ネットワークサービスの監視 243
AAA ネットワークサービスのモニター 243
DHCP ネットワークサービスの監視 247
DNS ネットワークサービスの監視 252

第 10 章 SD-Access の正常性のモニターとトラブルシューティング 257
SD-Access ファブリック 257
ファブリックサイトの追加 257
デバイスをファブリックに追加 261
SD-Access ファブリックの正常性のモニターとトラブルシューティング 265
ファブリックサイトの正常性の監視 271
トランジットおよびピアネットワークの正常性の監視 276
仮想ネットワークの正常性の監視 281

第 11 章 サイト分析を使用したネットワークのモニターとトラブルシューティング 287

サイト分析について 287

[Site Analytics] ダッシュボードのインサイト 289

サイト分析の表示 292

サイト分析設定の構成 297

第 12 章 問題の表示と管理 299

問題について 299

機械推論エンジンについて 300

VLAN に関連するレイヤ 2 ループの問題について 300

未解決の問題の表示 301

AI 駆動型の問題の問題インスタンスの詳細 306

AP 切断の問題についての [Issue Instance Details] 309

レイヤ 2 ループ問題の問題インスタンスの詳細 310

PoE の問題に関する問題インスタンスの詳細 314

アプリケーション正常性低下の問題に関する問題インスタンスの詳細 317

MRE を使用した有線クライアントの問題のトラブルシューティング 319

解決済みの問題の表示 322

無視された問題の表示 324

問題の解決または無視 326

無線にアクティビティなしの問題のトリガー 328

自動問題解決 328

グローバルな問題の設定の管理 332

ユーザー定義問題の設定の管理 334

カスタム問題の設定の管理 336

問題の通知の有効化 338

Assurance、Cisco AI Network Analytics、および MRE の問題 341

ルータの問題 341

コア層、ディストリビューション層、アクセス層に関する問題 344

サードパーティ製デバイスの問題 349

コントローラの問題 349
アクセスポイントの問題 350
有線クライアントの問題 352
ワイヤレスクライアントの問題 353
AAA 障害の根本原因分析問題を有効化 357
アプリケーションは、次を発行する。 358
センサーの問題 358
AI 駆動型の問題 361
MRE の問題 362

第 13 章 イベントの表示と管理 365
イベントダッシュボードの概要 365
デバイスイベントの表示 366
エンドポイントイベントの表示 369
イベント分析ダッシュボードの表示 375

第 14 章 センサーの管理とセンサー主導のテスト 381
センサーとセンサー主導のテストについて 381
センサーのプロビジョニング 382
ワイヤレス Cisco Aironet 1800s アクティブセンサーのプロビジョニング 382
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 382
Cisco Catalyst 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 383
AP またはセンサーデバイスのプロビジョニング 384
センサーを使用したネットワーク正常性のモニターとトラブルシューティング 388
すべてのワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング 388
ワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング 394
センサーとバックホール設定の管理 396
ネットワーク内のセンサーの管理 396
バックホール設定の管理 398

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 400
SCEP プロファイルの管理 401
センサー主導テスト 402
テンプレートを使用したセンサー主導テストの作成と実行 402
センサー主導テストのテンプレートの管理 407

第 15 章 Wi-Fi 対応状況のモニター 409
Wi-Fi 対応状況の評価 409
Wi-Fi ネットワークの対応状況の確認 409

第 16 章 Power over Ethernet の監視 417
Power Over Ethernet について 417
PoE テレメトリの設定ワークフロー 417
PoE テレメトリに使用するデバイスでの NETCONF の設定 419
PoE テレメトリのテレメトリ設定の更新 422
ネットワーク内の PoE 対応デバイスのモニター 422

第 17 章 ダッシュボードの管理 431
ダッシュボードについて 431
カスタムダッシュボードの作成 431
ダッシュボードの表示 432
ダッシュボードの編集または削除 433
ダッシュボードの複製 433
ダッシュボードをお気に入りに設定 434
ダッシュレットの位置の変更 434
フィルタグループの設定 435

第 18 章 ネットワークのトレンドの観察およびインサイトの取得 437
ネットワークのトレンドとインサイトについて 437
ワイヤレス AP のパフォーマンスアドバイザリの表示 438
ネットワークのトレンドの表示とインサイトの取得 442

ネットワークヒートマップでのアクセスポイントおよびスイッチの比較 448
ネットワーク内のピアとの KPI 値の比較 451
建物、AP モデルファミリ、ワイヤレス エンドポイント タイプの比較 453
ベースラインを使用したネットワークパフォーマンスの表示と監視 457
AI 拡張 RRM ダッシュボードを使用した RF ネットワークの表示 460

第 19 章 インテリジェントキャプチャの管理 479
インテリジェントキャプチャについて 479
インテリジェントキャプチャのサポート対象デバイス 480
インテリジェントキャプチャのベストプラクティス 480
インテリジェントキャプチャの設定方法と使用方法 481
クライアントデバイスのオンボーディング パケット キャプチャ 481
クライアントデバイスのオンボーディング パケット キャプチャについて 481
クライアント統計情報について 482
クライアントデバイスのライブ オンボーディング パケット キャプチャ セッションの実行 482
クライアントデバイスのオンボーディングパケットキャプチャセッションのスケジュール 488
進行中のクライアントデバイスのオンボーディング パケット キャプチャ セッションの停止 489
クライアントデバイスのフルパケットキャプチャ 489
クライアントデバイスのフルパケットキャプチャについて 489
クライアントデバイスのフル パケット キャプチャ セッションの実行 490
フルパケットキャプチャ履歴の表示 493
Wi-Fi 帯域およびチャネルの OTA スニファキャプチャ 494
Wi-Fi 帯域およびチャネルの OTA スニファキャプチャについて 494
Wi-Fi 帯域およびチャネルの OTA スニファ キャプチャ セッションの実行 494
完了した OTA スニファキャプチャ セッションからの PCAP ファイルのダウンロード 497
AP およびワイヤレスコントローラの AP 統計情報のキャプチャ 498
AP およびワイヤレスコントローラの AP 統計情報キャプチャについて 498
特定の AP での AP 統計キャプチャの有効化または無効化 498

ワイヤレスコントローラでの AP 統計キャプチャの有効化/無効化 499
AP 統計情報キャプチャに対応していない AP の表示 501
AP の RF 統計の表示 502
AP およびワイヤレスコントローラの異常キャプチャ 505
AP およびワイヤレスコントローラの異常キャプチャについて 505
特定の AP での異常キャプチャの有効化または無効化 505
ワイヤレスコントローラ での異常キャプチャの有効化または無効化 506
異常キャプチャに対応していない AP とサポートされている AP の表示 508
AP のスペクトル解析 509
スペクトル解析時の Cisco AP 機能について 509
AP でのスペクトル解析セッションの開始 510
AP のスペクトル解析データの表示 511
有線クライアントデバイス向けパケットキャプチャ 514
有線クライアントデバイスでのパケットキャプチャの実行 515
実行中のキャプチャの停止 517
完了したパケットキャプチャのダウンロード 517
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 518
クライアントまたは AP がインテリジェント キャプチャ データを Catalyst Center に送信できない 518
有線パケットキャプチャの問題のトラブルシューティング 518

第 20 章 SSID モニタリング設定の管理 521
SSID モニタリングについて 521
SSID モニタリングの設定 522
SSID モニタリングのプロビジョニングステータスの表示 523

第 21 章 デバイスのパスをトレース 525
パストレースについて 525
パストレースの制限事項 525
パストレースの実行 528

第 22 章 ワイヤレスマップ向け Cisco CMX の統合 533

Cisco Connected Mobile Experiences の統合について 533

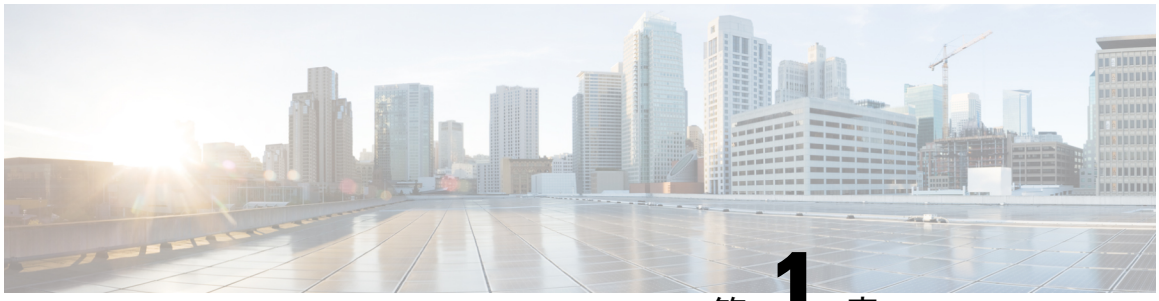
Cisco CMX API サーバーへのユーザーの追加 533

Cisco CMX 設定の作成 534

Cisco CMX のトラブルシューティング 536

第 23 章 アシュアランス監査ログの表示 539

Assurance の監査ログの表示 539



第 1 章

新機能および変更された機能に関する情報

• Cisco Catalyst Assurance の新機能および変更された機能 （1 ページ）

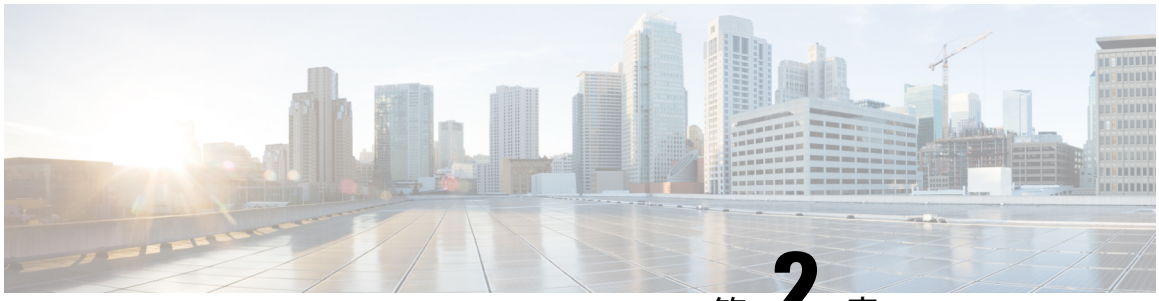
Cisco Catalyst Assurance の新機能および変更された機能

Cisco Catalyst Assurance での新機能および変更された機能の要約と参照先を次の表に示します。

表 *1 : Cisco Catalyst Assurance 3.2.2* の新機能および変更された機能

機能	説明
クライアントがネットワークから切断される場合の追跡	クライアントがネットワークから切断された場合に追跡し、切断通知を受信できるようになりました。 クライアント追跡 （186 ページ）を参照してください。
Wi-Fi 7 機能のサポート	Wi-Fi 7 機能のサポートが Client 360 に追加されます。マルチリンク動作（MLO）対応クライアントが、2.4GHz、5GHz、または 6GHz 帯域のさまざまな組み合わせに同時接続できるようになりました。 「Wi-Fi 対応状況の評価」および「ネットワークの Wi-Fi 対応状況の確認」を参照してください。
デバイスとクライアントの正常性の拡張機能	再試行などの重要な KPI を組み込み、WLC HA ペア障害とモビリティ トンネル ステータスを監視して、ワイヤレス LAN コントローラとクライアントの正常性スコアと問題検出を強化し、お客様固有のエスカレーションしたユースケースを含む正確なユーザー正常性スコアを反映するように、問題のトリガーを改善しています。
ThousandEyes エージェントの機能強化	直接、静的、および PAC の各プロキシ設定、カスタマイズ可能な Docker ランタイムオプション、およびリソースとネットワーク設定をモニタリングするためのエージェント詳細ビューのサポートが追加されました。 企業エージェントとテストの管理 （224 ページ）を参照してください。

機能	説明
産業用イーサネット（IE）スイッチのサポート	Catalyst Center は、Cisco Catalyst Industrial Ethernet（IE）3500 シリーズと Cisco Catalyst Industrial Ethernet（IE）9300 シリーズ スイッチの ThousandEyes エージェント管理をサポートするようになりました。 「ThousandEyes Enterprise Agent のインストール」を参照してください。
屋外エリアのサポート	Catalyst Center は、[屋外エリア（Outdoor Areas）] を Assurance ダッシュボードで明確なサイトタイプとしてサポートするようになりました。屋外アクセスポイントを監視し、サイトマップや階層内でその正常性ステータスを表示できます。 「ネットワークの正常性のモニターとトラブルシューティング」、「すべてのクライアントデバイスの正常性のモニターとトラブルシューティング」、「ネットワーク内の PoE 対応デバイスのモニター」、および「ネットワークの Wi-Fi 対応状況の確認」を参照してください。
AAA Network Services の拡張機能	ワイヤレスコントローラとスイッチの両方から、AAA サーバーのトランザクション統計情報、遅延の傾向、クライアントイベントを集約して表示できるようになりました。 AAA ネットワークサービスのモニター （243 ページ）を参照してください。
OTA スニファキャプチャの拡張機能	OTA パケットキャプチャの拡張機能により、複雑な Wi-Fi 7 やマルチリンク動作（MLO）環境の障害対応における柔軟性が向上します。この拡張機能により、複数の無線とアクセスポイント（AP）にわたる同時トラフィックキャプチャが可能になります。
AI syslog の自動要約と説明	イベント分析ダッシュボードでの syslog メッセージの AI による自動要約と AI インサイトにより、生の syslog データが実用的なインサイトに変換されるため、傾向を迅速に特定できるようになり、効率的なイベント分析と管理が容易になります。 イベント分析ダッシュボードの表示 （375 ページ） を参照してください
正常性スコアベースの問題	Catalyst Center では、アプリケーションの正常性スコアが設定可能なしきい値（デフォルトで 7 に設定）を下回っている場合、[アプリケーションの正常性低下（Application Health Degradation）] の問題が自動的に生成されるようになりました。 問題はアプリケーションとサイトの両方によって分類され、正常性低下が複数のロケーションにまたがる場合は、サイトごとに個別の問題が作成されます。
有線クライアントデバイス向けパケットキャプチャ	Assurance からパケットキャプチャを開始して、有線クライアントデバイスの接続やトラフィックの問題をトラブルシュートできるようになりました。 有線クライアントデバイス向けパケットキャプチャ （514 ページ）を参照してください。



第 2 章

Cisco Catalyst Assurance の概要

- Assurance の概要 （3 ページ）
- Assurance のアーキテクチャ （4 ページ）
- IPv6 アドレスのサポート （5 ページ）
- ユーザープロファイルのロールおよび権限 （5 ページ）
- Assuranceの開始 （6 ページ）

Assurance の概要

Assurance 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。

Assurance には次の利点があります。

- 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。Assurance 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。Assurance 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行われます。
- 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。

Assurance のアーキテクチャ

Assurance アーキテクチャは、次のようなネットワークデータ収集および分析システムです。

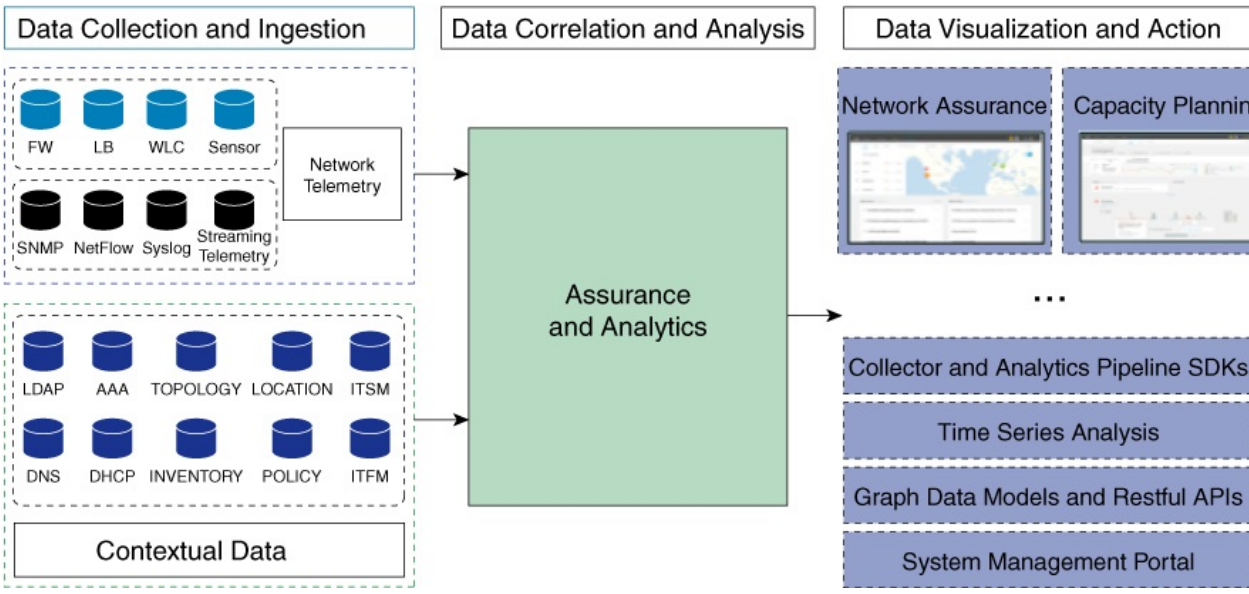
- ストリーミングテクノロジーを使用してさまざまなテレメトリおよびコンテキストデータをリアルタイムで収集します。
- データ収集および分析レイヤを抽象化し、リッチな API と Web インターフェイスを公開します。
- モニタリングや障害対応からポリシー検出やキャパシティプランニングまで、幅広いビジネスユースケースに対応できます。

企業は多数のネットワークデータを扱っています。ネットワークデータの量、種類、速度、および精度に対処することは、IT 部門にとって重要です。Assurance のアーキテクチャは、大規模な複数タイプのネットワークデータを処理するためのソリューションを提供することで、これらの課題に対処するように設計されています。

Assurance 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。

次の図とその後の情報で、Assurance のアーキテクチャについて説明します。

図 *1 : Assurance* のアーキテクチャ



- **データ収集と取り込み**：Assurance 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、Assurance 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 Assurance やキャパシティプランニング用のその他のアプリケーションに公開されます。Assurance は、以下を提供するオープンシステムです。
  - コレクタと分析パイプライン SDK
  - 時系列分析
  - グラフデータモデルと RESTful API
  - システム管理ポータル

IPv6 アドレスのサポート

IPv6 アドレスは、次のようなネットワーク識別子です。

- IPv6 対応ネットワーク上のデバイスを一意に識別します。
- 128 ビットアドレス方式に従います。
- 複数のテキスト形式で表すことができます。

Catalyst Center および Cisco Catalyst Assurance では IPv6 アドレスがサポートされています。単一の IPv6 アドレスは多くのテキスト形式で表現できますが、Catalyst Center でサポートされているのは標準形式の IPv6 アドレスのみです。標準形式は、正規化圧縮形式とも呼ばれます。

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

ユーザープロファイルのロールおよび権限

Catalyst Center は、ロールベースアクセスコントロール（RBAC）をサポートします。権限は、ユーザーロールによって定義されます。Catalyst Center には次の 3 つの主要なデフォルトユーザーロールがあります。

- SUPER-ADMIN-ROLE
- NETWORK-ADMIN-ROLE
- OBSERVER-ROLE

SUPER-ADMIN-ROLE は、包括的なアクセスを許可し、Catalyst Center GUI でのカスタムロールの作成と割り当てをサポートします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE のユーザーロールは、アクセスが制限されます。

特定のネットワークサイトへのアクセスを制限するアクセスグループを作成できます。アクセスグループはロールとサイトの組み合わせです。特定のアクセスグループにいつでもログインできます。

Catalyst Center は、次のデフォルトアクセスグループをサポートしています。

- **NW-ADMIN_Global**：NW-ADMIN ロールへのグローバルアクセス用のアクセスグループ
- **[OBSERVER_Global]**：OBSERVER ロールへのグローバルアクセス用のアクセスグループ
- **SUPER-ADMIN_Global**：SUPER-ADMIN ロールへのグローバルアクセス用のアクセスグループ

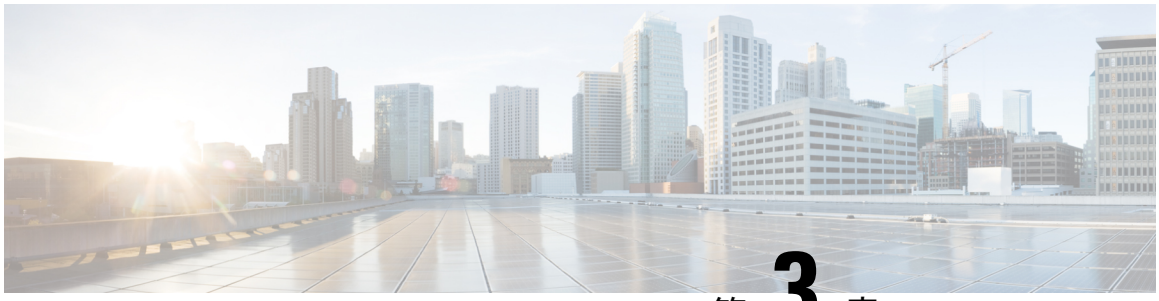
Catalyst Center の機能の動作は、アクセスグループで指定されたユーザーロールとサイトによって異なります。詳細については、『Cisco Catalyst Center Administrator Guide』の「Configure site-based, role-based access control」を参照してください。

Assuranceの開始

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

Catalyst Center の設定後、現在の環境で Assurance 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（既存の展開）があれば、ディスカバリを実行して開始します。ディスカバリを実行すると、すべてのデバイスが [Inventory] ウィンドウに表示されます。詳細については、基本的な設定のワークフロー（13 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 Catalyst Center User Guide*を参照してください。



第 3 章

Cisco AI Network Analytics の概要

- About Cisco AI Network Analytics （7 ページ）
- Cisco AI Network Analytics の利点 （10 ページ）
- Cisco AI Network Analytics のライセンスと導入 （11 ページ）

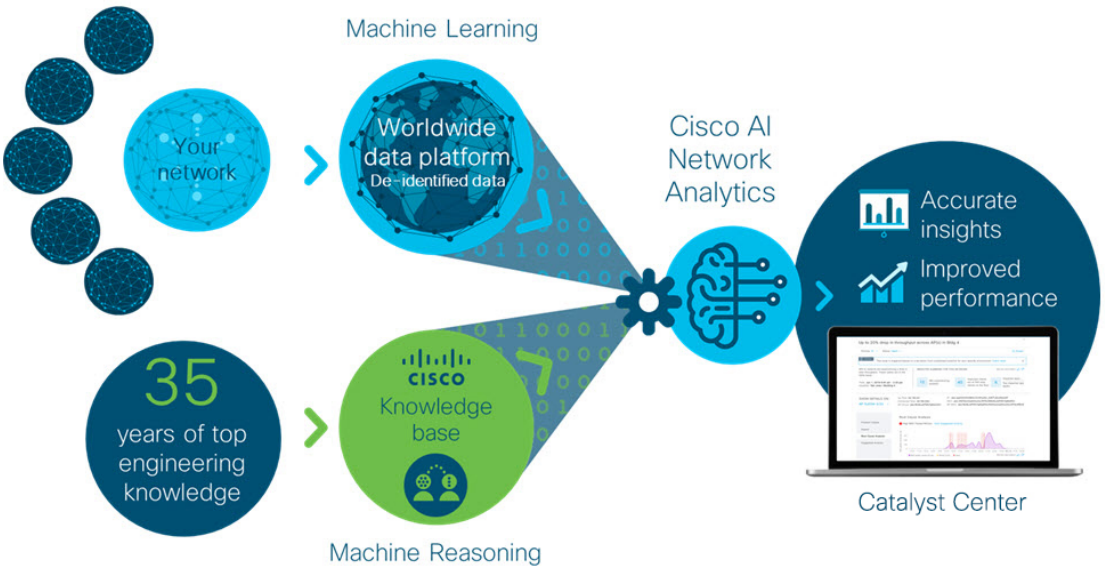
About Cisco AI Network Analytics

AI分析機能のセットは、次のようなネットワーク管理アプリケーションコンポーネントです。

- 機械学習と推論を活用して、匿名化されたネットワークイベントを分析します。
- プロアクティブなインサイト、基準値設定、異常検出、比較ベンチマーク、トレンド分析を提供します。
- クラウドベースのデータプラットフォームと統合して、ネットワークのトラブルシューティングを自動化し、運用効率を向上させます。

次の図とその後の情報で、Cisco AI Network Analytics のアーキテクチャについて説明します。

図 *2 : Cisco AI Network Analytics* のアーキテクチャ



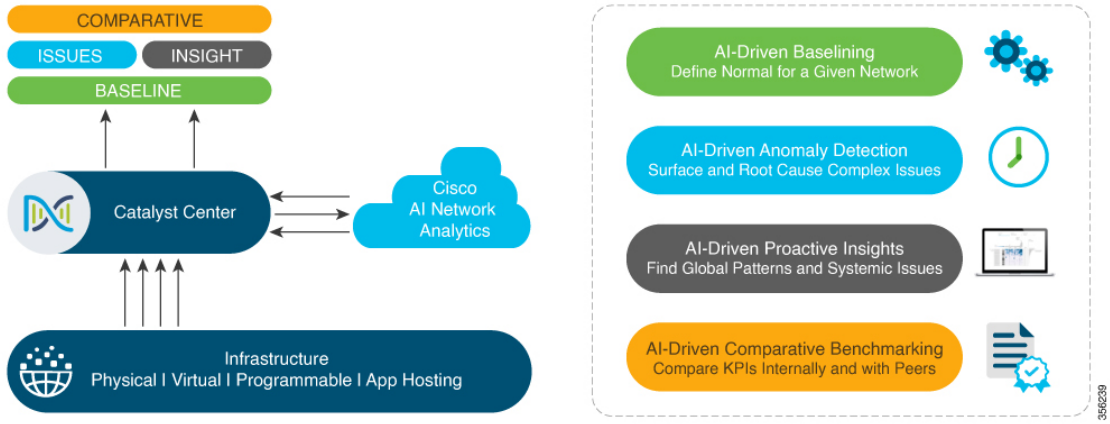
Cisco AI Network Analytics の次の要素で構成されています。

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

機械学習

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

図 *3 : Cisco AI Network Analytics* の機能



Cisco AI Network Analytics 次の機能を提供します。

- **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 Catalyst 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 Catalyst Center に返します。
- [Intelligent Issue Detection and Analysis] には次のものが含まれます。
  - **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 は次のタイプの AI 駆動型の問題を検出できます。
    - **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な DHCP 時間、過剰な DHCP 障害回数、過剰な AAA 時間、過剰な AAA 障害回数、過剰な関連付け時間、過剰な関連付け障害回数。
    - **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーションアプリケーションのスループット、およびソーシャルアプリケーションのスループット。

- [Trends and Insights] には次のものが含まれます。
  - [Trend Deviations]：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。
  - [AP Performance Advisories]：一貫してクライアントエクスペリエンスが低い AP を検出し、根本原因と推奨されるアクションを提供します。
- [Comparative Benchmarking] には次のものが含まれます。
  - [AI-Driven AP Comparisons in Network Heatmaps]：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-Driven Peer Comparisons]：選択されている主要業績評価指標（KPI）について、ピアネットワークと比較したネットワークのパフォーマンスを判断します。
  - [AI-Driven Network Comparisons]：選択されている KPI について、別のネットワークと比較したネットワーク（サイト、建物、AP モデル、クライアントタイプなど）のパフォーマンスを判断します。

Cisco AI Network Analytics の利点

Cisco AI Network Analytics には次の利点があります。

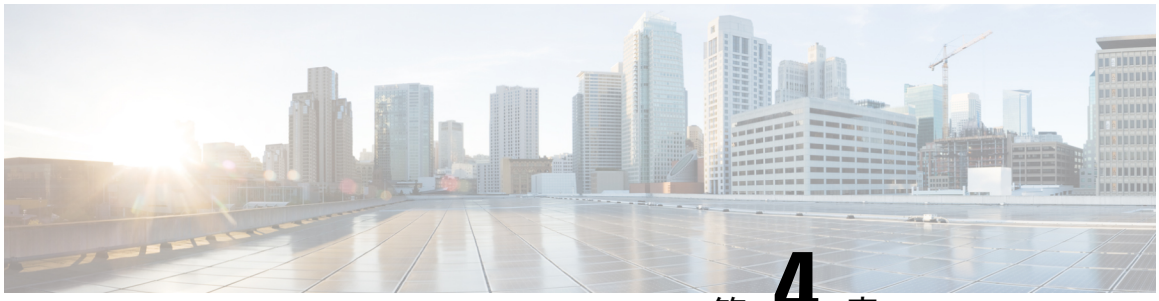
- [More Visibility]：各ネットワークは一意であり、ネットワーク環境は常に変化しています。Cisco AI Network Analytics は、ローカルネットワークから継続的に関連データを収集し、そのデータを集約非特定化データセットと関連付けた後、高度な機械学習モデルを活用して、特定のネットワークとサイトに関連する基準を作成します。これらの基準は、ネットワーク環境の変化に応じて、デバイス、ユーザー、およびアプリケーションが増加するのに伴い学習し、適応していきます。
- [Greater Insight]：Cisco AI Network Analytics では、機械学習を使用して、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。
- [Guided Action]：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、Advantage ソフトウェアライセンス の一部であり、Assurance のユーザーインターフェイスとシームレスに統合される、追加のコンポーネントとして提供されます。Cisco AI Network Analytics により、最先端の機械学習によって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、および対処に必要な可視化ツールも一緒に提供されます。

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）Catalyst Center の実行インスタンスと、Cisco AI Network Analytics クラウドへの HTTPS 接続が必要です。HTTPS 接続は、プロキシサーバーを介してもサポートされます。HTTPS 接続にプロキシサーバーを使用する場合、設定は Catalyst 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、Assurance ユーザーインターフェイスに直接表示されます。詳細については、『Cisco Catalyst Center Offer Disclosure』を参照してください。

Cisco AI Network Analytics では、ストレージと分析のためにクラウドインフラストラクチャへの接続が必要です。ワイヤレス AP の数が 500 未満の場合、効率的なエンコーディングおよび最適化スキームにより、1 日あたりの予測データ使用量はわずか 150 ～ 200 MB です。AP とワイヤレスクライアントに関して、データ使用量はネットワーク展開サイズに比例します。したがって、1800 の AP を使用した大規模な展開では、1 日あたりのデータ使用量は 500 ～ 700 MB になります。



第 4 章

Assurance を使用するための Catalyst Center の設定

- Assurance での制限事項と制約事項 （13 ページ）
- 基本的な設定のワークフロー （13 ページ）
- デバイスの検出 （16 ページ）
- ネットワーク階層 （37 ページ）
- インベントリの管理 （64 ページ）
- プロビジョニングされていないデバイスのサイトへの割り当て （81 ページ）
- マップへの AP の追加 （83 ページ）
- AP をマップ上に配置する （84 ページ）
- Cisco ISE の Catalyst Center 設定について （88 ページ）
- テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （93 ページ）
- Cisco AI Network Analytics の設定 （95 ページ）
- 機械推論ナレッジベースの更新 （98 ページ）
- ローカリゼーションの有効化 （99 ページ）

Assurance での制限事項と制約事項

Assurance では、ネットワークアドレス変換（NAT）を介して接続されたデバイスをサポートしません。

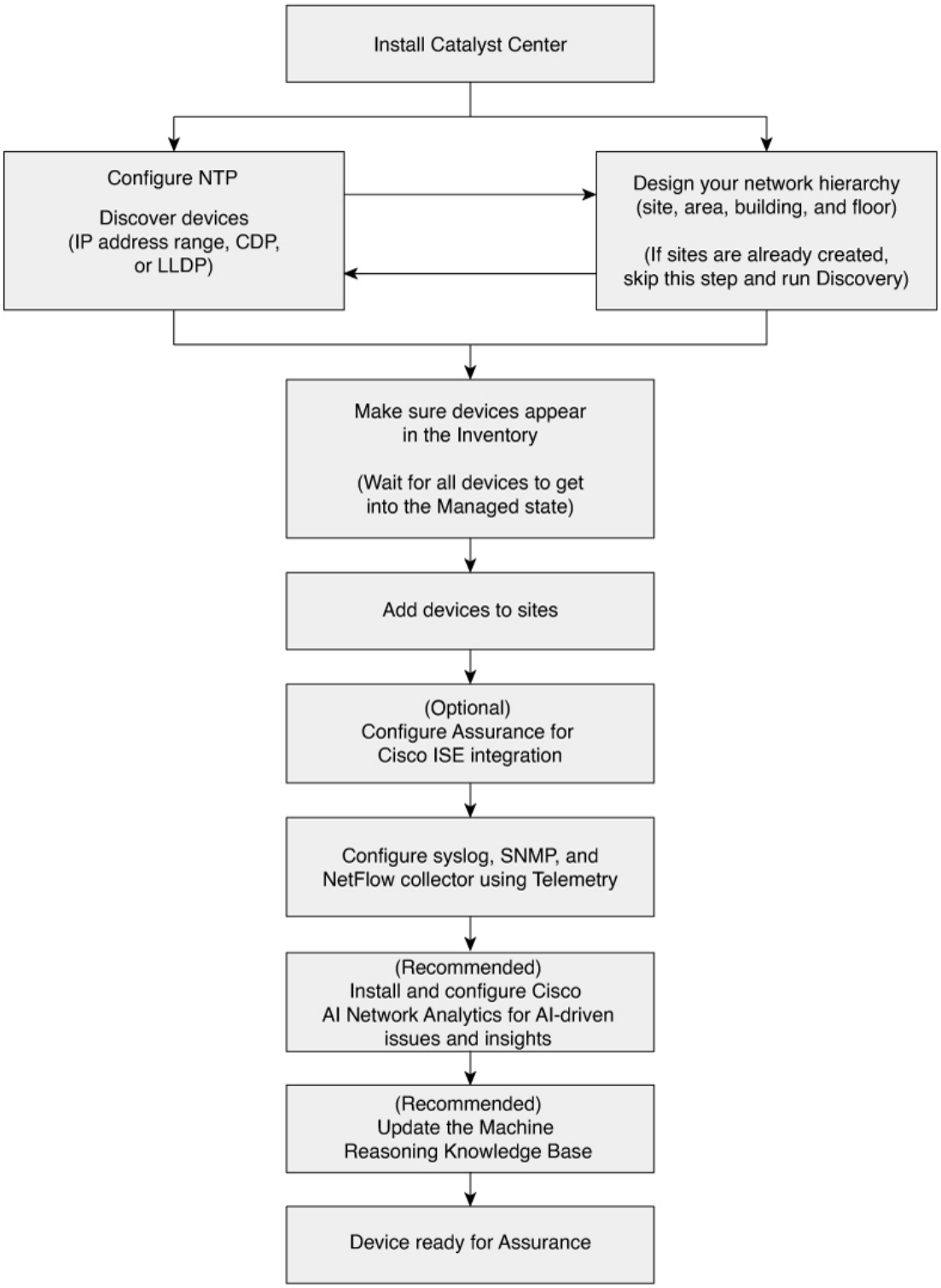
基本的な設定のワークフロー

Assurance アプリケーションの使用を開始する前に、Assuranceを使用するために Catalyst Center を設定する必要があります。

ここでは、Assurance 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 Catalyst Center User Guide* と併用してください。

基本的なワークフローを理解するには、次の図と手順を参照してください。

図 *4 : Assurance* を使用するように *Catalyst Center* を設定するための基本的なワークフロー



始める前に

Assurance での制限事項と制約事項 （13 ページ）を参照してください。

手順

ステップ 1 Catalyst Center をインストールします。

*Cisco Catalyst Center Installation Guide*を参照してください。

ステップ 2 次の操作を任意の順序で行います。

- Catalyst Center およびその管理対象デバイスが Network Time Protocol（NTP）を使用して同期していることを確認します。
- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、アクセス ポイント）を検出します。

  IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、およびLLDP を使用したネットワークの検出 （32 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 のウィンドウでは、データが表示されません。

- 新しいネットワーク階層を設計するか、既存のものを使用します。

  ネットワーク階層の作成 （39 ページ）または既存のシスコのネットワーク階層 （44 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 （66 ページ）を参照してください。

（注） デバイスをサイトに追加する前に、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

プロビジョニングされていないデバイスのサイトへの割り当て （81 ページ）を参照してください。

ステップ 5 AP がある場合は、フロアマップに追加することをお勧めします。

マップへの AP の追加 （83 ページ）を参照してください。

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

Cisco ISE の Catalyst Center 設定について （88 ページ）を参照してください。

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

テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （93 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 の設定 （95 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 （98 ページ）を参照してください。

ステップ 10 Assurance アプリケーションの使用を開始します。

デバイスの検出

Catalyst Center ディスカバリ機能を使用してネットワーク内のデバイスをスキャンします。

検出の概要

検出メソッドは、次の機能を提供するネットワーク検出技術です。

- 複数のプロトコルまたは IP 範囲を使用してネットワーク内のデバイスをスキャンします。
- 検出されたデバイスのリストを管理用にインベントリに送信します。
- デバイスの可制御性と連携して、デバイスでネットワーク設定が欠落している場合に自動的にネットワーク設定を構成します。

デバイスは次の 4 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範囲には最大 4,096 台のデバイスを含めることができます。
- Link Layer Discovery Protocol（LLDP）を使用し、シード IP アドレスを指定します。
- Classless Inter-Domain Routing（CIDR）を使用し、シード IP アドレスを指定します。

検出基準を設定する場合、設定を使用して、デバイスの検出に必要な時間を短縮できます。

- [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。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します。
- [**Prefix Length**]：検出方法として [**CIDR**] を使用する場合は、20 ～ 30 の範囲でプレフィックス長の値を設定できます。デフォルト値は 30 です。
- [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、CIDR、または IP アドレスの範囲のいずれを使用する場合でも、Catalyst 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 Catalyst Assurance については、デバイスのループバックアドレスを指定します。

どの方式を使用する場合でも、Catalyst 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 Catalyst 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、Catalyst 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。

- Catalyst Center によって検出されるデバイスの情報を把握するために、*Cisco Catalyst Center Compatibility Matrix* を参照してください。
- Catalyst Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間（RTT）であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。

- Catalyst 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、この設定は SNMPv2C 読み取りクレデンシャルにできます。
- Catalyst Center がデバイスを検出して管理できるようにするには、デバイスで SSH ログイン情報を設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Catalyst 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 Catalyst 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、検出設定のガイドラインと制限事項 （19 ページ）を参照してください。
- デュアルスタック IPv4/IPv6 環境では、次の点に注意してください。
  - 単一の検出セッション中、デバイスが IPv4 と IPv6 の両方を介して到達可能である場合、Catalyst Center は検出された最初のアドレスファミリのみを保持します。デバイスエントリの重複を防ぐため、 Catalyst Center はセカンダリアドレスファミリを無視します。
  - サイトベースのロールベースアクセス制御（SRBAC）の場合、検出はサイトアクセスグループによって制限されます。あるサイトアクセスグループですでに検出されたデバイスは、別のサイトアクセスグループで再検出または管理できません。
  - ループバックオプションを有効にすると、システムのデフォルト設定は IPv6 になります。IPv6 ループバックを使用できない場合、システムは自動的に IPv4 にフォールバックします。
  - Catalyst Center は、クロスファミリネイバー探索をサポートしています。IPv4 でシードされた検出セッションは IPv6 のネイバーを特定でき、IPv6 でシードされたセッションは、CDP または LLDP を介して IPv4 のネイバーを特定できます。

優先管理 IP アドレス

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

優先管理 IP アドレスとして [Use Loopback IP] を選択した場合、Catalyst Center では次の表で詳しく説明されているように優先管理 IP アドレスが指定されます。

表 *2 :* 優先管理 *IP* アドレスの決定基準

条件	解決策
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	Catalyst 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	Catalyst 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	Catalyst 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）。また、最上位の IP アドレスを持つループバック インターフェイスも使用します。
イーサネット インターフェイスがない場合	Catalyst Center は最上位の IP アドレスを持つシリアルインターフェイスを使用します。

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

検出設定のガイドラインと制限事項

ここでは、デバイス検出の制限事項とガイドラインについて説明します。

- Catalyst 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。これらのログイン情報は、ディスカバリ機能に関して Catalyst Center で設定する CLI ユーザー名およびパスワードと同じです。Catalyst 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、Catalyst 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。
- Catalyst Center が ワイヤレスコントローラ と AP を検出する際のガイドラインと制限事項は次のとおりです。

- シスコ 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 のウィンドウでは、データが表示されません。
- ワイヤレスコントローラ が検出されると、Catalyst Center にインベントリ内の関連付けられた AP のリストが表示されます。リストされた AP は、検出中またはインベントリ同期を通じて ワイヤレスコントローラ に接続されます。

（注） インベントリの同期後に ワイヤレスコントローラ に参加する新しい AP の場合：

- ワイヤレスコントローラがサイトに割り当てられていない場合、またはCatalyst Centerでプロビジョニングされていない場合は、手動で再同期を実行する必要があります。
- ワイヤレスコントローラ がサイトに割り当てられている場合、新しい AP が ワイヤレスコントローラに参加すると、SNMP トラップがトリガーされます。この SNMP トラップを使用して、Catalyst Center は新しく参加した AP を検出します。手動での再同期は必要ありません。
- ワイヤレスコントローラ がサイトに割り当てられている場合、[Device Controllability] を有効にする必要があります。サイトの割り当て中に [Device Controllability] を無効にして、後で有効にした場合は、新しい AP を手動で同期する必要があります。

- サードパーティ製デバイスは、Catalyst Center 検出機能では検出できません。サードパーティ製デバイスはネットワークに手動で追加する必要があります。詳細については、*Cisco Catalyst Center User Guide*の「Add a Third-Party Device」を参照してください。

ディスカバリクレデンシャル

ディスカバリクレデンシャルは、検出するデバイスに関するCLI、SNMPv2c、SNMPv3、HTTP、HTTPS、およびNETCONF設定値です。検出を試みるデバイスの種類に基づいてクレデンシャルを指定する必要があります。

- ネットワークデバイス：CLI と SNMP のクレデンシャル。

（注） 組み込みワイヤレスコントローラなどの NETCONF 対応デバイスについては、管理者権限で SSH クレデンシャルを指定し、NETCONF ポートを選択する必要があります。

- コンピューティングデバイス（NFVIS）：CLI、SNMP、HTTP、HTTPS のクレデンシャル。

ネットワーク内のさまざまなデバイスが異なるクレデンシャルセットを持つことが可能であるため、Catalyst Center で複数のクレデンシャル セットを設定できます。ディスカバリプロセスでは、デバイスに使用できるクレデンシャルセットが見つかるまで、ディスカバリジョブ用に設定されているすべてのセットで反復処理されます。

ネットワーク内の大半のデバイスに同じクレデンシャル値を使用する場合は、それらを設定して保存し、複数のディスカバリ ジョブで再利用できます。固有のクレデンシャルを使用するデバイスを検出するために、ディスカバリ ジョブの実行時にジョブ固有のディスカバリ クレデンシャルを追加できます。クレデンシャルタイプごとに最大 10 のグローバルクレデンシャルを設定し、そのうちの5つを定義できます。ジョブ固有のログイン情報を定義する必要がある場合は、ログイン情報の種類ごとに 5 つのグローバルログイン情報と 1 つのジョブ固有のログイン情報を定義できます。

ディスカバリクレデンシャルを定義するには、メニューアイコンをクリックして次を選択します。**[Tools]** > **[Discovery]** > **[Add Discovery]**の順にクリックします。続行するには、次の手順とディスカバリクレデンシャル情報を使用します。

- CDP を使用したネットワークの検出 （26 ページ）
- IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）
- LLDP を使用したネットワークの検出 （32 ページ）

表 *3 : CLI* クレデンシャル

フィールド	説明
Name/Description	CLIクレデンシャルを説明する名前または語句。 CLI の認証が失敗した場合、Catalyst Center は、認証プロセスを 300 秒（5 分）間再試行します。
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
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、この設定では非表示になります。

表 *4 : SNMPv2c* 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、この設定では非表示になります。
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、この設定では非表示になります。

表 *5 : SNMPv3* クレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。

フィールド	説明
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] 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。 • [SHA256]：HMAC-SHA256 に基づく認証。 • [MD5 (not recommended)]：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Catalyst 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、この設定では非表示になります。
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のプライバシータイプのいずれかを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。
Privacy Password	暗号化の標準規格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Catalyst 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、この設定では非表示になります。

表 *6 : SNMP* のプロパティ

フィールド	説明
Retries	Catalyst Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
[Timeout (in Seconds)]	再試行の時間間隔（秒単位）。

表 *7 : HTTP* および *HTTPS* クレデンシャル

フィールド	説明
Type	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明です。 • [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。以下の文字から少なくとも 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（: # _ * ?）– （注） 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（?）を使用できません。

フィールド	説明
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明です。 • [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。以下の文字から少なくとも 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（: # _ * ?）– （注） 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（?）を使用できません。

表 *8 : NETCONF* 設定

フィールド	説明
Port	デバイスのポート。次のいずれかのポートを使用できます。 • ポート 830（デフォルト） • デバイスで使用可能なその他のポート • Catalyst Center で構成するカスタムポート。（デバイス可制御性が有効になっている場合にのみ、カスタムポートを使用できます詳細については、*Cisco Catalyst Center Administrator Guide* の「Device Controllability」の項を参照してください NETCONF の認証に失敗した場合、Catalyst Center は認証プロセスを 300 秒（5 分）間再試行します。

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、CIDR または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。ディスカバリ メソッドの詳細については、IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）およびLLDP を使用したネットワークの検出 （32 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 （17 ページ）で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。（ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザデバイスです。）

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Discover Devices] ウィンドウで、次のフィールドに入力します。

a) 検出ジョブの名前を入力します。

b) [Discovery Type] で、[CDP] を選択します。

c) [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、Catalyst Centerでディスカバリ スキャンを開始します。

d) （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、20 ～ 32 の値です。

e) をクリックします。

手順 d および e 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。

f) （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。

g) [Preferred Management IP] 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
なし（**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） [Use Loopback IP] 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、Catalyst Center は「優先管理 IP アドレス （18 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Catalyst Centerから到達可能であることを確認します。

ステップ 4 [Provide Credentials] ウィンドウで、必要に応じてディスカバリ クレデンシャルとその他の設定を行います。

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （20 ページ）を参照してください。

a) 左側のペインで、[CLI] をクリックして CLI ログイン情報を追加します。

b) [SNMP] を展開して、SNMP ログイン情報を追加します。

c) [Advanced Settings] を展開し、次の設定を行います。

設定	タスク
Protocol Order	[SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。

設定	タスク
SNMP Polling Properties	**[Network Settings]** > **[Device Credentials]** ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

（注） 必要に応じて、NETCONF、HTTP、HTTPS などの他のログイン情報を設定できます。

ステップ 5 [Schedule Job] ウィンドウで、次の手順を実行します。

a) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

b) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。

c) [Assign devices to an existing site] リンクをクリックします。

[設定の可視性と制御（Visibility and Control of Configurations）] ダイアログボックスが表示され、サイトの割り当て時にデバイスで有効になる設定に関する情報が示されます。[設定の可視性（Visibility of Configurations）] が有効であり、検出中にサイトが割り当てられている場合、設定のプレビューは生成されません。

検出ワークフローの間、デバイスは既存のサイトにのみ割り当てることができ、新しいサイトの作成はサポートされません。

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 [Start Discovery] をクリックします。

[Activities] > **[Tasks]** ウィンドウでタスクのステータスを確認できます。

次のタスク

[Device Discovery] ウィンドウに、サイト割り当てに基づいて検出されたデバイスを表示するオプションが表示されます。このオプションを使用して、サイトまたはネットワークに割り当てられたデバイス、またはインベントリ内の未割り当てのデバイスを表示します。

IP アドレス範囲または CIDR を使用したネットワークの検出

IP アドレス範囲、CIDR、CDP、または LLDP を使用してデバイスとホストを検出できます。この手順では、IP アドレス範囲または CIDR を使用して検出を実行する方法について説明します。その他の検出方法の詳細については、「CDP を使用したネットワークの検出 （26 ページ）」および「LLDP を使用したネットワークの検出 （32 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 （17 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。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Discover Devices] ウィンドウで、次のフィールドに入力します。

a) 検出ジョブの名前を入力します。

b) [Discovery Type] で、[IP Address/Range] または [CIDR] を選択します。

c) [IP Address/Range] 検出タイプを選択した場合は、次の手順を実行します。

1. [From] フィールドと [To] フィールドに、スキャンする Catalyst 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。

2. （オプション）追加の IP アドレス範囲を入力するには、前のステップを繰り返します。

d) [CIDR] 検出タイプを選択した場合は、次の手順を実行します。

1. [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、Catalyst Center でディスカバリ スキャンを開始します。

2. [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、20 ～ 32 の値です。

3. ⊕ をクリックします。

   （オプション）検出ジョブから追加のサブネットを除外するには、前のステップを繰り返します。

4. [Prefix Length] フィールドに、20 ～ 30 の値を入力します。

e) [Preferred Management IP Address] 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） [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、Catalyst Centerは優先管理 IP アドレス （18 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 [Provide Credentials] ウィンドウで、必要に応じてディスカバリ クレデンシャルとその他の設定を行います。

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （20 ページ）を参照してください。

a) 左側のペインで、[CLI] をクリックして CLI ログイン情報を追加します。
b) [SNMP] を展開して、SNMP ログイン情報を追加します。
c) [Advanced Settings] を展開し、次の設定を行います。

設定	タスク
Protocol Order	[SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。
SNMP Polling Properties	**[Network Settings]** > **[Device Credentials]** ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

（注） 必要に応じて、NETCONF、HTTP、HTTPS などの他のログイン情報を設定できます。

ステップ 5 [Schedule Job] ウィンドウで、次の手順を実行します。

a) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

b) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。

c) [Assign devices to an existing site] リンクをクリックします。

[設定の可視性と制御（Visibility and Control of Configurations）] ダイアログボックスが表示され、サイトの割り当て時にデバイスで有効になる設定に関する情報が示されます。[設定の可視性（Visibility of Configurations）]が有効であり、検出中にサイトが割り当てられている場合、設定のプレビューは生成されません。

検出ワークフローの間、デバイスは既存のサイトにのみ割り当てることができ、新しいサイトの作成はサポートされません。

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 [Start Discovery] をクリックします。

タスクのステータスは**[Activities]** > **[Tasks]**ウィンドウに表示されます。

次のタスク

[Device Discovery] ウィンドウに、サイト割り当てに基づいて検出されたデバイスを表示するオプションが表示されます。このオプションを使用して、サイトまたはネットワークに割り当てられたデバイス、またはインベントリ内の未割り当てのデバイスを表示します。

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol（LLDP）、CDP、CIDR、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説明します。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（26 ページ）およびIP アドレス範囲または CIDR を使用したネットワークの検出（29 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。
- ホストの検出に CLI ログイン情報は必要ありません。システムは、接続されているネットワークデバイスを使用してホストを検出します。

始める前に

- ネットワークデバイスで LLDP プロトコルを有効にします。
- ディスカバリの前提条件 （17 ページ） に従って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 IP アドレスを設定します。ホストは、ラップトップコンピュータまたはモバイルデバイスなどのエンドユーザーデバイスです。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ 3 [Discover Devices] ウィンドウで、次のフィールドに入力します。

a) 検出ジョブの名前を入力します。

b) [Discovery Type] で、[LLDP] を選択します。

c) [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、Catalyst Centerでディスカバリ スキャンを開始します。

d) （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。

アドレスを、個別の IP アドレス（*x.x.x.x*）またはクラスレス インタードメイン ルーティング（CIDR）アドレス（*x.x.x.x/y*）として入力します。CIDR アドレスでは、*x.x.x.x* は IP アドレスを、*y* はサブネットマスクを示します。サブネットマスクは、20 ～ 32 ビットの値です。

e) をクリックします。

手順 c と手順 d の両方を繰り返して、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。

f) （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。

g) [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。
- [ローカル IP を使用（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、Catalyst Center は「優先管理 IP アドレス （18 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 Catalyst Center から到達可能であることを確認します。

ステップ 4 [Provide Credentials] ウィンドウで、必要に応じてディスカバリ クレデンシャルとその他の設定を行います。

少なくとも 1 つの CLI ログイン情報と 1 つの SNMP ログイン情報を入力します。このログイン情報は、Catalyst Center によって検出されたデバイスに対して構成されます。最大 5 つのグローバルログイン情報、およびタイプごとに 1 つのタスク固有のログイン情報を使用できます。詳細については、ディスカバリ クレデンシャル （20 ページ）を参照してください。

a) 左側のペインで、[CLI] をクリックして CLI ログイン情報を追加します。
b) [SNMP] を展開して、SNMP ログイン情報を追加します。
c) [Advanced Settings] を展開し、次の設定を行います。

設定	タスク
Protocol Order	[SSH] または [Telnet] を選択します。両方を選択した場合は、プロトコルを上下にドラッグして、使用する順序を指定できます。

設定	タスク
SNMP Polling Properties	**[Network Settings]** > **[Device Credentials]** ウィンドウで定義されたグローバル SNMP ポーリングプロパティを使用するか、この検出インスタンス用に変更します。

（注） 必要に応じて、NETCONF、HTTP、HTTPS などの他のログイン情報を設定できます。

ステップ 5 [Schedule Job] ウィンドウで、次の手順を実行します。

a) [Now] をクリックしてデバイスの検出をすぐに開始するか、[Later] をクリックしてデバイスの検出を特定の時間にスケジュールします。

[Daily] または [Weekly] の繰り返しオプションを選択すると、[Discover new devices only] オプションは無効になります。

b) トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にします。

c) [Assign devices to an existing site] リンクをクリックします。

[設定の可視性と制御（Visibility and Control of Configurations）] ダイアログボックスが表示され、サイトの割り当て時にデバイスで有効になる設定に関する情報が示されます。[設定の可視性（Visibility of Configurations）] が有効であり、検出中にサイトが割り当てられている場合、設定のプレビューは生成されません。

検出ワークフローの間、デバイスは既存のサイトにのみ割り当てることができ、新しいサイトの作成はサポートされません。

ダイアログボックスで、次のオプションのいずれかを選択します。

オプション	タスク
Assign to site without Configuration Preview	[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。詳細については、ネットワーク階層の検索を参照してください。
Skip site assignment for now	後でデバイスをインベントリからサイトに割り当てる場合は、このオプションを使用します。

ステップ 6 [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

ステップ 7 [Start Discovery] をクリックします。

[Activities] > **[Tasks]** ウィンドウでタスクのステータスを確認できます。

次のタスク

[Device Discovery] ウィンドウに、サイト割り当てに基づいて検出されたデバイスを表示するオプションが表示されます。このオプションを使用して、サイトまたはネットワークに割り当てられたデバイス、またはインベントリ内の未割り当てのデバイスを表示します。

ディスカバリジョブの管理

ここでは、ディスカバリジョブの管理方法について説明します。

ディスカバリ ジョブの停止および開始

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

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、[**Actions**] 列の省略記号アイコン（ *** ）にカーソルを合わせ、[**Stop Discovery**] を選択します。

ステップ 3 非アクティブなディスカバリジョブを再開するには、[**Actions**] 列の省略記号アイコンにカーソルを合わせ、[**Re-discover**] を選択します。

ディスカバリジョブの複製

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

始める前に

少なくとも 1 つのディスカバリジョブを実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 ディスカバリジョブをコピーするには、[**Actions**] 列の省略記号アイコン（ *** ）にカーソルを合わせて、[**Copy & Edit**] を選択します。

Catalyst Center では、「Clone 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 3 （任意） ディスカバリジョブの名前を変更するには、[Discovery Name] フィールドのデフォルト名を新しい名前に置き換えます。

ステップ 4 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。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 ディスカバリ ジョブを削除するには、[**Actions**]列の省略記号アイコン（ ••• ）にカーソルを合わせ、[**Delete**]を選択します。

ステップ 3 [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。

手順

ステップ 1 メインメニューから次を選択します。**[Tools]** > **[Discovery]**。

ステップ 2 [Discovery] ウィンドウで、[All discoveries page from previous release] をクリックします。

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

ステップ 4 次のいずれかのエリアの横にある下矢印をクリックすると、詳細が表示されます。

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

  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

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。

ネットワーク階層の構造

ネットワーク階層はサイトで構成されます。サイトは、エリア、ビルディング、フロア、または屋外エリアを指している場合があります。各サイトの配置は、ネットワーク階層ルールによって異なります。ネットワーク階層内のサイトを構造化する方法については、図と表を参照してください。

図 *5:* ネットワーク階層

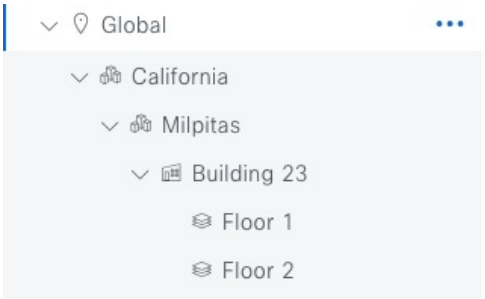


表 *9:* ネットワーク階層の要素

サイトタイプ	説明	ルール
Global（ ）	他のすべてのサイト要素が存在するデフォルトのサイト要素。	[Global] の下に直接配置できるのはエリアとビルディングのみです。
Areas（ ）	エリアは、地理的なリージョンを識別します。他のエリア、建物、またはその両方をグループ化します。そのため、物理アドレスはありません。	エリアは、[Global] または他のエリアの下に直接配置できます。

サイトタイプ	説明	ルール
Buildings（  ）	ビルディングでは物理アドレスまたは緯度と経度の座標を設定できます。	ビルディングは、[Global] またはエリアの下に直接配置できます。エリアを含めることはできませんが、フロアまたは屋外エリアを含めることはできます。
屋外エリア（  ）	屋外エリアは、住所または緯度経度座標を使用して、イメージマップありまたはなしで追加できます。	屋外エリアは、[グローバル（Global）] またはエリアやビルディングの下に配置できます。マップありまたはマップなしで追加できます。マップを使用する場合は、手動で作成するか、DXF、DWG、JPG、GIF、PNG、または PDF などのファイル形式のファイルからインポートできます。次に、ワイヤレスデバイスをマップに配置して、ワイヤレスネットワークのカバレッジを視覚化できます。 屋外エリアの下にサイト要素を追加したり、既存の屋外エリアをサイト間で移動したりすることはできません。
Floors（  ）	フロアは、壁や窓など、ビルディングのさまざまなコンポーネントを含むバックグラウンドイメージの有無にかかわらず、ビルディングに追加できます。 フロアマップでは、フロアマップ上のワイヤレスデバイスの位置に基づいて、ワイヤレスネットワークのカバレッジを可視化できます。フロアマップを手動で作成するか、DXF、DWG、JPG、GIF、PNG、または PDF などのファイル形式のバックグラウンドイメージから追加できます。	ビルディングの下に配置されているフロアのみ。 （注） • 既存のフロアを別の建物に移動することはできません。 • プロビジョニングされていないデバイスのサイト階層は、フロアマップ上の AP の場所を維持したまま変更できます。

サイトにデザインの設定を適用する

ネットワーク階層を使用すると、特定のサイトにデザインの設定を適用できます。たとえば、デザインの設定をエリア全体に適用したり、1 つのフロアに適用したりできます。

ヒント　階層のサイトに名前を付けると、後でデザインの設定を適用する場所を識別するのに役立ちます。

ネットワーク階層の構築

開始するには、次のいずれかの方法を使用してネットワーク階層を構築します。

- ネットワーク階層を作成します。詳細については、ネットワーク階層の作成 （39ページ）を参照してください。
- Cisco Prime Infrastructure または Ekahau Pro から既存のネットワーク階層をインポートする。詳細については、「既存のシスコのネットワーク階層 （44 ページ）」または「既存の Ekahau ネットワーク階層の使用 （48 ページ）」を参照してください。

ネットワーク階層の作成

新しいエリア、ビルディング、およびフロアを作成して、ネットワーク階層を作成します。

サイトの作成、編集、削除

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

手順

ステップ 1　メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

世界地図が右側のペインに表示されます。

ステップ 2　このウィンドウから、サイトを追加、編集、および削除できます。詳細については、次の表を参照してください。

アクション	手順
サイトを追加します。	**1.** マップツールバーから、**[+ Add Site]** > **[Add Area]** をクリックします。 または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Area] を選択することもできます。 **2.** [Area Name] フィールドに、サイト名を入力します。 [Area Name] フィールドには、次のような制限があります。 • エリア名は 40 文字までです。 • 特殊文字（& > < ? ' " / [ ]）は使用できません。 **3.** [Parent] ドロップダウンリストから、親ノードを選択します。[Global] がデフォルトの親ノードです。 **4.** [Add]をクリックします。
サイトを編集します。	**1.** 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Edit Area] を選択します。 **2.** [Edit Area] ダイアログボックスで、必要な編集を行います。 **3.** [更新（Update）] をクリックします。
サイトを削除する。	**1.** 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Delete Area] を選択します。 **2.** [OK] をクリックします。

（注） ネットワーク階層を作成した後は、次の場合にのみ、異なる親サイト間でサイトを移動できます。

- 新しい親サイトは、現在の親サイトと同じネットワーク設定になります。
- 新しい親サイトには、移動先のサイトと同じネットワークプロファイルが割り当てられます。

ビルディングの追加、編集、および削除

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 このウィンドウから、ビルディングを追加、編集、および削除できます。詳細については、次の表を参照してください。

アクション	手順
ビルディングを追加します。	**1.** [Network Hierarchy] ウィンドウで、**[+Add Site]** > **[Add Building]** をクリックします。 または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせ、[Add Building] を選択することもできます。 **2.** [Add Building] ダイアログボックスでビルディングの詳細を追加します。 [Building Name] フィールドには、次のような制限があります。 • 建物名は 40 文字までです。 • 特殊文字（& > < ? ' " / [ ]）は使用できません。 フィールドに住所を入力するか、マップをクリックできます。住所を追加すると、[Longitude] および [Latitude] の座標フィールドが自動的に設定されます。この座標はビルディングの北西角を意味し、Catalyst Center と統合されている場合は、Cisco Spaces や Cisco Connected Mobile Experiences（CMX） などのロケーションサービスで使用されます。 **3.** [Add]をクリックします。
ビルディングを編集します。	**1.** 左側のペインで、サイトの横にある省略記号 ••• にカーソルを合わせて、[Edit Building] を選択します。 **2.** [Edit Building] ダイアログボックスで、必要な編集を行います。 **3.** [更新（Update）] をクリックします。
ビルディングを削除します。	**1.** 左側のペインで、ビルディングの横にある省略記号 ••• にカーソルを合わせて、[Delete Building] を選択します。 **2.** [OK] をクリックします。

フロアの追加、編集、および削除

ビルディングを追加したら、それにフロアを追加できます。フロアマップのない基本フロアを追加してフロアマップを後から追加することも、フロアを追加すると同時にフロアマップを含めることもできます。

建物に基本フロアを追加するには、次の手順を使用します。

フロアとフロアマップを同時に追加するには、*Cisco Catalyst Center User Guide* を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[Design]** > **[Network Hierarchy]**。

ステップ 2 このウィンドウから、フロアを追加、編集、および削除できます。詳細については、次の表を参照してください。

アクション	手順
基本フロアの追加	1. 左側のペインで、建物の横にある省略記号 ••• にカーソルを合わせ、[**Add Floor**] を選択します。 2. [Floor Name] フィールドにフロアの名前を入力します。 [**Floor Name**] フィールドには次のような制限があります。 • フロア名は 40 文字までです。 • 特殊文字（& > < ? ' " / [ ]）は使用できません。 3. [Global Unit System] エリアで、[Feet] または [Meters] を選択します。 フロアが追加されると、すべてのサイトの全フロアが同期され、選択した単位系ですべての測定値が表示されます。グローバル単位系を更新するには、*Cisco Catalyst Center User Guide* の「2D Map View Options」を参照してください。 4. ワイヤレスデバイスがある場合は、[**Type (RF Model)**] ドロップダウンリストで、フロアに適用する RF モデルを選択します。 RF モデルにより、カバレッジエリア内の RF 信号の相対強度を示す 2D および 3D ヒートマップを計算するときの RF の計算方法が決まります。 5. [Floor Number]、[Floor Type]、および [Thickness] フィールドを設定します。 フロアのタイプと厚さは、ワイヤレスデバイスのヒートマップを計算するときに使用されます。 6. [Floor Image]エリアでのフロアマップイメージのアップロードをスキップします。 7. [Width]、[Length]、および [Height] フィールドでマップの寸法を設定します。 8. [Add]をクリックします。
フロアの編集	1. 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせ、[**Edit Floor**] を選択します。 2. [Edit Floor] ダイアログボックスで、必要な変更を行います。 3. [更新（Update）] をクリックして変更を保存します。
フロアの削除	1. 左側のペインで、そのフロアの横にある省略記号 ••• にカーソルを合わせ、[**Delete Floor**] を選択します。 2. [OK] をクリックします。

既存のシスコのネットワーク階層

既存のシスコのネットワーク階層は、Cisco Prime Infrastructure からエクスポートして Catalyst Center にインポートし、サイト階層とマップのデータを保存するために使用できるサイト構造です。

Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、エクスポートしてから Catalyst Center にインポートすることで、新しいネットワーク階層の作成に費やす時間と労力を削減できます。

次の情報を使用して、ネットワーク階層を再作成できます。

- [サイト階層（Site Hierarchy）]：既存のサイト階層が CSV ファイル形式でダウンロードされます。CSV ファイルには、サイト名、親階層、フロア数、場所、サイトアドレスなどの詳細が含まれています。
- [マップアーカイブ（Map Archive）]：マップ情報が TAR ファイル形式のマップアーカイブとしてダウンロードされます。マップアーカイブファイルには、日時、フロアの数、AP などのデータが格納されます。ダウンロードするものに応じて、マップアーカイブには、フロアの寸法（長さ、幅、高さ）や、フロアマップに配置されている AP およびオーバーレイオブジェクトに関する詳細などのマップ情報も含めることができます。各フロアに適用されている RF 減衰モデルなどのキャリブレーション情報をダウンロードすることもできます。

  マップアーカイブは、グローバル階層ベースか、単一のサイト、建物、またはフロアベースにできます。

  - [Site]：選択したサイトとそのすべてのサブサイト、建物、およびフロアがエクスポートされます。
  - [Building]：選択した建物とそのすべてのフロアがエクスポートされます。
  - [Floor]：選択したフロアがエクスポートされます。

（注） Catalyst Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Catalyst Center イメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

FIPS モードは、マップアーカイブのエクスポートとインポートに影響します。

FIPS モードが有効な場合：

- エクスポートされるマップアーカイブは暗号化されません。
- 暗号化されていないマップアーカイブのみをインポートできます。

FIPS モードが無効な場合：

- エクスポートされるマップアーカイブは暗号化されます。
- 暗号化されたマップアーカイブと暗号化されていないマップアーカイブの両方をインポートできます。

詳細については、「*Cisco Catalyst Center User Guide*」を参照してください。

Cisco Prime Infrastructure からのサイト階層のエクスポート

Cisco Prime Infrastructure からサイト階層を CSV ファイル形式でエクスポートできます。CSV ファイルには、サイト名、親階層、フロア数、場所、サイトアドレスなどの詳細が含まれています。

サイト階層のエクスポートは Cisco Prime Infrastructure リリース 3.2 以降でサポートされます。

手順

ステップ 1 Cisco Prime Infrastructure で、**[Inventory]** > **[Group Management]** > **[Network Device Groups]** の順に選択します。

ステップ 2 [Device Groups] ウィンドウで、[Export Groups] をクリックします。

ステップ 3 [Export Groups] ダイアログボックスで、[APIC-EM] オプションボタンをクリックします。

ステップ 4 CSV ファイルをダウンロードするには、[OK] をクリックします。

Cisco Prime Infrastructure からの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て Catalyst Center にインポートするには、次の手順を実行します。マップアーカイブには、フロア寸法などのマップ情報と Cisco Prime Infrastructure の各フロアに適用されている無線周波数（RF）減衰モデルなどのキャリブレーション情報が含まれています。

手順

ステップ 1 Cisco Prime Infrastructure GUI から、**[Maps]** > **[Wireless Maps]** > **[Site Maps (New)]** の順に選択します。

ステップ 2 [**Export**] ドロップダウンリストで [**Map Archive**] を選択します。

[Export Map Archive] ウィンドウが開き、デフォルトで [Select Sites] ウィンドウが開きます。

ステップ 3 エクスポートする特定のサイト、キャンパス、ビルディング、またはフロアの横にある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場合は、[Select All] チェックボックスをオンにします。

ステップ 4 次のオプションのうち 1 つ以上を選択します。

- [Map Information]：[On] をクリックして、フロアの寸法（長さ、幅、高さ）と、フロアマップに配置された AP およびオーバーレイオブジェクトに関する詳細をエクスポートします。
- [Calibration Information]：[On] をクリックして、各フロアに適用されている RF 減衰モデルをエクスポートします。既存のキャリブレーションデータを Cisco Prime Infrastructure からエクスポートすることをお勧めします。それ以外の場合は、キャリブレーションの詳細を手動で再入力する必要があります。

  キャリブレーション情報を含める場合は、選択したマップの情報を含めるのか、すべての情報を含めるのかを指定する必要もあります。

  - [Calibration Information for selected maps]：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。
  - [All Calibration Information]：選択したマップに加えて、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。

ステップ 5 [マップアーカイブを生成（Generate Map Archive）] をクリックします。

次のメッセージは、操作の進行状況を示しています。

```
Exporting data is in progress
```

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 6 [Done] をクリックします。

Catalyst Center へのサイト階層のインポート

Cisco Prime Infrastructure から CSV ファイルとしてエクスポートしたサイト階層をインポートできます。サイト階層のエクスポートについては、『*Cisco Catalyst Center User Guide*』を参照してください。

始める前に

- Catalyst Center インベントリにシスコ ワイヤレス コントローラおよび AP があることを確認します。ない場合は、[Discovery] 機能を使用して検出します。
- フロアマップ上に AP を追加して配置します。
- Cisco Prime Infrastructure にあるサイトを Catalyst Center で手動作成した場合は、インポートする前にそれらのサイトを Catalyst Center から削除する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

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

ステップ 3 ダイアログボックスで、次のオプションのいずれかを選択します。

- [既存のサイトとマージ（Merge with Existing Sites）]：インポートしたサイト情報を既存のサイト情報と結合します。
- [既存のサイトを上書き（Overwrite Existing Sites）]：Catalyst Center に同じサイトがすでに存在する場合、既存のサイト情報はインポートしたサイト情報で上書きされます。

ステップ 4 ダイアログボックスで、CSV ファイルをダウンロードエリアにドラッグアンドドロップします。

または、[ファイルの選択（Choose a file）] をクリックして CSV ファイルの場所に移動し、[インポート（Import）] をクリックすることもできます。

（注） CSV ファイルがない場合は、[CSV Template] をクリックして、CSV ファイルをダウンロードし、編集してからアップロードできます。

Catalyst Center へのマップアーカイブのインポート

マップアーカイブ TAR ファイルを Catalyst Center にインポートできます。たとえば、Cisco Prime Infrastructure からエクスポートした TAR ファイルをアップロードできます。

（注） Catalyst Center は米国の連邦情報処理標準（FIPS）をサポートしています。FIPS は、Catalyst Centerイメージのインストール時に有効にできるオプションのモードです。デフォルトでは、FIPS モードはディセーブルです。

サイト階層のエクスポートについては、「Cisco Prime Infrastructure からのマップアーカイブのエクスポート （45 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 マップツールバーで **[Import]** をクリックし、**[Import Floor Maps]** を選択します。

ステップ 3 [Import Floor Maps] ダイアログボックスに、マップアーカイブファイルをドラッグアンドドロップします。

ステップ 4 [Import] をクリックします。

マップアーカイブファイルがインポートされます。

既存の Ekahau ネットワーク階層の使用

Ekahau Pro ツールを使用すると、フロアレイアウト、AP の場所、障害物など、企業の完全なネットワーク計画を作成できます。フロアレイアウトを作成したら、シミュレートしたネットワーク計画を Ekahau プロジェクトファイルとしてエクスポートできます。実際のサイト調査データを、Catalyst Center で使用できる形式にエクスポートすることもできます。

Catalyst Center からの Ekahau プロジェクトのエクスポート

事前設定済み作業フロアを拡張するために、Catalyst Center では、Catalyst Center から作業フロアを Ekahau プロジェクトとしてエクスポートし、プロジェクトを Ekahau Pro ツールにインポートできます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

世界地図が右側のペインに表示されます。

ステップ 2 左側のペインで、目的のサイト、建物、またはフロアを選択します。

ステップ 3 完全なネットワークマップを Ekahau プロジェクトとしてエクスポートするには、**[Export]** ドロップダウンリストから **[Export Floor Maps]** を選択します。

サイト、建物、またはフロアマップの Ekahau プロジェクトをエクスポートするには、左側のペインで、サイト、建物、またはフロアの横にある省略記号 ••• にカーソルを合わせて **[Export Floor Maps]** を選択します。

[Export Floor Maps] ダイアログボックスが表示されます。

ステップ 4 [Export Floor Maps] ダイアログボックスで、[Ekahau Project] エクスポート形式を選択します。

ステップ 5 [エクスポート（Export）] をクリックします。

ESX 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 6 ESX ファイルを Ekahau Pro ツールにインポートし、フロアを拡張して、ファイルを保存します。

ステップ 7 Ekahau プロジェクトをサイトの下の Catalyst Center にインポートします。詳細については、Ekahau プロジェクトを Catalyst Center にインポートします。（48 ページ）を参照してください。

Ekahau プロジェクトを Catalyst Center にインポートします。

始める前に

Ekahau Cloud プロジェクトと同期していないローカルの変更（AP や壁の削除など）がプロジェクトにある場合、Ekahau Cloud プロジェクトのインポートが失敗する可能性があります。この状況を回避するには、ローカルの変更を Ekahau Cloud に同期してから、Ekahau Cloud プロジェクトを Catalyst Center にインポートしてください。

Catalyst Center でサポートされる Ekahau のバージョンについては、「Compatibility Matrix」[英語] を参照してください。Ekahau は定期的に新しいバージョンをリリースします。Ekahau 11.0.2 以降のバージョンをインポートする方法については、Ekahau のサポート記事「How to import Ekahau data into the Cisco Catalyst Center」[英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 サイト、ビルディング、フロアなどのネットワーク階層を設計します。

（注） 詳細については、サイトの作成、編集、削除 （39 ページ）、ビルディングの追加、編集、および削除 （41 ページ）、およびフロアの追加、編集、および削除 （42 ページ）を参照してください。

フロアを追加する際には、必ず、Ekahau プロジェクトで指定されたものと同じ名前でフロアを作成してください。

ステップ 3 左側のペインで、Ekahau プロジェクトのインポート先サイトの横にある省略記号 ••• のアイコンにカーソルを合わせ、[**Import Ekahau Project**] を選択します。

[Import Ekahau Project] ダイアログボックスが表示されます。

ステップ 4 [Import Ekahau Project] ダイアログボックスのボックスエリアに ESX ファイルをドラッグアンドドロップするか、または [click to select] リンクをクリックして ESX ファイルを参照します。

（注） 建物をインポートするには、Ekahau プロジェクト内に座標が含まれている必要があります。Ekahau Pro で座標を追加できます。Ekahau プロジェクトのインポートが成功すると、計画された各 AP は、AP 名を使用してインベントリ内の既存の実際の AP にマッピングされます。計画された AP は、フロアマップ上にアイコン [P] とともに表示されます。たとえば、計画済みの AP の名前が SJC01-02-AP-B-1 の場合、インポートプロセスでは同じ名前の実際の AP が検索されます。

ステップ 5 インベントリで AP が見つからず、マッピングが解除されたままの場合、計画された AP はフロア上に保持されます。

不一致の理由を表示するには、フロアマップ上の計画された AP アイコンの上にカーソルを置いて、[Import History] をクリックします。

次の試行は、計画された AP を実際の AP にマッピングするために行われます。

- 新たに検出された AP が計画された AP と一致する場合、計画された AP は検出された実際の AP で置き換えられます。

- 計画された AP のマッピングが解除されたままの場合、計画された AP を実際の AP に手動で置き換えて、失敗の原因を示すことができます。

ステップ 6 実際の AP に計画された AP を手動で割り当てるには、フロアマップ上の計画された AP アイコンの上にカーソルを合わせて、[Assign] > [Assign] > をクリックします。

[Assign Planned APs] パネルが表示されます。

ステップ 7 [Assign Planned APs] パネルで、AP 名、AP タイプ、またはすべての AP によって計画された AP を実際の AP にマッピングします。

ステップ 8 AP 名の横にあるオプションボタンをクリックし、[Assign] をクリックして、計画された AP を手動で割り当てます。

ステップ 9 [Save] をクリックします。

Ekahau サイト調査の Catalyst Center へのインポート

ネットワーク階層を作成するには、Ekahauサイト調査ファイルとAPマッピングファイル（CSV形式）をアップロードします。

Ekahau サイト調査には、フロアマップと、名前とマップ上の位置が分かっている AP のみが含まれます。デフォルトでは、AP モデルが Ekahau サイト調査で設定されていない場合があります。Catalyst Center へのインポートの前提条件は、Ekahau でプロジェクトを開き、Ekahau で許可されているモデル名（たとえば、Catalyst Center 9130 AP の場合は *Cisco C9130i*）を使用して AP モデルを設定することです。

Ekahau サイト調査では各 AP の無線に関する情報が Catalyst Center に提供されないため、AP マッピングファイルは、この情報を Ekahau サイト調査に追加します。AP マッピングファイルには、必要な AP マッピングを AP 名ではなく AP モデルによってのみ提供できるという制限があります。そのため、同じタイプでアンテナ設定が異なる複数の AP がある場合、プロジェクトに含まれるそのタイプのすべての AP に適用できるアンテナ設定は 1 つだけです。

AP マッピングファイルの各 AP について、モデル番号と、その後に各アンテナの設定を定義します。

```
model,antennaName0,antennaAzimuth0,antennaElevation0,antennaName1,antennaAzimuth1,antennaElevation1
```

たとえば、次の AP マッピングファイルでは、2 つのアンテナを持つ Catalyst 9130I の設定が定義されます。

```
AP9130I,Internal-9130-2.4GHz,90d,0d,Internal-9130-5GHz,90d,0d
```

モデル属性は、Catalyst Center GUI の同等の計画済み AP モデルと同じである必要があります（たとえば、Catalyst Center 9130 AP の場合は AP9130I）。同様に、*antennaName* 属性も、Catalyst Center GUI で検出およびサポートされる名前と同じである必要があります。AP に 3 つ以上の無線がある場合は、引き続き *antennaName*、*antennaAzimuth*、および *antennaElevation* パラメータの *n* ベースの番号付けパターンを使用して、そのAPモデルでサポートされているスロット番号ごとに各無線のアンテナ情報を定義できます。

Catalyst Center には、ダウンロードして編集して必要な AP アンテナ情報を定義できる CSV テンプレートファイルが含まれています。

図 *6*：フィールドとデフォルトが含まれた *CSV* テンプレートファイル。

	A	B	C	D	E	F	G	H	I	J
1	model	antennaName0	antennaAzimuth0	antennaElevation0	antennaName1	antennaAzimuth1	antennaElevation1	antennaName2	antennaAzimuth2	antennaElevation2
2	AP2700I	Internal-2700-5GHz	90d	0d	Internal-2700-2.4GHz	90d	0d			
3	AP1850I	Internal-1850-5GHz	90d	0d	Internal-1850-2.4GHz	90d	0d			
4	AP3800E	AIR-ANT2524DB-R-5GHz	179.9543762d	0d	AIR-ANT2524DB-R-2.4GHz	179.9543762d	0d			
5										

AP が Catalyst Center デバイスインベントリにない場合、計画された AP としてインポートされます。ただし、命名規則を使用して、AP をデバイスインベントリに追加するときに、Catalyst Center ではそれを実際の AP に自動的に変換することができます。

命名規則は、AP の後に AP の MAC アドレスの最後の 4 桁が続きます（例：AP-c4:e0）。この情報を使用して、Catalyst Center は提供された数字を AP のイーサネット MAC アドレスまたは無線 MAC アドレスの最後の 4 桁と照合しようとします。この情報がない場合、または一致に失敗した場合は、Catalyst Center は AP 名の照合を試みます。

始める前に

- Ekahau でプロジェクトを開き、Ekahau で許可されているモデル名（たとえば、Catalyst Center 9130 AP の場合は *Cisco C9130i*）を使用して AP モデルを設定します。
- AP マッピングファイル（CSV 形式）を作成して、使用されている各 AP モデルの無線に関する情報を Catalyst Center に提供します。

手順

ステップ 1 メインメニューから次を選択します。[Design] > [Network Hierarchy] の順に選択します。

ステップ 2 [Add Site] > [Add Area] をクリックします。

または、左側のペインで親サイトの横にある省略記号 ••• にカーソルを合わせるか、[**Global**] を選択して、[**Add Area**] を選択することもできます。詳細については、サイトの作成、編集、削除 （39 ページ）を参照してください。

ステップ 3 左側のペインで、作成したサイトの横にある省略記号 ••• アイコンにカーソルを合わせて、[**Import Ekahau Survey**] を選択します。

ステップ 4 [Import Ekahau Survey] ダイアログボックスの [Ekahau Survey] ボックス領域に、Ekahau 調査ファイルをドラッグアンドドロップするか、または [Choose a file] リンクをクリックして ESX ファイルを参照します。

ステップ 5 CSV ファイルを [AP Mapping CSV] ボックス領域にドラッグアンドドロップするか、[Choose a file] をクリックして CSV ファイルを参照します。

（注） CSV ファイルがない場合は、[Download AP Mapping 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、アップロードすることができます。

ステップ 6 [Import] をクリックします。

ファイルが正常にダウンロードされると、成功メッセージが表示されます。

ステップ 7 [View Hierarchy] をクリックし、フロアに移動して、デバイスがインポートされ、適切に配置されていることを確認します。

詳細を表示するには、デバイスにカーソルを合わせます。

2D フロアマップのデバイスとオーバーレイオブジェクトの設定

2D マップで、デバイスを設定し、フロアマップ上にオブジェクトをオーバーレイできます。『Cisco Catalyst Assurance User Guide』[英語] には、2D マップの操作に関する基本的なガイダンスが記載されています。2D マップに加えて、Catalyst Center はより多くの機能を備えた 3D マップをサポートします。2D と 3D の両方のマップ機能の詳細については、『*Cisco Catalyst Center User Guide*』[英語] を参照してください。

デバイス

- [APs]：アクセスポイント（AP）は、無線ネットワークと有線ネットワーク間の接続ポイントとして、またはスタンドアロンの無線ネットワークのセントラルポイントとして機能します。2Dマップでは、APは実際にインストールされているデバイスを表します。Catalyst Center でサポートされる AP の一覧については、「*Cisco Catalyst Center Compatibility Matrix*」[英語] を参照してください。
- [Planned APs]：計画済み AP は、まだインストールされていない AP を表します。計画済みAPをマップ上に配置することで、実際にAPをインストールする前に、ワイヤレスネットワークの RF カバレッジを想定して変更を加えることができます。
- [Sensors]：センサーは、Cisco PnP を使用してブートストラップされる専用の Cisco Aironet 1800S アクティブセンサーです。Assurance サーバーに到達可能かどうかの詳細情報を取得してから、Assurance サーバーと直接通信します。センサーテストに関する情報を含む詳細については、「センサーの管理とセンサー主導のテスト （381 ページ）」[英語] を参照してください。

オーバーレイオブジェクト

- [Coverage Areas]：デフォルトでは、フロアマップの一部として定義されたエリアは、無線カバレッジエリアと見なされます。ただし、長方形以外のビルディングがある場合、またはフロア内で長方形以外または多角形のエリアをマークする場合には、[Coverage Areas] 描画ツールを使用してカバレッジエリアを作成できます。
- [Openings]：吹き抜けはアトリウムとも呼ばれ、ビルディング内のオープンエアーまたは天窓で覆われたエリアです。吹き抜けは複数のフロアに伸びる可能性があり、ワイヤレス信号のカバレッジエリアに影響を与える可能性があります。

- [Location Regions]：ロケーションリージョンは、ロケーションサービス（Cisco CMX または Cisco Spaces）で使用されます。ロケーションリージョンでは、クライアントの配置時に包含エリアまたは除外エリアを定義します。包含エリアは計算に含まれ、除外エリアは計算に含まれません。デフォルトでは、フロアを作成すると、フロア上のリージョン全体が包含リージョンとして定義されます。デフォルトの包含リージョンを手動で編集し、フロアに除外リージョンを設定できます。たとえば、実際のクライアントを配置できない建物内の開口部やアトリウム、大型ラックなどのエリアを除外できます。
- [Walls]：壁は、窓、小部屋、ドアなど、建物の外部または内部の垂直構造を定義します。それぞれ異なる材料で構成され、密度が異なる可能性があるため、RF 信号の減衰とヒートマップの計算に大きな影響を与える可能性があります。たとえば、フロアマップに含める壁の数が多いほど、ヒートマップの計算にかかる時間が長くなります。ただし、フロアマップに多数の壁がある場合でも、ヒートマップの計算に使用される数を調整できます。詳細については、『*Cisco Catalyst Center User Guide*』の「2D Map View Options」および「3D Map View Options」を参照して ください。
- [Shelving Units]：シェルフユニットは、RF 信号の減衰とヒートマップの計算に大きな影響を与える可能性のある障害物です。シェルフユニットがある場所の例としては、天井が高い倉庫などがあります。
- [Markers]：マーカーは、マップ上の場所を示します。マーカーを作成するときは、後で識別しやすいように、マーカーに名前を付けて配置することができます。
- [GPS Markers] ：Catalyst Centerと統合すると、Cisco Spacesや Cisco Connected Mobile Experiences（CMX）などのロケーションサービスは、GPS マーカーを使用してクライアントのおおよその地理的位置を計算します。
- [Align Points]：位置合わせポイントは、物理的な形状が異なる複数のフロアを配置するために使用されるマーカーです。3D マップでは、フロアはマップの左上隅（ポイント 0,0）に配置されます。各フロアを独立して管理する場合、配置のずれは問題になりません。ただし、一部の 3D マップの機能を使用するには、実際のフロアをそのまま配置する必要があります。このずれを補正するために、2 つ以上のフロアに 1 つ以上の位置合わせポイントを挿入して、3D マップ内でフロアを上下に適切に配置できます。

AP の追加、配置、編集、削除

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 左側の階層ツリーで、フロアを選択します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** をクリックします。

デフォルトでは、[Devices] トグルボタンと [Access Points] トグルボタンが選択されています。

ステップ 4 このウィンドウから、AP を追加、配置、編集、および削除できます。詳細については、次の表を参照してください。

アクション	手順
AP の追加	**1.** マップの左側のペインで、[Add Access Points] をクリックします。 **2.** [Add Access Points] スライドインペインにあるテーブルで、次のいずれかを行います。 • **単一の AP を追加するには**：追加する AP を見つけ、右にスクロールして [Add] をクリックします。 • **複数の AP を追加するには**：追加する AP の横にあるチェックボックスをオンにして、[Add Selected] をクリックします。 新しく追加された AP は、マップの左側のペインにある [Unpositioned] カテゴリに表示されます。 **3.** [Unpositioned] カテゴリから、AP をクリックします。 **4.** AP を配置するマップ上の場所をクリックします。 **5.** マップツールバーで [Save] をクリックします。
計画済み AP の追加	**1.** マップの左側のペインにある [Planned AP Models] エリアで、追加する計画済み AP の AP モデルをクリックします。 その AP モデルがリストにない場合は、[Add Model] をクリックして、リストに追加する AP モデルを選択します。 **2.** フロアマップで、計画済み AP を配置する場所をクリックします。 **3.** [Edit Planned AP] スライドインペインで歯車アイコンをクリックし、一意の名前パターンを追加します。 **4.** 必要に応じて、アンテナタイプと方位角と仰角を定義します。 **5.** 引き続き同じプロパティを持つ計画済み AP を追加するには、マップ上の場所をクリックします。 **6.** 計画済み AP の追加を止めるには、**Esc** を押すか、フロアマップを右クリックします。 **7.** マップツールバーで [Save] をクリックします。

アクション	手順
AP の編集	**1.** マップで AP を右クリックして [Edit] を選択します。 **2.** 編集可能な AP 設定を変更します。次のフィールドに関する情報を理解しておきます。 • [Antenna]：外部 AP の場合は、アンテナを選択する必要があります。アンテナを選択しないと、AP がマップに表示されません。 • **Azimuth**：方位角は、x 軸に対して測定されたアンテナの角度です。方位角の範囲は 0 ー 360 です。Catalyst Center では、右向きは 0 度または 360 度で、下向きは 90 度です。 値を手動で入力するか、フィールドの下の青色の矢印を使用して値を変更できます。 無指向性アンテナの場合、仰角が 0 の場合、方位角は関係ありません。 • **Elevation**：仰角（度）を手動で入力するか、フィールドの下の青色の矢印を使用して、値を変更できます。 天井に配置するように設計された AP およびアンテナモデルの場合、仰角が 0 の場合は下を向きます。壁に配置するように設計された AP およびアンテナモデルの場合、仰角を 0 にすると水平方向を向き、負の値の場合は下を向きます。 **3.** マップツールバーで [Save] をクリックします。
AP の削除	**1.** AP をクリックするか、複数の AP を選択する場合は、最初の AP をクリックし、Shift キーを押しながら残りの AP をクリックします。 **2.** [Edit] ペインで、[Remove] をクリックします。 **3.** マップツールバーで [Save] をクリックします。

センサーの追加、配置、削除

始める前に

インベントリに Cisco AP 1800S センサーがあることを確認します。Cisco Aironet 1800s アクティブセンサーをインベントリで表示するには、プラグアンドプレイを使用してプロビジョニングする必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** > **[Sensors]** をクリックします。

ステップ 4 このウィンドウから、センサーを追加、配置、編集、および削除できます。詳細については、次の表を参照してください。

アクション	手順
センサーの追加	1. [Add Sensors] スライドインペインから、追加するセンサーの横にある [Add] をクリックします。または複数のセンサーを追加する場合は、追加するセンサーの横のチェックボックスをオンにして、[Add Selected] をクリックします。 新しく追加されたセンサーは、マップの左ペインの [Unpositioned] カテゴリに表示されます。 2. マップの左ペインの [Unpositioned] カテゴリから、センサーをクリックします。 3. センサーを配置するマップ上の場所をクリックします。 4. [Save] をクリックします。
センサーの削除	1. センサーをクリックします。複数のセンサーを選択する場合は、最初のセンサーをクリックし、Shift キーを押しながら残りのセンサーをクリックします。 2. [Edit] ペインで、[Remove] をクリックします。 3. マップツールバーの [Save] をクリックします。

カバレッジエリアの追加、編集、削除

この手順では、フロアマップで長方形以外または多角形のエリアをカバレッジエリアとしてマークする方法を示します。

カバレッジエリアの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）」[英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Coverage Areas]** をクリックします。

ステップ 4 カバレッジエリアを追加するには、次の手順を実行します。

a) [Coverage Area] ダイアログボックスで、フィールドにカバレッジエリアの名前を入力します。

b) [Add Coverage] をクリックします。

c) マップをクリックしてポイントを作成し、描画ツールを開始します。

d) 引き続きポイントを作成して、カバレッジエリアの形状を定義します。

（注） カバレッジエリアの形状には、少なくとも 3 つのポイントが必要です。ポイントをクリックしてドラッグすると、カバレッジエリアの形状を定義し直すことができます。

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

ステップ 5 カバレッジエリアを編集するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Coverage Areas]** をクリックします。

b) カバレッジエリアの形状を定義し直すには、ポイントをクリックしてドラッグします。

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

ステップ 6 カバレッジエリアを削除するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Coverage Areas]** をクリックします。

b) カバレッジエリアを右クリックし、[**Remove**] を選択します。

ステップ 7 マップツールバーで [Save] をクリックします。

吹き抜けの追加、編集、コピー、および削除

吹き抜けの作成は、フロアでのオープンスペース（アトリウム）の作成と似ています。通常、複数フロアのビルディングでは、吹き抜けは複数のフロアを縦方向に伸びています。この手順では、フロアマップで吹き抜けを追加、編集、および削除する方法を示します。また、吹き抜けを他のフロアにコピーする方法も示します。

吹き抜けの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）」[英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Openings]** をクリックします。

ステップ 4 吹き抜けを追加するには、次の手順を実行します。

a) マップの左ペインで、[Opening] をクリックします。

b) マップをクリックしてポイントを作成し、描画ツールを開始します。

c) 引き続きポイントを作成して、吹き抜けの形状を定義します。

（注） 吹き抜けの形状には、少なくとも 3 つのポイントが必要です。ポイントをクリックしてドラッグすると、吹き抜けの形状を定義し直すことができます。

d) ダブルクリックして描画ツールを終了し、形状を確定します。

ステップ 5 吹き抜けを編集するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜けの形状を定義し直すには、ポイントをクリックしてドラッグします。

c) 吹き抜けを移動するには、網掛けされたエリア内をクリックします。次に、吹き抜けを配置する場所にドラッグアンドドロップします。

ステップ 6 吹き抜けを別のフロアにコピーするには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜けを右クリックし、[**Copy to other floors**] を選択します。

c) ダイアログボックスで、関連フロアの横にあるチェックボックスをオンにします。

d) [Copy] をクリックします。

e) [Close] をクリックします。

ステップ 7 吹き抜けを削除するには、次の手順を実行します。

a) マップツールバーで、**[Add/Edit]** > **[Openings]** をクリックします。

b) 吹き抜けを右クリックし、[**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

ロケーションリージョンの追加、編集、および削除

ロケーションリージョンは、ヒートマップの計算に含まれるまたは計算から除外されるマップ上の領域です。次のトピックで、ロケーションリージョンを追加、編集、および削除する方法を示します。

包含リージョンの追加、編集、および削除

この手順では、包含リージョンを追加、編集、および削除する方法を示します。次のガイドラインを使用して、フロアマップで包含リージョンを定義します。

- 包含リージョン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。

包含リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。

ステップ 4 マップの左側のペインで、[Inclusion] アイコンをクリックします。

ステップ 5 包含リージョンを作成するには、描画ツールを使用します。

a) マップをクリックして、包含リージョンを開始するポイントを作成します。
b) カーソルを次のポイントに移動して、もう一度クリックします。
c) 引き続きポイントを作成して、包含リージョンの形状を定義します。
d) 形状を完成させるには、マップをダブルクリックします。

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 6 包含リージョンの場所を編集するには、その形状を新しい場所にドラッグアンドドロップします。

ステップ 7 包含リージョンを削除するには、形状を右クリックして [**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

除外リージョンの追加、編集、および削除

この手順では、除外リージョンを追加、編集、および削除する方法を示します。次のガイドラインを使用して、フロアマップで除外リージョンを定義します。

- 除外リージョン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。
- 除外リージョンは包含リージョンの境界内で定義されます。
- フロアマップ上で除外リージョンを複数定義できます。

除外リージョンの詳細については、2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Location Regions]** をクリックします。

ステップ 4 マップの左側のペインから、[Exclusion] アイコンをクリックします。

ステップ 5 除外リージョンを作成するには、描画ツールを使用します。

a) マップをクリックして、除外リージョンを開始するポイントを作成します。

b) カーソルを次のポイントに移動して、もう一度クリックします。

c) 引き続きポイントを作成して、除外リージョンの形状を定義します。

d) 形状を完成させるには、マップをダブルクリックします。

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

e) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 6 除外リージョンの場所を編集するには、その形状を新しい場所にドラッグアンドドロップします。

ステップ 7 除外リージョンを削除するには、形状を右クリックして [**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

壁の追加、編集、および削除

この手順では、フロアマップで壁を追加、編集、および削除する方法を示します。

壁がRF信号の減衰とヒートマップの計算に与える影響については、2Dフロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Walls]** をクリックします。

ステップ 4 壁を追加するには、次の手順を実行します。

a) マップの左側のペインで、[Others] または [On this floor] カテゴリの壁のタイプをクリックします。

（注） 壁タイプがリストにない場合は、[Add Wall Type] をクリックしてカスタムの壁タイプを作成します。

b) マップをクリックして、壁の開始ポイントを作成します。
c) 壁を終了する次のポイント、またはコーナーを作成する次のポイントにカーソルを移動して、もう一度クリックします。
d) 引き続きポイントを作成して、壁の形状を定義します。
e) 壁を終了するには、マップをダブルクリックします。

   または、左側のペインで壁のタイプをクリックします。

f) 描画ツールを終了するには、マップをもう一度ダブルクリックします。

ステップ 5 壁のタイプを変更し、壁のタイプに応じてそのパラメータを設定するには、次の手順を実行します。

a) 変更する壁をクリックします。

   [Wall Type] ダイアログボックスが表示されます。

b) [**Wall Type**] ドロップダウンリストから、壁のタイプを選択します。
c) 新しい壁タイプに適したその他のパラメータを設定します。
d) [Update] をクリックします。

ステップ 6 壁を移動するには、次の手順を実行します。

a) 移動する壁にカーソルを合わせます。

   壁が黒くなります。これは選択されたことを意味します。

b) 壁をクリックし、新しい場所にドラッグアンドドロップします。

ステップ 7 壁を削除するには、壁を右クリックして [**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

シェルフユニットの追加、コピー、編集、および削除

この手順では、フロアマップでシェルフユニットを追加、コピー、編集、および削除する方法を示します。

シェルフユニットの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）」[英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Shelving Units]** をクリックします。

ステップ 4 シェルフユニットを追加するには、次の手順を実行します。

a) マップの左ペインで、追加するシェルフタイプをクリックします。

b) シェルフダイアログボックスで、名前、寸法、向き、およびユニットが両面かどうかを構成するか、デフォルト値のままにします。向きとは、シェルフユニットの角度を意味します。向きが 0 のシェルフユニットは、垂直で y 軸に平行であることを意味します。

シェルフタイプがリストにない場合は、[Add Shelving Type] をクリックしてシェルフタイプを作成します。

c) [Add Shellving] をクリックします。

シェルフユニットがマップに表示されます。

d) シェルフユニットをマップ上の場所にドラッグアンドドロップします。

ステップ 5 シェルフユニットのコピーまたはアレイを作成するには、次のいずれかを実行します。

- コピーを作成するには、シェルフユニットを右クリックして [**Clone**] を選択します。
- アレイを作成するには、シェルフユニットを右クリックして [**Array**] を選択します。次に、ユニットの数とそれらの間の距離を指定します。

ステップ 6 名前、寸法、向き、および両面かどうかを編集するには、シェルフユニットを右クリックし、[**Edit**] を選択します。

ステップ 7 シェルフユニットを削除するには、シェルフユニットを右クリックし、[**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

マーカーの追加、編集、および削除

この手順では、マーカーを追加、編集、および削除する方法を示します。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Markers]** をクリックします。

ステップ 4 マップの左側のペインで、[Markers] アイコンをクリックします。

ステップ 5 [Place Markers] ダイアログボックスで、マーカーの名前を入力し [Add] をクリックします。

ステップ 6 マーカーを配置するには、マーカーを配置するマップをクリックします。

ステップ 7 マーカーを移動するには、マーカーが青色に変わるまでカーソルを合わせます。次に、マーカーを新しい場所にドラッグアンドドロップします。

ステップ 8 マーカーを編集するには、マーカーを右クリックして [**Edit**] を選択します。

ステップ 9 マーカーを削除するには、マーカーを右クリックして [**Remove**] を選択します。

ステップ 10 マップツールバーで [Save] をクリックします。

GPS マーカーの追加、編集、および削除

この手順では、GPS マーカーを追加、編集、および削除する方法を示します。GPS マーカーの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）」[英語] を参照してください。

（注） GPS マーカーは建物の属性です。建物のすべてのフロアに適用できます。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[GPS Markers]** をクリックします。

ステップ 4 GPS マーカーを追加するには、次の手順を実行します。

a) マップの左側のペインから、[GPS Markers] アイコンをクリックします。

b) マップ上で、GPS マーカーを配置する場所をクリックします。

GPS マーカーは、外壁の内側、通常は建物の角に配置する必要があります。

c) [Place Markers] ダイアログボックスで、適切なフィールドに名前、緯度、経度、X 座標、および Y 座標を入力します。

フロアの北西角にある GPS マーカーの緯度と経度の座標が、建物の座標と一致する必要があります。

d) [Add] をクリックします。

計算に GPS マーカーを含めるには、少なくとも 3 つの GPS マーカーを追加する必要があります。

ステップ 5 GPS マーカーを編集するには、GPS マーカーを右クリックして [**Edit**] を選択します。

ステップ 6 GPS マーカーを移動するには、マーカーにカーソルを合わせ、オレンジ色に変わるまで待ちます。次に、マーカーを新しい場所にドラッグアンドドロップします。

ステップ 7 GPS マーカーを削除するには、GPS マーカーを右クリックして [**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

位置合わせポイントの追加、編集、および削除

この手順では、位置合わせポイントを追加、編集、および削除する方法を示します。位置合わせポイントの詳細については、「2D フロアマップのデバイスとオーバーレイオブジェクトの設定 （52 ページ）」[英語] を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** > **[Overlays]** > **[Align Points]** をクリックします。

ステップ 4 位置合わせポイントを追加するには、次の手順を実行します。

a) マップの左側のペインで、[Align Points] アイコンをクリックします。

b) マップ上で、位置合わせポイントを配置する場所をクリックします。

ステップ 5 位置合わせポイントの名前を編集するには、次の手順を実行します。

a) 位置合わせポイントを右クリックし、[**Edit**] を選択します。

b) 名前を変更して、[Update] をクリックします。

ステップ 6 位置合わせポイントの位置を変更するには、次の手順を実行します。

- 位置合わせポイントにカーソルを合わせ、青色に変わるまで待ちます。次に、マーカーを新しい場所にドラッグアンドドロップします。
- 位置合わせポイントを右クリックし、[**Edit**] を選択します。[x] 座標と [y] 座標を更新し、[Update] をクリックします。

ステップ 7 位置合わせポイントを削除するには、位置合わせポイントを右クリックして [**Remove**] を選択します。

ステップ 8 マップツールバーで [Save] をクリックします。

インベントリの管理

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

インベントリについて

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

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

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery（このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 （17 ページ） を参照してください。

初期検出後、Catalyst 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 24 時間ごとです。ただし、この間隔は、ネットワーク環境の必要性に応じて変更できます。詳細については、デバイスポーリング間隔の更新 （66 ページ）を参照してください。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。以下の状況下では、インベントリサービスの再起動後にもデバイスの再同期がトリガーされます。

- インベントリサービスの再起動後にアップグレード（Catalyst Center アップグレード）が存在する場合。
- サービスの再起動後にデバイスの同期が終了状態または遅延状態になっている場合。
- デバイスの [Last Sync] 時間が、デバイスに設定されている定期的な再同期間隔の 75% を超えている場合。たとえば、インベントリサービスの再起動後、デバイスの [Last Sync] 時間が 18 時間を超え、設定された定期的な再同期間隔が 24 時間である場合、デバイスは定期的な再同期間隔の前に再同期されます。再同期間隔のカットオフ時間のパーセンテージは、デバイスに設定されている値によって異なる場合があります。

（注） デバイスの再同期に関するポイントは次のとおりです。

- ポートのアップ/ダウンイベントは 80 秒ごとにグループ化されます。結果として、80 秒の時間枠ごとに、各デバイスにつき 1 件のイベントのみが報告されます。このプロセスにより、デバイスのポート関連の一覧データが更新されます。
- 構成変更イベントは 10 分ごとにグループ化され、デバイスの再同期要求をトリガーします。
- ポートのアップ/ダウン トラップまたは設定変更トラップによって 3 回連続して同期が発生すると、そのデバイスの次のイベントベースの同期は 5 分遅延します。
- 統合期間内でイベントバーストのレートが 60% を超えると、そのデバイスの再同期が 45 分遅延します。

デバイスポーリング間隔の更新

[システム（System）] > [設定（Settings）] > [ネットワーク再同期間隔（Network Resync Interval）] の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。特定のデバイスのポーリング間隔を更新するには、[デバイスインベントリ（Device Inventory）]を選択します。[ネットワークの再同期間隔（Network Resync Interval）] を使用して設定した値は、[デバイスインベントリ（Device Inventory）] で設定された値を置き換えます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

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

手順

ステップ 1 メインメニューから次を選択します。**[Provision] > [Inventory]** の順に選択します。

ステップ 2 更新するデバイスを選択します。

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

ステップ 4 [Edit Device] スライドインペイン で、[Resync Interval] をクリックします。

ステップ 5 再同期タイプを選択します。

（注）
- 再同期タイプをグローバルとして設定するには、**[System] > [Settings]**の順に移動します。
- デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Catalyst Center は引き続きデバイス固有のポーリング時間を使用します。

ステップ 6 [Resync Interval (in Mins)] 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。

ステップ 7 [Update] をクリックします。

インベントリに関する情報の表示

インベントリで検出されたデバイスに関する情報を表示およびフィルタリングできます。[Device] テーブルに表示される情報をカスタマイズまたは変更できます。

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。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセスからのデバイス情報が表示されます。

（注） 完全修飾ドメイン名（FQDN）として追加されたデバイスの場合、[IP address] 列のデバイス名の横にある [i] アイコンにマウスのカーソルを合わせると、**解決された IP アドレス**が表示されます。

[Inventory] ウィンドウにライセンス要件を満たしていない AP が含まれている場合、Catalyst Center は詳細を示すダイアログボックスを表示します。このダイアログボックスには、次のオプションがあります。

オプション	タスク
今後はこのダイアログボックスをスキップします。	[Don't show this again] チェックボックスをオンにします。
[License Manager] ウィンドウを開いて、ライセンスを有効にします。	[License Manager] をクリックします（詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください）。
後でライセンスを有効にします。	[Do this later] をクリックします。

ステップ 2 （任意） サイトを変更するには、[Global] をクリックし、検索バーまたはネットワーク階層のいずれかを使用してサイトを見つけます。

選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 （任意） インベントリビューを変更するには、右上隅にあるトグルボタン（ ）を使用します。

既定のビュー（リストレイアウト）を、トポロジやマップレイアウトなどの他のレイアウトに変更できます。

ステップ 4 （任意） [Devices] テーブルのフォーカスビューを変更するには、[Focus] ドロップダウンリストから、[Default]、[Inventory]、または [Software Images] などのビューを選択します。

（注）
- 表示される列は、選択したフォーカスビューに応じて変わります。
- 選択したデバイスは、それぞれの新しいフォーカスビューで保持されます。

ステップ 5 （任意） [Devices] テーブルで特定のデバイスの詳細をフィルタ処理するには、次のフィルタオプションを使用します。

オプション	タスク
デバイスファミリをフィルタ処理する	[Inventory] ウィンドウの上部にある 1 つまたは複数のデバイスファミリボタンを選択します。 たとえば、[Routers] をクリックすると、テーブル内にルーターのみを表示できます。
左ペインでデバイスの作業項目をフィルタ処理する	1 つ以上の作業項目のチェックボックスをオンにします。 テーブルは、作業項目に対してすぐにフィルタ処理されます。たとえば、[Unreachable] チェックボックスをオンにして、到達不能なデバイスのみをテーブルに表示できます。
特定のデバイスの詳細をフィルタ処理する	[Filter devices] をクリックし、フィルタオプション（[Quick Filters]、[Advanced Filters]、[Recent Filters]）から選択します。次に、[Apply] をクリックします。

ステップ 6 （任意） 右上隅にある[Take a tour] をクリックすると、[Inventory] ウィンドウの詳しい説明が見られます。

ステップ 7 （任意） [Devices] テーブルのすべてのデータをエクスポートするには、右上隅の[Export] をクリックします。

ステップ 8 （任意） [Devices] テーブルをカスタマイズするには、右上隅にある設定アイコン（⚙）をクリックし、[Table Settings] スライドインペインで希望するオプションを選択して、[Apply] をクリックします。

オプション	説明
Table Appearance	選択すると、デフォルトまたはコンパクトなテーブルビューとテーブルストライピングが使用されます。
Edit Table Columns	選択するとカスタムビューが作成され、列が非表示または表示されます。

（注） 列の選択はセッション間では保持されません。

このテーブルには、特定のテーブル列に関する重要な情報が表示されます。

カラム	説明
Device Name	デバイスの名前。 デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。 （注） デバイス名が赤色で表示されている場合は、インベントリがデバイスをポーリングしておらず、その情報を 30 分以上更新していません。

カラム	説明
Support Type	デバイスのサポートレベルが表示されます。 • [Supported]：Catalyst Center のすべてのアプリケーションに対してデバイスプロファイルがテスト済みです。これらのデバイスのいずれかの Catalyst 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。 • [Limited]：レガシーデバイス用のデバイスプロファイルは、Catalyst Center の次の機能のみを対象にベストエフォートベースでのみテストされています。 • 検出 • トポロジ • デバイスの到達可能性 • 構成変更監査 • インベントリ • ソフトウェアイメージ管理（ソフトウェアイメージは、cisco.com に記載の EOL デバイスでは利用できない場合があります。EOL デバイスには推奨されません。） • テンプレート プロビジョニング（スイッチにのみ適用されます。） 詳細については、『*Legacy Device Compatibility Matrix*』[英語] を参照してください。 • [サードパーティ（Third Party）]：デバイスプロファイルは、SNMP MIB 2 値を入力できるサードパーティデバイスの Catalyst Center でテストされています。Catalyst Center は、限定的な基本自動化（インベントリとトポロジ）と、サードパーティデバイス 360、到達可能性ステータスに基づくデバイスの正常性計算、デバイスインターフェイスと到達可能性の問題などの限定的なアシュアランス機能をサポートします。 詳細については、*Cisco Catalyst Center Compatibility Matrix*を参照してください。 • [Unsupported]：Catalyst Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Catalyst 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、Catalyst 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やバグを申請することはできません。
Reachability	さまざまなステータスを表示します。 • [Reachable]：Catalyst Center から SNMP、HTTP（S）、および NETCONF ポーリングを使用してデバイスに到達できます。 • [Ping Reachable]：Catalyst Center から ICMP ポーリングを使用してデバイスに到達できます。SNMP、HTTP、HTTPS および NETCONF ポーリングでは到達できません。 • [Unreachable]：SNMP、HTTP、HTTPS、NETCONF、ICMP のいずれのポーリングでもデバイスに到達できません。

カラム	説明
EoX Status	EoX スキャンのステータスが表示されます。 • [Success]：デバイスでの EoX アラートのスキャンに成功しました。 • [Not Scanned]：デバイスは EoX アラートについてスキャンされていません。 • [Scan Failed]：Catalyst Center でデバイスでの EoX アラートのスキャンに失敗しました。 • [Scanning]：Catalyst Center でデバイスでの EoX アラートのスキャンを実行しています。 [EoX Status] の横にある [i] アイコンにカーソルをホバーし、[Consent to Connect] ハイパーリンクをクリックします。EoX スキャンを開始するには、[Consent to Connect] ダイアログボックスで承認を受け入れて送信する必要があります。 正常にスキャンされたデバイスについては、[EoX Status] 列にアラートの数が表示されます（ある場合）。アラートの数をクリックすると、アラートの詳細が表示されます。 スライドインペイン で、[Hardware]、[Software]、および [Module] タブをクリックして、ハードウェア、ソフトウェア、およびモジュールの EoX アラートを表示します。 （注） EoX 機能は、AP での EoX アラートのスキャンはサポートしていません。

カラム	説明
Manageability	デバイスのステータスが示されます。 • [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、NETCONF ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 （注） デバイスの SSH キーの検証に失敗した場合の対処方法については、SSH キー検証エラーへの対処 （76 ページ） を参照してください。 • [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。 （注） デバイスの再同期が進行中の場合は、[Syncing] ステータスが表示されます。ステータスをクリックすると、次が表示されます。 • 進行中の同期の詳細 • 以前の同期の詳細 • 同期の理由 • 同期を要求したアプリケーション。 キューにある保留中の再同期要求については、メッセージが表示されます。複数の要求が保留中の場合は、同期する機能と優先順位に基づいてマージされます。同期の詳細には、同期イベントの理由が複数表示される場合があります。
Platform	シスコ製品の部品番号
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Catalyst 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。Catalyst 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、デバイスロールを更新しません。 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。

カラム	説明
Site	デバイスに割り当てられているサイト。 デバイスがどのサイトにも割り当てられていない場合は、次の手順を実行します。 **1.** [**Assign**] をクリックします。 **2.** [Choose a Site] をクリックします。 **3.** 階層からサイトを選択します。 **4.** [Save] をクリックします。 詳細については、ネットワーク階層 （37 ページ）を参照してください。
Last Updated	Catalyst 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。 （注） [Sync Details] をクリックして、**最後の同期の開始時刻**と**最後の同期の理由**を表示します。 デバイスの再同期が進行中の場合は、[Sync Details] に次が表示されます。 • 進行中の同期の詳細 • 以前の同期の詳細 • 同期の理由 • 同期を要求したアプリケーション。 キューにある保留中の再同期要求については、メッセージが表示されます。複数の要求が保留中の場合は、同期する機能と優先順位に基づいてマージされます。同期の詳細には、同期イベントの理由が複数表示される場合があります。
Resync Interval	デバイスのポーリング間隔。 再同期間隔は、[Inventory] ウィンドウから **[Actions]** > **[Edit Device]** > **[Resync Interval]** の順に選択して設定します。 再同期タイプを [Global] として設定するには、メインメニューから **[System]** > **[Settings]** の順に選択します。詳細については、*Cisco Catalyst Center Administrator Guide*を参照してください。

カラム	説明
Provisioning Status	デバイスで試行された最後のプロビジョニング操作のステータスが示されます。過去のプロビジョニング操作のステータスを確認するには、[See Details] をクリックします。 • [Success]：デバイスでの最近の操作が成功しました。 • [Success] と警告アイコン：デバイスでの最近の操作は成功しましたが、過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Failed]：デバイスでの最近の操作が失敗しました。 • [Failed] と警告アイコン：デバイスでの最近の操作が失敗しました。過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Configuring]：デバイスは現在設定中です。 • [Pending]：システムは、進行中のプロビジョニング操作によってデバイスが影響を受けるかどうかを判断しようとしています。 • [Not Provisioned]：デバイスは一度もプロビジョニングされていません。 • [Out of Sync]：デバイスのネットワーク設定またはネットワークプロファイルが、最後のプロビジョニング操作の後に変更されました。IPv6 デバイスは、[非同期（Out of Sync）] としてマークできます。
Credential Status	デバイスのクレデンシャルステータスが示されます。 • [Not Applied]：デバイスのログイン情報がデバイスに適用されていません。 • [Success]：デバイスのクレデンシャルがデバイスに正常に適用されました。 • [Failed]：デバイスのクレデンシャルがデバイスで失敗しました。 クレデンシャルの詳細を表示するには、[See Details] をクリックします。 [Credential Status] スライドインペインには、クレデンシャルの [Type]、[Name/Description]、[Status]、および [Details] が表示されます。 ステータスが [Failed] のデバイスの場合、[Actions] 列の省略記号アイコン（ *** ）の上にカーソルを置き、[Retry] または [Clear] を選択します。 • [Retry]：デバイスにクレデンシャルを適用します。 • [Clear]：デバイスのクレデンシャルをクリアします。
AP CDP Neighbors	[Inventory] ウィンドウの AP に接続されているスイッチとポートに関する詳細が表示されます。 このウィンドウには、接続されたアクセススイッチが Catalyst Center によって管理されている場合でも、AP CDP ネイバーに関する情報が表示されます。

• [Edit Custom Views] ：最初に、[Edit Table Columns] タブでカスタム ビューを作成する必要があります。それから、カスタムビューを編集できます。

- [Reset All Settings] ：テーブル設定をデフォルト設定にリセットします。

ステップ 9 （任意） [Devices] テーブルからデバイスを管理するには、デバイスにタグを付けるか、デバイスを追加するか、 [Actions] ドロップダウンリストを使用します。

名前	説明
Tag	[タグ（Tag）] をクリックして、デバイスにタグを付けたり、タグを編集および削除したり、ポートグループを作成したりします。
Add Device	[デバイスの追加（Add Device）] をクリックして、ネットワークデバイスを追加するか、コンピューティングデバイスを追加するか、Cisco Meraki ダッシュボードまたは Firepower Management Center（FMC）を Catalyst Center と統合します。
[Actions] ドロップダウン リスト	[Actions] ドロップダウンリストを使用して、デバイス、ソフトウェアイメージ、テレメトリなどを管理します。 各アクションオプションの詳細を表示するには、右隣の情報アイコン（ⓘ）をクリックします。

ステップ 10 （任意） [Devices] テーブルでは、さまざまなアクションを実行できます。

- 昇順または降順で列をソートするには、列ヘッダーをクリックします。
- デバイスの詳細を表示するには、デバイス名をクリックしてから、[View Device Details] をクリックします。
- デバイスのコンプライアンスの詳細を表示するには、[Compliance] 列で [Non-Compliant] または [Compliant] をクリックします。
- サイトをデバイスに割り当てるには、[Site] 列の下の [Assign] をクリックします。
- デバイスロールを変更するには、[Device Role] 列の下にある編集アイコンをクリックし、[ACCESS] や [CORE] などのオプションから選択します。
- エントリの数を変更するには、ウィンドウの一番下までスクロールし、[Show Records] ドロップダウンリストから、表示するエントリの数を選択します。

（注） テーブルに 25 を超えるエントリがあり、別のフォーカスビューを選択した場合、新しい各ビューで同じ数のエントリが表示されます。

（注） 各フォーカスビューには異なる列が表示され、テーブルビューをカスタマイズして、[Compliance]、[Site]、[Device Role]、[Software Image] などの列を含めることができます。

SSH キー検証エラーへの対処

[**Inventory**] ウィンドウで、Catalyst Center は SSH キーの検証に失敗したデバイスを表しています。このエラーに対処するには次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 [管理性（Manageability）] 列で、デバイスの [SSHキー検証の失敗（SSH key verification failed）] リンクをクリックします。

ステップ 3 表示されるダイアログボックスで、次のいずれかの手順を実行します。

問題	結果
SSH キー変更のグローバルな自動受け入れを有効または無効にするには、	[**SSH key configuration**] をクリックします。 詳細については、SSH キー変更の自動承認の設定（77 ページ） を参照してください。
SSH キー検証エラーがあるすべてのデバイスの一覧が表示されるスライドインペインを開くには、	1. [**All errors**] をクリックします。 2. SSH キーの変更を承認するデバイスのチェックボックスをオンにします。 3. [確認（Confirm）] をクリックします。 これにより、選択したデバイスの再同期がトリガーされます。
デバイスの SSH キーが意図的に変更されたことを把握した場合は、	[**Confirm**] をクリックします。 これにより、デバイスの再同期がトリガーされます。

SSH キー変更の自動承認の設定

[**SSH key configuration**] ウィンドウでは、Catalyst Center が SSH キーの変更を自動的に受け入れるかどうかを設定できます。

重要 このオプションを有効にした場合は、SSH キー検証に失敗したすべてのデバイスを手動で再同期する必要があります。

手順

ステップ 1 メインメニューから次を選択します。 [**System** > **Device Settings** > **SSH key trust**]。

ステップ 2 行われた SSH キーの変更の自動承認を有効または無効にするには、[**Accept all changes**] トグルボタンをクリックします。

ネットワークデバイスの削除

Catalyst Center からネットワークデバイスを削除するには、次の手順を実行します。

ファブリックネットワークの一部ではないデバイスを Catalyst Center データベースから削除できます。

（注）
- デバイスがファブリックネットワークの一部である場合は削除できません。ファブリックネットワークからデバイスを削除し、その後インベントリから削除します。詳細については、*Cisco Catalyst Center User Guide*の「Remove a device from a fabric」を参照してください。
- ワイヤレスセンサーをインベントリから削除すると、センサーは工場出荷時のデフォルト状態にリセットされます。センサーが再参加すると、現在の設定が取得されます。

始める前に

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

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

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するか、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することができます。

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。



（注） Cisco ISE と統合されたデバイスを削除すると、削除されたデバイスは Cisco ISE の新しいネットワーク デバイス グループ（NDG）グループに移動します。

ステップ 4 （任意）[**Warning**] ウィンドウで、[**Config Clean-Up**] チェックボックスをオンにします。

デバイス可制御性ワークフローがトリガーされます。ネットワーク設定とテレメトリ設定が、選択したデバイスから削除されます。詳細については、『Cisco Catalyst Center Administrator Guide』の「Device Controllability」セクションを参照してください。



（注） Catalyst Center を介してプロビジョニングされたワイヤレスコントローラに対してこのチェックボックスをオンにすると、Catalyst Center で検出される前にワイヤレスコントローラで手動で設定したコマンドを含む、すべての AAA 関連コマンドが削除されます。

- デバイスの削除中に AAA 設定を保持する場合は、このチェックボックスをオンにしないでください。
- どの AAA コマンドが削除されたかを確認するには、Catalyst Center で AAA 設定を管理します。

ステップ 5 **[OK]** をクリックして、アクションを確認します。

デバイス構成を今すぐまたは後で展開する

設定の可視性と制御をサポートするワークフローのスケジュールの手順で、次の手順を完了してデバイス設定を今すぐ、または後で展開します。

始める前に

設定で [Visibility and Control of Configurations] が無効になっていることを確認してください。

手順

ステップ 1 [Now] または [Later] をクリックします。必要に応じてタスクの名前を更新します。



（注） 可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Preview and Deploy (Recommended)] がデフォルトで選択されます。[Now] および [Later] オプションはグレー表示されます。

ステップ 2 [Performing Initial Checks] ウィンドウで、展開するためのタスクを準備して送信します。

a) すべての問題に対処し、デバイス設定を展開します。

[Recheck] をクリックし、すべての検証が成功したことを確認します。

b) [Submit] をクリックします。

デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認します。

デバイス設定のプレビューと展開

設定の可視性と制御をサポートするワークフローのスケジュールの手順まで来たら、この手順を実行してデバイス設定のプレビューと展開を行います。

始める前に

設定で [Visibility and Control of Configurations] が有効になっていることを確認してください。

手順

ステップ 1 [Preview and Deploy (Recommended)] をクリックし、必要に応じてタスク名を更新します。



（注） デフォルトでは、可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Preview and Deploy (Recommended)] が選択されます。[Now] および [Later] オプションはグレー表示されます。

ステップ 2 [初期チェックの実行（Performing Initial Checks）] ウィンドウで、すべての問題に対処して、[次へ（Next）] をクリックし、現在の展開を続行します。

ウィンドウの右下隅にある [Recheck] をクリックし、すべての検証が成功したことを確認します。

ステップ 3 [Preparing Devices and Configuration Models] ウィンドウで、システムがデバイスを準備してデバイス設定を生成するのを待ちます。



ヒント　準備には時間がかかる場合があります。[Exit and Preview Later] をクリックすると、[Tasks] ウィンドウで作業項目を確認できます。

ステップ 4 **[設定のプレビュー（Preview Configuration）]** ウィンドウで、次の手順を実行します。

a) デバイス構成を確認します。

b) 展開オプションを選択します。

クリックする対象	目的
[Deploy] または [Submit for Approval]	デバイス構成を展開します。
[Exit and Preview Later]	後でデバイス構成を確認して展開します。 後で、[Tasks] ウィンドウに移動して作業項目を開き、[Deploy] または [Submit for Approval] をクリックします。



（注）　ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

ステップ 5 展開のスケジュールを設定します。

a) 設定を展開するタイミングと場所（該当する場合）を指定します。

確認のために設定を送信する場合は、IT 管理者へのメモを追加します。

b) [Submit] をクリックします。

作業項目の承認ステータスまたはタスクの展開ステータスは、[Tasks] ウィンドウで確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信します。承認された作業項目は、スケジュールされた時刻に展開されます。



（注）　タスクを送信したら、タスク名をクリックして **[Activities]** > **[Tasks]** ウィンドウの [Task Progress] バーでプロビジョニングタスクの進行状況を確認します。

プロビジョニングされていないデバイスのサイトへの割り当て

この手順を使用して、まだプロビジョニングされていないデバイスをサイトに割り当てます。

（注）
- デバイスをサイトに割り当てると、SyslogサーバーおよびSNMPトラップサーバーとしてCatalyst Center が設定されます。Syslog レベル 2 が有効になり、グローバルテレメトリを設定できます。
- まだプロビジョニングされていないワイヤレス AP は、フロアにのみ割り当てることができます。その後、まだプロビジョニングされていない場合は、割り当てられたフロアマップから削除することで、フロアからワイヤレス AP の割り当てを解除できます。詳細については、*Cisco Catalyst Center User Guide*の「Remove APs from a map」を参照してください。
- サードパーティ製デバイスはサイトに割り当てられますが、そのデバイスはCatalyst Centerによって管理されません。可視性だけが提供されます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

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。

（注） Firepower Threat Defense（FTD）高可用性（HA）ペアのデバイスを異なるサイトに割り当てることはできません。ペアの両方のデバイスを同じサイトに割り当てます。

ステップ 3 [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。

ステップ 4 [Assign Device To Site] スライドインペインで、デバイスのサイトアイコン（  ）の横にあるリンクをクリックします。

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、[Save] をクリックします。

ステップ 6 （任意） 複数のデバイスを選択して同じ場所に追加する場合は、最初のデバイスで [Apply to All] チェックボックスをオンにして残りのデバイスに同じ場所を割り当て、[Next] をクリックします。

ステップ 7 [Summary] 設定を確認し、[Next] をクリックします。

（注） アプリケーションテレメトリとコントローラベースのアプリケーション認識（CBAR）は、[Design] > [Network Settings] > [Telemetry] ウィンドウで [Application Telemetry] と [CBAR] を有効にすると、該当するネットワーク デバイスでデフォルトで有効になります。詳細については、テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （93 ページ）を参照してください。

[Application and Endpoint Visibility] の有効化は、コントローラベースのアプリケーション認識（CBAR）の有効化または展開解除されたアプリケーション可視性サービス（AVS）がサポートされないデバイスについてはデフォルトでスキップされます。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（79 ページ）を参照してください。

（注） MD5 認証タイプのみがデバイスに設定されている場合、ソフトウェア イメージ バージョンまたはゴールデンタグ付きイメージバージョン 17.14.1 以降のデバイスのサイト割り当てはブロックされます。

サイトの割り当てを続行するには、SHA 認証も設定する必要があります。SNMP ログイン情報の認証タイプとして SHA を設定する方法については、『*Catalyst Center* ユーザーガイド』の「グローバル デバイス クレデンシャルの編集」を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 10 サイトにデバイスを割り当てるときに [Device Controllability] が有効になっていると、ワークフローが自動的にトリガーされ、サイトからデバイスにデバイス設定がプッシュされます。

詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Device Controllability」セクションを参照してください。

[Focus] ドロップダウンリストから [Provision] を選択し、[Provision Status] 列の [See Details] をクリックします。[Device Controllability] を有効にしている場合、デバイスにプッシュされる設定が別のウィンドウに表示されます。

マップへの AP の追加

この手順では、フロアマップに AP を追加する方法について説明します。フロアには最大200個のAPを追加できます。

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、[Discovery] 機能を使用して検出します。『検出の概要 （16 ページ）』を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーから、**[2D]** > **[Add/Edit]** をクリックします。

デフォルトでは、[Devices] トグルボタンと [Access Points] トグルボタンが選択されています。

ステップ 4 マップの左側のペインで、[Add Access Points] をクリックします。

ステップ 5 [**Add Access Points**] スライドインペイン で、次のいずれかを実行します。

タスク	操作
単一 APを追加するには、次の手順を実行します。	追加するAP を見つけ、右にスクロールして [**Add**] をクリックします。
複数のAPを追加するには、次の手順を実行します。	複数の AP を追加するには：追加する AP の横にあるチェックボックスをオンにして、[**Add Selected**] をクリックします。
すべての AP を追加するには	[**All APs**] をクリックし、[**Add Selected**] をクリックします。
自動検出に対応した AP を追加するには	[**Auto Locate Capable APs**] をクリックし、[**Add Selected**] をクリックします。

（注） 利用可能な検索オプションを使用して、AP を検索できます。[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 AP 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。

編集モードでは、新しく追加されたAPは、マップの左ペインの**[Unpositioned]**カテゴリに表示されます。詳細については、AP をマップ上に配置する （84 ページ）を参照してください。

ステップ 6 AP をフロアに追加したら、[Add Access Points] スライドインペインを閉じます。

次のタスク

APをマップに追加すると、APがインベントリから削除された後でも、ワイヤレスマップに次のデータが自動的に保存されます。

- AP 名
- AP MAC address
- AP の現在のサイト
- マップ上の AP の現在位置

（注） 対応するサイトをネットワーク階層から削除すると、保存されている AP データも削除されます。

ワイヤレスコントローラ とそのすべての管理対象 APをインベントリから削除すると、Catalyst Centerはマップ上に対応するAPの計画済みAPアイコンを表示します。詳細については、*Cisco Catalyst Center User Guide* の「About the AP Icon and Planned AP Icon」を参照してください。

同じ AP が後でインベントリで再検出された場合、Catalyst Center は、別の ワイヤレスコントローラ がそれを管理している場合でも、マップ上の同じサイトと位置にそれを自動的に再配置します。

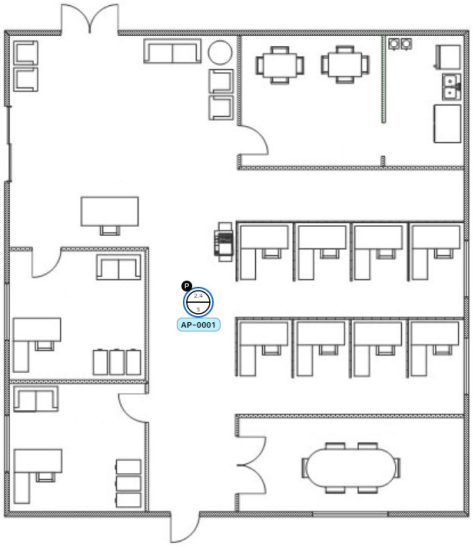
AP がインベントリから削除されたときに AP データをマップから削除するには、次のいずれかを実行します。

- インベントリから ワイヤレスコントローラ を削除する前に、対応する AP を **[Global]** サイトに割り当てます。詳細については、プロビジョニングされていないデバイスのサイトへの割り当て （81 ページ）を参照してください。
- インベントリから ワイヤレスコントローラ を削除した後、対応する計画済み AP をマップから削除します。詳細については、*Cisco Catalyst Center User Guide*の「Remove APs from a Map」を参照してください。

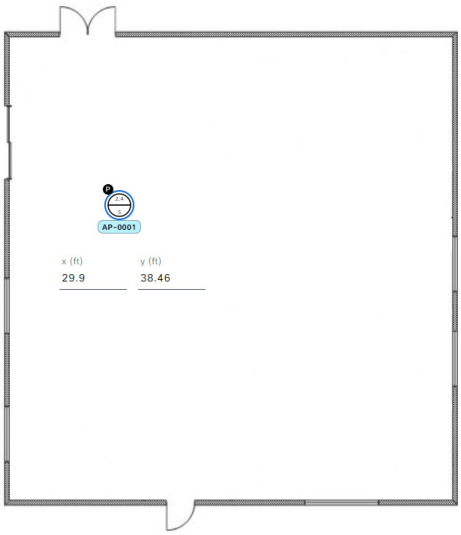
AP をマップ上に配置する

APをフロアに追加した後、次のいずれかの方法を使用して、APをマップ上に配置する必要があります。

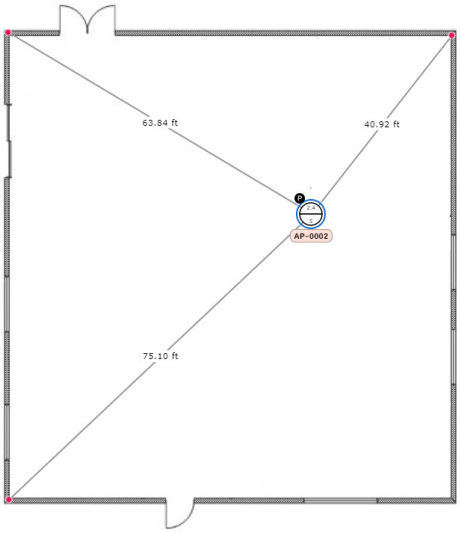
- マップ上に手動で配置します。フロアマップの詳細に関連付けることができる建物内の参照ポイントを使用して AP のおおよその位置を把握できる場合は、この方法を使用します。



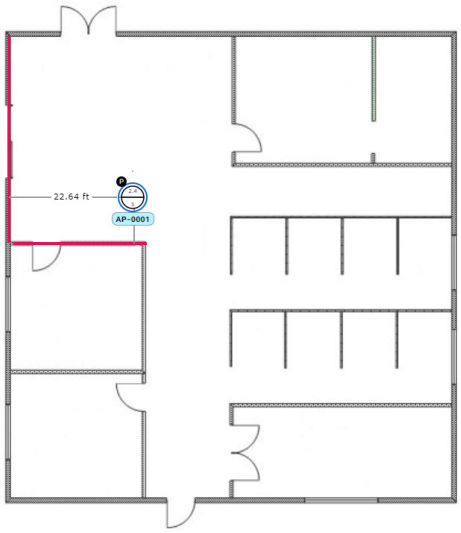
- **x** 座標と **y** 座標を定義します。AP の正確な座標が分かっており、マップ上の位置をできるだけ正確なものにしたい場合は、この方法を使用します。



- 3 点を使用して三角測量します。AP までの距離を測定するポイントが数点しかない大規模なオープンスペースがある場合は、この方法を使用します。たとえば、AP から部屋の各隅までを測定できます。



- 2 つの壁からの距離に基づいて位置を特定します。2 つの壁が交差するスペースに AP が配置されている場合は、それらが互いに垂直でなくても、この方法を使用します。



最初の方法（手動配置）を除くすべての方法では、測定値を手元に用意し、[**Global Map Properties**] 設定で測定単位が正しく指定されていることを確認する必要があります。詳細については、2D マップビューオプションを参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Design]** > **[Network Hierarchy]**。

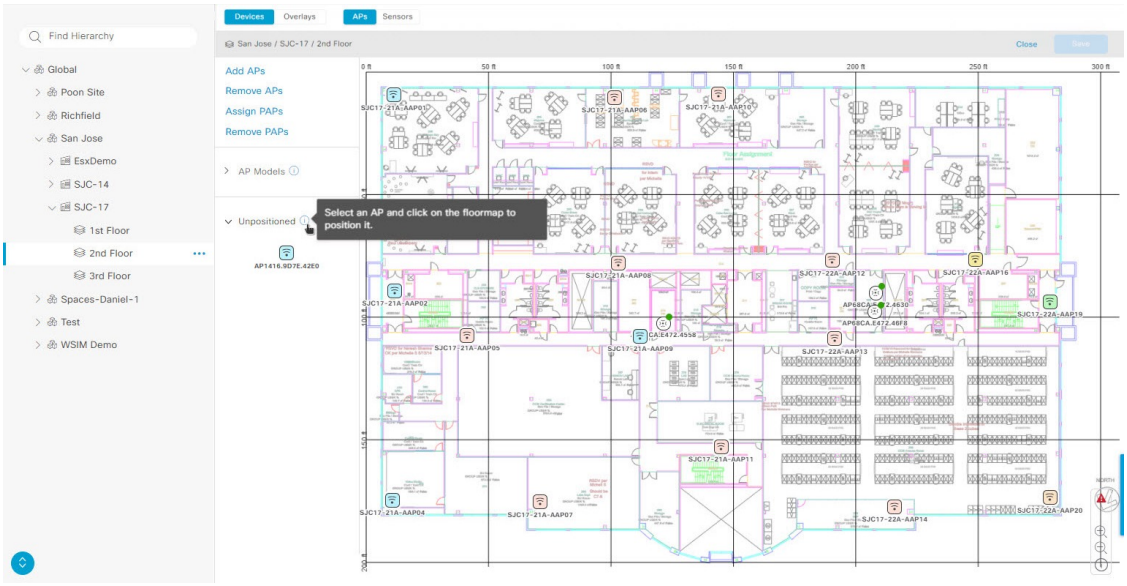
ステップ 2 フロアを 左側の階層ツリーから、以下を選択します します。

ステップ 3 マップツールバーで、**[2D]** > **[Add/Edit]** をクリックします。

デフォルトでは、[Devices] トグルボタンと [Access Points] トグルボタンが選択されています。

ステップ 4 マップの左側のペインにある [Unpositioned] エリアで、AP をクリックします。

図 7 : 未配置の *AP*



ステップ 5 AP を配置するには、次のいずれの方法を使用します。

- AP を配置するフロアマップ上の場所をクリックします。
- [Edit AP] スライドインペインで **x** 座標と **y** 座標を定義します。
- その場所を三角測量します。

1. [Edit AP] スライドインペインで、[3 points] をクリックします。
2. フロアマップをクリックして、最初の点を描画します。
3. ダイアログボックスで、AP から最初の点までの距離を設定し、[Set Distance] をクリックします。
4. 2 番目と 3 番目の点を同様の方法で定義し、[保存（Save）] をクリックします。

- フロアマップに 2 つの壁を定義し、定義した壁の間に AP を配置します。

1. [Edit AP] スライドインペインで、[2 walls] をクリックします。
2. 最初の壁を定義するには、フロアマップをクリックして線の描画を開始します。再度クリックすると線の描画が終了します。

   AP から最初の壁までの距離を設定するためのダイアログボックスが表示されます。
3. 距離をメートル単位で入力し、[Set Distance] をクリックします。
4. 同様に 2 つ目の壁を定義し、最初の壁と 2 つ目の壁から AP までの距離が交差する点があることを確認します。
5. [Save] をクリックします。

壁の間の定義された距離に基づいて AP が配置されます。

ステップ 6 マップツールバーで [Save] をクリックします。

（注） Cisco Connected Mobile experience（CMX）が Catalyst 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 （534 ページ）を参照してください。

Cisco ISE の Catalyst Center 設定について

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

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

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

認証サーバーとポリシーサーバーの設定

Catalyst 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。

Before you begin

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、Catalyst Center および Cisco ISE が統合されていることを確認します。

他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、次のタスクを実行します。

- AAA サーバーで Catalyst Center を登録します。これには、AAA サーバーと Catalyst Center の共有秘密を定義することが含まれます。
- AAA サーバーで Catalyst Center の属性名を定義します。
- Catalyst Center マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。

Cisco ISE を設定する前に、以下の点を確認してください。

- Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『Cisco Catalyst Center Compatibility Matrix』[英語] を参照してください。Cisco ISE のインストールについては、Cisco Identity Services Engine インストールおよびアップグレードガイド [英語] を参照してください。
- スタンドアロン Cisco ISE 展開環境がある場合は、Catalyst Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。
- 分散型 Cisco ISE 展開がある場合：

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

Note PAN 経由で ERS を使用することを推奨します。ただしバックアップの場合は、ポリシーサービスノード（PSN）で ERS を有効化できます。

分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。

TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する Protected Access Credential（PSN）は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達できる必要があります。

- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは完全修飾ドメイン名（FQDN）が含まれている必要があります。
- Catalyst Center システム証明書の SAN フィールドに、Catalyst Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

Procedure

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]**。

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

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

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密は 4 ～ 100 文字で指定する必要があります。スペース、疑問符（?）、小なり山カッコ（<）を含めることはできません。

Note 既存の Cisco ISE クラスタの一部である PSN をプライマリ AAA サーバーに設定しないでください。

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

- [Server IP Address]：Cisco ISE サーバーの IP アドレス。
- [Shared Secret]：デバイス認証のキー。共有秘密は 4 ～ 100 文字で指定する必要があります。スペース、疑問符（?）、小なり山カッコ（<）を含めることはできません。
- [Username]：Cisco ISE に HTTPS 経由でログインするために使用するユーザー名。
- [Password]：Cisco ISE HTTPS ユーザー名のパスワード。

Note ユーザー名とパスワードは、ネットワーク管理者に属する ISE 管理者アカウントである必要があります。

- [FQDN]：Cisco ISE サーバーの完全修飾ドメイン名（FQDN）。

Note

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

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

hostname.domainname.com

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

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

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

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

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

  このオプションを有効にする場合は、次のことを確認してください。

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

- [Enable Multiple Catalyst Center operation]：複数の Catalyst Center クラスターを単一の Cisco ISE システムに統合するには、このチェックボックスをオンにします。
- [Protocol]：[RADIUS]（デフォルト）と [TACACS]。両方のプロトコルを選択できます。

Attention

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

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

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

Cisco ISE サーバー登録フェーズ：

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

pxGrid サブスクリプション登録フェーズ：

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

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

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

ステップ 8 デバイスの Cisco ISE 統合ステータスを表示するには、次の手順を実行します。

a. メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウにデバイス情報が表示されます。

b. [Focus] ドロップダウンメニューから [Provision] を選択します。

c. [Devices] テーブルの [Provisioning Status] 列に、デバイスのプロビジョニングステータスに関する情報（[Success]、[Failed]、[Not Provisioned]）が表示されます。

[See 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. 表示されるスライドインペインで、[See Details] をクリックします。

e. [ISE Device Integration] タイルまでスクロールダウンして、デバイスの統合ステータスに関する詳細情報を表示します。

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

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

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『サイトの作成、編集、削除 （39 ページ）』を参照してください。

手順

ステップ 1 [Design] > [Network Settings] > [Telemetry] の順に選択します。メインメニューから次を選択します。

ステップ 2 [SNMP Traps] 領域で、次のいずれかのタスクを実行します。

- [Use Catalyst Center as SNMP trap server] チェックボックスをオンにします。
- [Add an external SNMP trap server] チェックボックスをオンにし、外部 SNMP トラップサーバーの IP アドレスを入力します。選択したサーバーによってネットワークデバイスから SNMP トラップとメッセージが収集されます。

ステップ 3 [Syslogs] 領域で、次のいずれかのタスクを実行します。

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

ステップ 4 [Application Visibility] 領域で、[Enable by default on wireless access devices] チェックボックスをオンにして、ネットワークデバイスサイトの割り当て時にアプリケーションテレメトリおよびコントローラベースのアプリケーション認識（CBAR）をデフォルトで有効にします。

次のいずれか 1 つのタスクを実行します。

- [Use Catalyst Center as NetFlow collector] オプションボタンをクリックします。デバイスインターフェイスの NetFlow の構成は、デバイスでアプリケーションテレメトリを有効にした場合にのみ完了します。NetFlow の宛先サーバーをデバイスに設定するには、サイトレベルで NetFlow コレクタを選択します。
- [Add Cisco Telemetry Broker (CTB)] オプションボタンをクリックし、Cisco Telemetry Broker の IP アドレスとポート番号を追加します。Cisco Telemetry Broker はデバイスから NetFlow レコードを収集し、その情報を宛先に送信します。

（注） NetFlow レコードを受信するには、Cisco Telemetry Broker で Catalyst Center が宛先として設定されている必要があります。Catalyst Center が宛先として設定されていない場合、アプリケーション エクスペリエンスは機能しません。

ステップ 5 [Wired Endpoint Data Collection] エリアで、[Enable Catalyst Center Wired Endpoint Data Collection At This Site] オプションボタンをクリックして、サイトのアクセスデバイスで IP デバイストラッキング（IPDT）をオンにします。

サイトの IPDT を有効にしない場合は、[Disable Catalyst Center Wired Endpoint Data Collection At This Site] オプションボタン（デフォルト）をクリックします。

IPDT を有効にすると、アクセスポートに接続されているクライアントが Catalyst Center に表示されます。トランクポートとポートチャネルに接続されているクライアントは、Catalyst Center に表示されません。

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

ソフトウェアバージョン 17.5.1 以降を実行している Cisco Catalyst 9410R スイッチの場合、4/0/48 で終わるポートは IPDT 設定中に意図的にスキップされます。

ステップ 6 [Wireless Controller, Access Point and Wireless Clients Health] エリアで、[Enable Wireless Telemetry] チェックボックスをオンにして、ネットワーク内のワイヤレスコントローラ、AP、およびワイヤレスクライアントの状態をモニターします。

デバイス可制御性ワークフローでワイヤレステレメトリを有効にすると、テレメトリデータ収集がアクティブになり、テレメトリコマンドがワイヤレス設定にプロビジョニングされます。この機能を無効にすると、テレメトリのセットアップが停止し、モニタリング機能が失われます。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Device Controllability」を参照してください。

ステップ 7 [Save] をクリックします。

Cisco AI Network Analytics の設定

この手順で、Cisco AI Analytics 機能を有効にして、ネットワークデバイスとインベントリ、サイト階層、トロポジデータからネットワークイベントのデータを Cisco AI Cloud にエクスポートします。

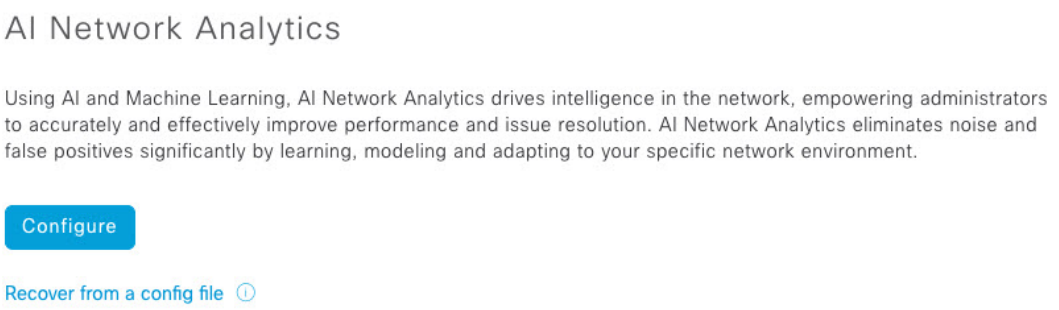
始める前に

- Catalyst Center の 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、Advantage ソフトウェアライセンスに含まれています。
- AI Network Analytics アプリケーションの最新バージョンがインストールされていることを確認してください。*Cisco Catalyst Center Administrator Guide*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）

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。

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



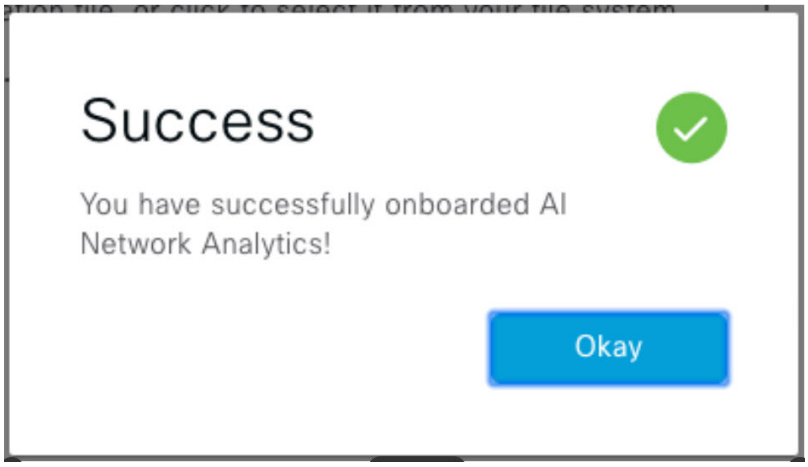
ステップ 3 次のいずれか 1 つのタスクを実行します。

- 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開きます。

2. 表示されたエリアに構成ファイルをドラッグアンドドロップするか、ファイルシステムからファイルを選択します。
3. [Restore] をクリックします。

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



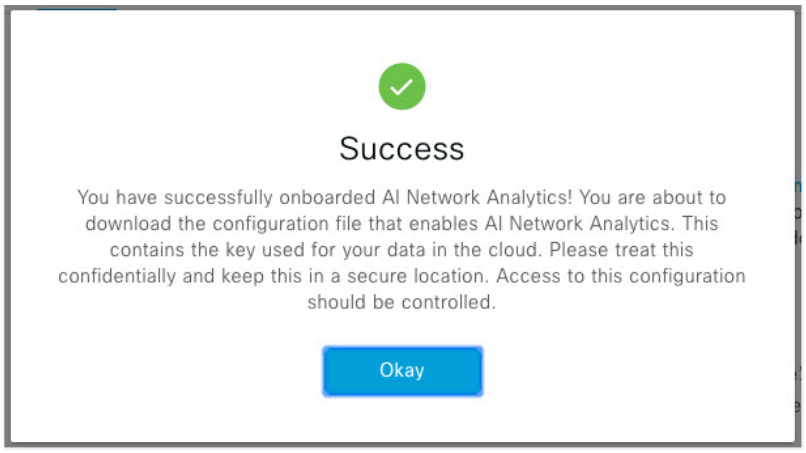
- Cisco AI Network Analytics を初めて構成する場合は、次の手順を実行します。

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. [Next] をクリックします。

   [Terms and Conditions] ウィンドウが表示されます。
4. [Accept Cisco Universal Cloud Agreement] チェックボックスをオンにして契約条件に同意してから、[Enable] をクリックします。

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



ステップ 4 [Success] ダイアログボックスで [Okay] をクリックします。
AI ネットワーク分析 ウィンドウが表示され、[Enable AI Network Analytics] トグルボタンが表示されます。

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

Cisco AI Network Analytics の無効化

Cisco AI Network Analytics のデータ収集を無効にするには、次の手順で AI Network Analytics の機能を無効にする必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] までスクロールし、[Cisco AI Analytics] を選択します。
各機能のチェックマーク（）は、その機能が有効になっていることを示します。チェックボックスがオフの場合（）、機能は無効になっています。

ステップ 3 [AI Network Analytics] 領域で、[Enable AI Network Analytics] トグルボタンをクリックしてオフにします（）。

ステップ 4 [Update] をクリックします。

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

ステップ 6 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は、機械推論ナレッジベースが毎日自動で更新されるよう Catalyst Center を設定するか、手動で更新することで入手できます。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。

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

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

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

- [AUTO UPDATE] ：機械推論ナレッジベースが Catalyst Center で自動的に毎日更新されます。
- [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER, SECURITY ADVISORY, FIELD NOTICES AND EOX]：自動構成を実行できる CX Cloud と Catalyst Center を統合します。この統合により、Catalyst Centerのセキュリティ アドバイザリ ツールから直接デバイスの脆弱性を検出する機能が更に強化されました。

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

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

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

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

  1. [Download] をクリックします。

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

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

ステップ 5 [CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY] チェックボックスをオンにして、ネットワークバグ ID およびセキュリティアドバイザリとの Cisco CX Cloud の連携を有効にします。

ステップ 6 [Security Advisories Settings] エリアで、[RECURRING SCAN] トグルボタンをクリックして、毎週の定期的なスキャンを有効または無効にします。

ステップ 7 [CISCO CX CLOUD] トグルボタンをクリックして、Cisco CX Cloud を有効または無効にします。

ローカリゼーションの有効化

Catalyst Center の GUI ウィンドウは、英語（デフォルト）、中国語、日本語、または韓国語で表示できます。

デフォルトの言語は変更するには、次の手順を実行します。

手順

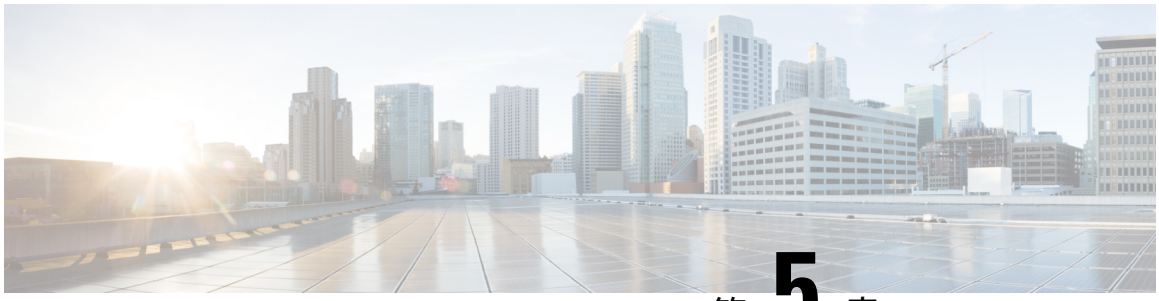
ステップ 1 ブラウザで、サポートされている言語（中国語、日本語、または韓国語）のいずれかにロケールを変更します。

- Google Chrome の場合：
  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. **[Languages]** をクリックします。
  3. [Add Languages] をクリックします。
  4. [**Add languages**] ダイアログボックスで、[**Chinese**]、[**Japanese**]、[**Korean**] のいずれかを選択して、[**Add**] をクリックします。
- Mozilla Firefox の場合：
  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. **[Language and Appearance]** > **[Language]** エリアで、**[Choose]** をクリックします。
  3. [**Select a language to add**] ドロップダウンリストで、[**Chinese**]、[**Japanese**]、[**Korean**] のいずれかを選択します。

4. [OK] をクリックします。

ステップ 2 Catalyst Center にログインします。

選択した言語で GUI が表示されます。



第 5 章

企業全体の健全性のモニターとトラブルシューティング

- エンタープライズ （101 ページ）
- 企業全体の健全性のモニターとトラブルシューティング （101 ページ）

エンタープライズ

エンタープライズは次のようなネットワークコンテキストです。

- ネットワークデバイス、ルータ、スイッチ、ワイヤレスコントローラ、アクセスポイントが含まれます。
- Assurance での、エンタープライズ全体の正常性のモニターとトラブルシューティングを可能にします。
- プロアクティブな管理のための分析と可視性をサポートします。

企業全体の健全性のモニターとトラブルシューティングに、Assurance を使用できます。エンタープライズはネットワークデバイスとクライアントで構成されます。

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、および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ます。メンテナンスモードのクライアントおよびデバイスはネットワーク健全性スコアに含まれ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。Catalyst Center は、有線クライアントと無線クライアントの両方をサポートしています。

企業全体の健全性のモニターとトラブルシューティング

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。Assurance は、ユーザーのアクセス範囲を特定のネットワークサイトに制限するサイトベースのロールベースアクセス

企業全体の健全性のモニターとトラブルシューティング

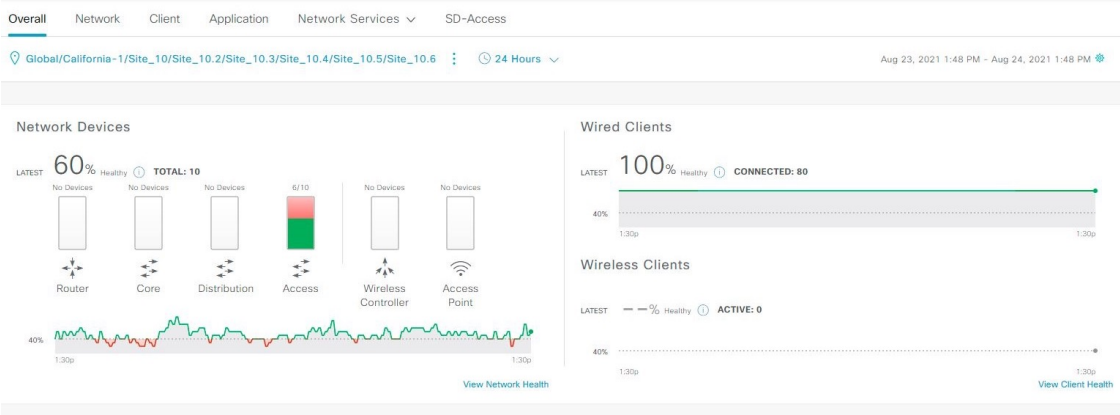
制御（SRBAC）をサポートしています。[Overall Health] ダッシュボードを使用している間は、サイトとデバイスにアクセスできるようにする必要があります。ユーザーのロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

図 *8 : [Overall Health]* ダッシュボード



ステップ 2 次の機能には [Overall Health] ダッシュボードの上部のメニューバーを使用します。

企業全体の健全性のモニターとトラブルシューティング

[Overall Health] ダッシュボードの上部のメニューバー	
アイテム	説明
Global [Location] ペイン	• Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 [Sites Details] テーブルでは次の機能を実行できます。 • Hide Sites をクリックして [Sites] テーブルを非表示にします。 • : このトグルボタンをクリックして、ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択に基づいて、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テーブルに表示されます。 • : このトグルボタンをクリックすると、企業のすべてのサイトの正常性が、地理的ロケーションに基づいた正常性マップで表示されます。デフォルトでは、提示されるサイトは問題の重大度に従って色分けされています。 ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、データを取得できなかったことを示します。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Overall] ダッシュボードに表示されます。
時間範囲	過去 3 時間、24 時間、または 7 日間のデータを表示できます。
[Actions] ドロップダウン リスト	[Overall] ダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。 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 （434 ページ）およびカスタムダッシュボードの作成 （431 ページ）を参照してください。

ステップ 3 次の機能には [Overall Health Summary] ダッシュレットを使用します。

企業全体の健全性のモニターとトラブルシューティング

[Overall Health Summary] ダッシュレット	
アイテム	説明
[Network Devices]	Network Score：企業全体での正常（良好）なデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アクセスポイント）の割合。ネットワークの正常性スコア （143 ページ）を参照してください。 Device Category Health Score：[Router]、[Core]（サードパーティ製デバイスを含む）、[Distribution]、[Access]、[Controller]、[Access Point] のデバイスカテゴリで正常（良好）なネットワークデバイスの割合。 （注） SD-Access ファブリックを選択すると、[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このエリアに表示されます。 [View Network Health] をクリックして、[Network Health] ダッシュボードを開きます。ネットワークの正常性のモニターとトラブルシューティング （107 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。クライアントの正常性スコア （192 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正常性のモニターとトラブルシューティング （156 ページ）を参照してください。

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

[Network Services] ダッシュレット	
アイテム	説明
AAA	企業全体のすべての AAA サーバーについて、成功したトランザクションと失敗したトランザクションの合計パーセンテージを示します。 [View AAA Dashboard] をクリックして、[Network Services AAA] ダッシュボードを開きます。AAA ネットワークサービスのモニター （243 ページ）を参照してください。
DNS	企業全体のすべての DNS サーバーについて、成功したトランザクションと失敗したトランザクションの合計パーセンテージを示します。 [View DNS Dashboard] をクリックして、[Network Services DNS] ダッシュボードを開きます。DNS ネットワークサービスの監視 （252 ページ）を参照してください。

企業全体の健全性のモニターとトラブルシューティング

[Network Services] ダッシュレット	
アイテム	説明
[DHCP]	企業全体のすべてのDHCPサーバーについて、成功したトランザクションと失敗したトランザクションの合計パーセンテージを示します。 [View DHCP Dashboard] をクリックして、[Network Services DHCP] ダッシュボードを開きます。DHCP ネットワークサービスの監視 （247 ページ）を参照してください。

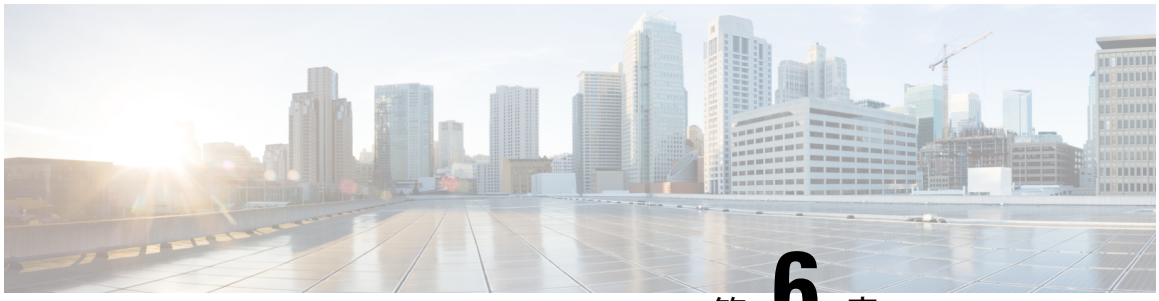
ステップ 5 次の機能には [Site Analytics] ダッシュレットを使用します。

[Site Analytics] ダッシュレット
[Site Analytics] ダッシュレットには、集約されたカバレッジ、オンボーディング、ローミング、および接続速度の観点から、ワイヤレスネットワークのパフォーマンスが最も低いサイトが表示されます。パフォーマンスは、デフォルトのパフォーマンスしきい値または [Site Analytics Settings] ウィンドウで設定したしきい値に基づいています。詳細については、サイト分析設定の構成 （297 ページ）を参照してください。 サイト分析データを収集するには、AI Network Analytics を有効にする必要があります。[Enable AI Network Analytics] リンクをクリックして、このシステム設定を構成できる [Cisco AI Analytics] ウィンドウに直接移動します。詳細については、Cisco AI Network Analytics の設定 （95 ページ）を参照してください。 各 KPI カテゴリで、サイト名をクリックしてサイトに関する詳細情報を表示するか、[View Site Analytics] をクリックして [Site Analytics] ウィンドウに直接移動します。詳細については、サイト分析を使用したネットワークのモニターとトラブルシューティング （287 ページ）を参照してください。 （注） AI Network Analytics が有効になっていない場合、Assurance ではサンプルデータを含むダッシュレットの例が表示されます。

ステップ 6 次の機能には [Top 10 Issue Type] ダッシュレットを使用します。

企業全体の健全性のモニターとトラブルシューティング

[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インスタンスをクリックし、必要に応じて次の操作を実行できます。 • 問題インスタンスを解決するには、[Status] ドロップダウンリストで [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、未解決の問題の表示 （301 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ーとトラブルシューティング

- ネットワークの正常性のモニターとトラブルシューティング （107 ページ）
- デバイスの正常性のモニターとトラブルシューティング （117 ページ）
- ネットワークデバイスの正常性スコアの設定 （139 ページ）
- ファブリックデバイスの SNMP コレクタメトリックの有効化 （141 ページ）
- ネットワークの正常性スコアと KPI メトリックについて （143 ページ）
- RF の計算について （152 ページ）

ネットワークの正常性のモニターとトラブルシューティング

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

ネットワークは、ルータ、スイッチ、ワイヤレスコントローラ、および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ます。メンテナンスモードのクライアントおよびデバイスはネットワークの正常性スコアに含まれないことに注意してください。

Assurance は、ユーザーのアクセス範囲を制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。[Network Health] ダッシュボードを使用している間は、サイトとデバイスにアクセスできるようにしておく必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

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

手順

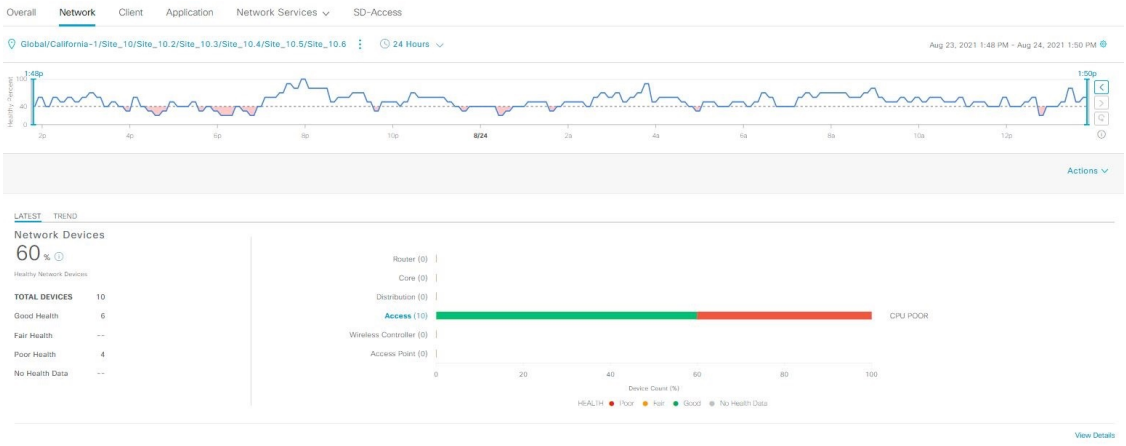
ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network] タブをクリックします。

[Network health] ダッシュボードが表示されます。

図 *9 : [Network Health]* ダッシュボード



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

ステップ 4 ロケーションアイコンの横にある をクリックして、以下を切り替えます。

- [サイトマップ（Site Map）]：ネットワーク階層の地理的ビューを提供します。
- [サイトテーブル（Site Table）]：正常性スコアやデバイス数を含む、すべてのサイトのリストベースビューを提供します。

[Location] ペインには次の機能があります。

[Location] オプション	
アイテム	説明
 トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。 ドロップダウンリストをクリックすると、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [建物/屋外エリアの表示（Building/Outdoor Area view）]：リストを建物レベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。
	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。
トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。
	マップビューまたはテーブルビューを非表示にするには、この閉じるアイコンをクリックします。

ステップ 5 上部のメニューバーにある時間範囲設定（  ）をクリックして、 ダッシュボードに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューで、[3 hours]、[24 hours]、[7 days] のいずれかの時間範囲を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 6 上部のメニューバーにある [Actions] ドロップダウンリストをクリックすると、次の機能を利用できます。

- [Export Dashboard]：ネットワークダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更（434 ページ） およびカスタムダッシュボードの作成 （431 ページ） を参照してください。

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

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

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

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

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

しきい値を変更するには、次の手順を実行します。

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

- タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。テレメトリのステータスを表示するには、次の手順を実行します。
  - 水平バーにカーソルを合わせると、ネットワークデバイスのテレメトリステータス（[Good]、[Fair]、[Poor] など）がツールチップに表示されます。
  - ツールチップの [Telemetry Status] をクリックするとスライドインペインが開き、テレメトリステータスの概要が表示されます。

（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。

（注） タイムラインのギャップは、デバイスからヘルスデータが取得されなかったことを示します。この状況は、デバイスがメンテナンスモードのときに発生する可能性があります。

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

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

[Network Devices Health Summary] ダッシュレット	
アイテム	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。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。ネットワークの正常性スコア （143 ページ） を参照してください。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数が表示されます。 • [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間の各デバイスカテゴリ（アクセス、コア、ディストリビューション、ルータ、ワイヤレスコントローラ、アクセスポイント）のパフォーマンスを示します。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスのヘルス スコアと数が表示されます。 チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。たとえば、リンクエラー、高い CPU 使用率、高いメモリ使用率、高ノイズ、低い電波品質などがあります。 ハイパーリンク付きのデバイスカテゴリ（[Access]、[Core]（サードパーティ製デバイスを含む）、[Distribution]、[Router]、[Wireless Controller]、[Access Point]）をクリックして、スライドインペインに追加の詳細情報を表示できます。 • **トレンド**：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 で

[Network Devices Health Summary] ダッシュレット	
アイテム	説明
	す。 ●：正常性データなし（サードパーティ製デバイスとメンテナンスモードのデバイスを含む）。ヘルス スコアは 0 です。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 9 [AP] ダッシュレットを使用すると、次の情報を確認できます。

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

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

[Top N APs by High Interference] ダッシュレット
高干渉の AP に関する情報。2.4 GHz、5 GHz、または 6 GHz を選択できます。 [Latest] タブには、5 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 10 [Network Devices] ダッシュレットを使用すると、次の機能を利用できます。

[Networks Devices] ダッシュレット	
アイテム	**説明**
Type	オプション（[All]、[Access]、[Core]、[Distribution]、[Router]、[WLC]、[AP]）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処理できます。 （注） デバイスタイプ「ルータ」に基づいてデバイスをフィルタ処理すると、デバイスロール「ボーダールータ」を持つデバイスが表示されます。
全体的な正常性	次のオプションを使用して、デバイスの全体的な正常性スコアに基づいてテーブルをフィルタ処理できます。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。

[Networks Devices] ダッシュレット	
アイテム	説明
[Network Devices] テーブル	ネットワーク内のすべてのデバイス、または選択したサイトのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、システムの正常性、データプレーンの接続性、およびコントロールプレーンの接続性の KPI メトリックの最小サブスコアです。 [Overall Health Score] 列で、正常性スコアの上にマウスカーソルを合わせます。デバイスの正常性スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。**デバイスの正常性**は、KPI メトリックの最小サブスコアです（デバイスのタイプに基づく）。ルータおよびスイッチの場合は、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）、ファブリック（コントロールプレーン到達可能性）の KPI メトリックがあります。[Fabric Domain Name]、[Fabric Name]、および [Fabric Role] 列には、ファブリックドメイン名、ファブリック名、およびファブリックロール（エッジ、ボーダー、マップサーバーなど）が表示されます。 各デバイスのデバイスアイコンにカーソルを合わせると、到達可能性ステータス（到達可能、稼働中、到達不能、再起動中など）が表示されます。 （注） サードパーティ製デバイスの場合、デバイスの到達可能性ステータスは [Reachable] または [Unreachable] のいずれかになります。
デバイス 360	[Device] 列でデバイスの名前をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。 （注） サイトに割り当てられていないデバイスをサイト管理者が検出した場合、割り当てられていないデバイスのデータは [Device 360] ウィンドウに表示されません。ただし、グローバル管理者は、[Device 360] ウィンドウで割り当てられていないデバイスのデータを確認できます。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。

[Networks Devices] ダッシュレット	
アイテム	説明
	テーブルの表示をカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 3. [Apply] をクリックします。

ステップ 11 [Network Devices Reachability] ダッシュレットを使用すると、次の情報を表示できます。

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

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

[WAN Link Utilization] ダッシュレット
棒グラフには、利用可能な WAN リンクに対してのみ、WAN リンク使用率のステータスが表示されます。 （注） リンクを WAN リンクと見なすには、システムで生成された WAN タグを必要なポートに手動で割り当てる必要があります。『Catalyst Center User Guide』の「Manage Your Inventory」の章の「Assign Tags to Ports」を参照してください。 [Latest] タブには、[Available] および [Not Available] の WAN リンクの 10 分間のスナップショットビューが表示されます。 [Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの要素を選択して、より詳細なデータを表示できます。 タイムラインスライダの下に水平バーとして表示されるデータを選択して、上位の場所、デバイスタイプ、および場所に基づいてテーブルをフィルタ処理できます。

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

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

デバイスの正常性のモニターとトラブルシューティング

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

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network] タブをクリックします。

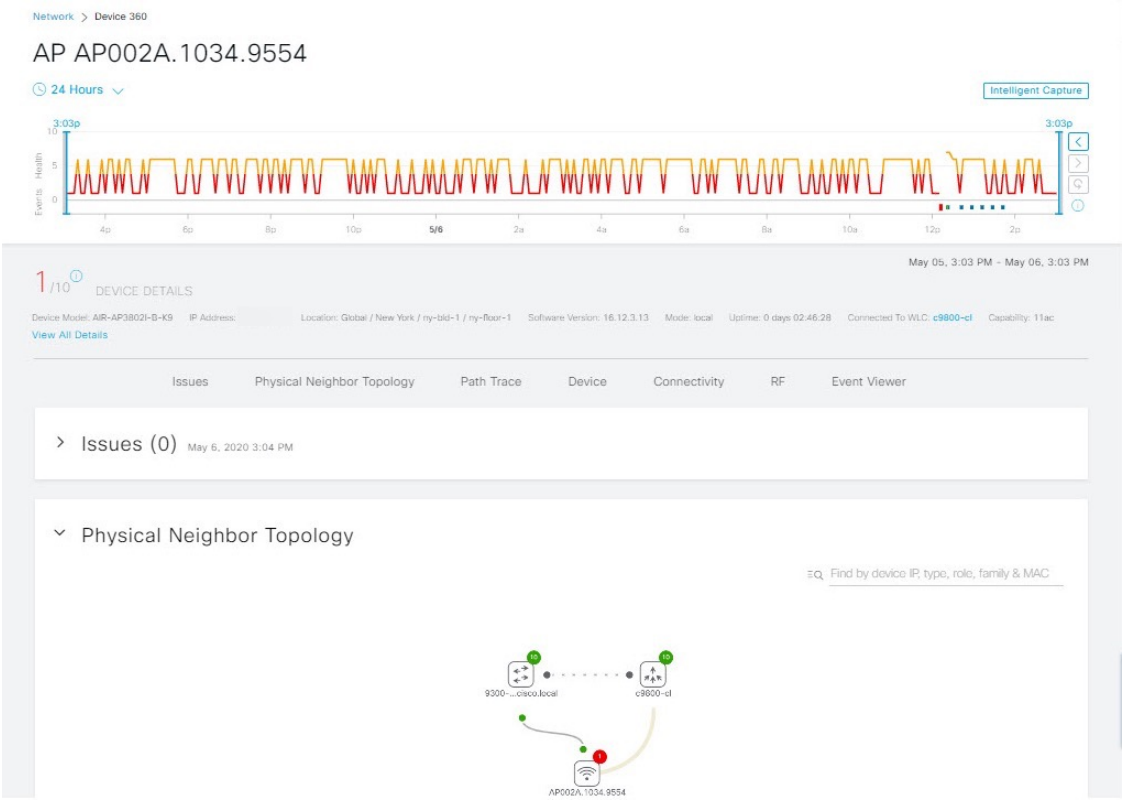
ステップ 3 [Network] 正常性ダッシュボードで、次のタスクのいずれかを実行します。

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

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

（注） デフォルトでは [Map View] が表示されます。

図 *10 : [Device 360]* ウィンドウ



（注） デバイス名の横にある [View Device Details] ハイパーリンクをクリックすると、デバイス インベントリ ウィンドウを相互起動できます。

ステップ 4 時間範囲設定（24 Hours）をクリックして、ウィンドウに表示されるデータの時間範囲を指定します。

a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。

b) 開始日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 [Intelligent Capture] をクリックすると、特定のネットワークデバイスのキャプチャされたオンボーディングおよびデータパケットを表示、モニターリング、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。AP の RF 統計の表示 （502 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がサポートされていない AP モデルもあります。[Intelligent Capture] が表示されない場合は、AP がサポート対象のモデルであること、また AP が [Network Health] ダッシュボード上の場所に割り当てられていることを確認します。

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

（注） タイムラインのギャップは、デバイスからヘルスデータが取得されなかったことを示します。この状況は、デバイスがメンテナンスモードのときに発生する可能性があります。

特定の期間にカーソルを合わせると、メンテナンスモードになっているアクセスポイントに対して [Under Maintenance] バナーが表示されます。

タイムラインスライダには、次の情報が表示されます。

- [正常性（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デバイスの正常性スコアと 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には、タイムラインスライダを必要な時間範囲に手動で移動します。

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

- タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。テレメトリのステータスを表示するには、次の手順を実行します。
  - 水平バーにカーソルを合わせると、ネットワークデバイスのテレメトリステータス（[Good]、[Fair]、[Poor] など）がツールチップに表示されます。
  - テレメトリが赤色で表示されている場合は、完全なデータ損失を示しています。
  - テレメトリが黄色で表示されている場合は、部分的なデータ損失を示しています。
  - ツールチップの [Telemetry Status] をクリックするとスライドインペインが開き、テレメトリステータスの概要が表示されます。

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

（注） メンテナンスモードのデバイスは、デバイスのヘルススコアの計算に含まれません。

デバイスの正常性スコアの詳細は次のとおりです。

- [Switch]：スイッチの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、CPU使用率、リンクエラー、リンク破棄、アップリンクの可用性、コントロールパネルへの到達可能性。また、ファブリックデバイスの場合は、ファブリックの正常性も含まれます。詳細については、「スイッチの正常性スコア （145 ページ）」を参照してください。

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

[Cisco StackWise Virtual]：アップリンクの可用性は、インフラストラクチャリンク、Cisco StackWise Virtual リンク（SVL）、およびデュアルアクティブ検出（DAD）リンクに基づいています。Cisco StackWise Virtual と制限事項について （138 ページ）を参照してください。

[Cisco StackWise]：アップリンクの可用性は、インフラストラクチャリンクおよび Cisco StackWise リンクに基づいています。Cisco StackWise と制限事項について （139 ページ）を参照してください。

- [Router]：ルータの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、CPU使用率、リンクエラー、リンク破棄、アップリンクの可用性、コントロールプレーンへの到達可能性。詳細については、「ルータの正常性スコア （146 ページ）」を参照してください。

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

- [AP]：APの正常性スコアは次のパラメータの最小サブスコアです。メモリ使用率、CPU使用率、リンクエラー、無線使用率、干渉、ノイズ、電波品質。詳細については、APの正常性スコア（148ページ）を参照してください。
- [Wireless Controller]：ワイヤレスコントローラの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、空きタイマー、空きメモリバッファ（MBufs）、作業キュー要素（WQE）プール、パケットプール、リンクエラー。ファブリック ワイヤレス コントローラの場合、ファブリックヘルスが含まれます。詳細については、ワイヤレスコントローラの正常性スコア（149ページ）を参照してください。

ヘルス スコアの色は、その重大度を示します。正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、データを取得できなかった、またはデバイスがメンテナンスモードであったことを示します。

- ●：重大レベルの問題。ヘルス スコアの範囲は 1 ～ 3 です。
- ●：警告。ヘルス スコアの範囲は 4 ～ 7 です。
- ●：エラーまたは警告はありません。ヘルス スコアの範囲は 8 ～ 10 です。
- ●：使用可能なデータがありません（メンテナンスモードのデバイスを含む）。ヘルス スコアは 0 です。

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

（注）
- [Fabric Site] の場合、[Fabric Role] 、[Fabric Domain] 、[System Resources] 、[Data Plane] 、[Virtual Network] 、[Transits] および [Events] の各要素がデバイス詳細エリアに表示されます。
- [Cisco StackWise Virtual] の場合、[Stack Status: Stackwise Virtual] と [StackWise Virtual Domain] の 2 つの追加要素が表示されます。
- [Cisco StackWise] の場合、[StackWise] という追加要素と、[StackWise (2)] のように、スタック内のスイッチ数が表示されます。スタックには最大 8 台のスイッチを設定できます。
- [Mesh AP] の場合、[Mode]、[Mesh Role] および [RAP] の各詳細情報がデバイス詳細領域に表示されます。
- PoE 対応デバイスの場合、[IEEE Class]、[Negotiated Power Level]、および [PoE Status] の各要素もデバイス詳細エリアに表示されます。

ステップ 9 [View Details] 領域で [View All Details] をクリックすると、一般的な情報、ネットワーク情報、ラックロケーションなど、デバイスの他の属性を表示するスライドインペインが開きます。デバイスタイプによっては、追加のデバイス固有の詳細が含まれる場合があります。

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

（注） デバイスがメンテナンスモードの場合、問題はトリガーされません。

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。問題名の横にメモアイコン（）があります。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

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、次のタスクを実行できます。

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

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

次のタスクを実行できます。

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

（注）

- AP 360 では、2 GHz および 5 GHz のクライアントが表示されます。これら 2 つのクライアントからの点線のリンク回線はクリックできません。また、APからワイヤレスコントローラへのリンク回線とワイヤレスコントローラから AP へのリンク回線はクリックできません。
- SD-Accessファブリックの場合、ファブリックグループはファブリックバッジアイコンで表示されます。
- Cisco StackWise Virtual および Cisco StackWise には、スタックのアイコン（  ）が表示されます。
- Cisco StackWise Virtual または Cisco StackWise が含まれているパスには、パストレースでスイッチのアイコンが表示されます。

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

- [APs]：シナリオと、各シナリオにつながる一連のサブイベントが表示されます。これにより、どのサブイベントの間に問題が発生したのかを特定できます。送信電力の変更、RF チャネル変更、無線リセットなどの無線リソース管理（RRM）イベントが表示されます。
- [Switches and Routers]：クリティカル以上の重大度（致命的およびアラート）を示すすべての syslog、アップ/ダウンしているあらゆるリンクのイベント、到達可能デバイスまたは非到達可能デバイスのイベントが表示されます。また、クリティカルレベルより重大度が低い syslog（エラー、注意、通知、および情報）も表示されます。
- [Wireless Controllers]：ワイヤレス コントローラ イベントを一覧表示します。Cisco AireOS デバイスの場合、選択したトラップと syslog が表示されます。Cisco IOS コントローラの場合、選択した syslog とイベントが表示されます。

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

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

パストレースの実行 （528 ページ）を参照してください。

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

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

アプリケーション エクスペリエンスとアプリケーションの可視性について （197 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 （206 ページ）を参照してください。

（注） このカテゴリは、ルータのみに表示されます。

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

次の各タブをクリックすると、対応する詳細が表示されます。

[Device Info] タブ
[Availability] セクションには、デバイスの CPU、メモリ、稼働時間、温度などに関する情報が表示されます。 [HA Redundancy] セクションには、Cisco Embedded Wireless Controller の冗長モード、冗長ユニット、ローカル状態、およびピア状態に関する情報が表示されます。 WLC 360 の場合、 [STANDARD POWER SERVICE] セクションには、デバイスの接続ステータスや直近の正常接続などの情報が表示されます。 （注） サードパーティ製デバイスの場合は、稼働時間チャートのみが表示されます。 • ワイヤレスコントローラに複数のセンサーがある場合、データには全センサーの最新の最高温度が反映されます。 • 帯域外で設定されたネットワークデバイスの場合、稼働時間のチャートは正常性スコアやその他のデータと正しく相関しません。たとえば、24 時間ウィンドウの稼働時間のチャートで、午前 11 時 39 分と午後 2 時 40 分にデバイスがダウンしたことが示されていたとします。その場合、午前 11 時 00 分 ー 午後 2 時 00 分の 3 時間ウィンドウを選択（タイムラインスライダを使用）しても、ダウンタイムが表示されません。この問題は、Catalyst Center がデバイスからシステム稼働時間情報を受信できないために発生します。この問題を回避するには、デバイスと Catalyst Center の間で構成を同期させます。

[Connectivity] タブ

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

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

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

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

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

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

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

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

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

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

- [Top Clients with Tx Drops per SSID]：パケットドロップ数についての上位 5 つのクライアントを、選択した SSID 別に表示します。このチャートは、バージョン 17.12 以降の Cisco 9800 ワイヤレスコントローラに接続されているクライアントでのみ使用できます。

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

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

[Fabric Site] タブ
このタブは、SD-Access ファブリックで使用できます。 ファブリック KPI は、[Fabric Site Connectivity]、[Fabric Infrastructure] および [Fabric Control Plane] の各カテゴリにグループ化されます。カテゴリをフィルタ処理して、それぞれの KPI を表示できます。KPI 選択に基づいて、接続先、IP アドレス、タイプなどの到達可能性情報を含むテーブルを表示できます。コントロールプレーンの到達可能性ステータス、LISP、および Pub/Sub セッションのステータスチャートを表示するには、接続先の横にあるチェックボックスをオンにします。 （注） アップリンク ステータス チャートには、ファブリックアンダーレイの自動化を使用してファブリックをプロビジョニングする場合にのみデータが表示されます。

[Interfaces] タブ

[Interfaces] タブ
名前、説明、動作ステータス、リンク速度など、選択したインターフェイスに関する情報が含まれます。 特定のポートタイプに関する情報を表示するには、[PORT TYPE] タブを使用します。表示されるタブは、選択されたデバイスのタイプによって異なります。 • [Switches and Routers]：[All]、[Access]、[Auto]、[Routed]、および [Trunk] ポートタイプを表示します。 • [Cisco StackWise Virtual]：[All]、[Access]、[Auto]、[Routed]、[Trunk]、[SVL]、および [DAD] ポートタイプを表示します。 • [Cisco StackWise]：[All]、[Access]、[Auto]、[Routed]、[Trunk]、および [StackWisePort] ポートタイプを表示します。 • [Wireless Controller]：[All]、[Ethernet]、および [Virtual] ポートタイプを表示します。 テーブルにはソート可能な列が含まれています。ただし、新しいパラメータを使用して列をソートしようとすると、拡張インターフェイスリストが折りたたまれます。 （注） [Link Speed] データの列には、インターフェイスまたは物理ポートの速度容量が表示されます。ポートが特定の速度にネゴシエートされた場合は、ネゴシエートされた速度が表示されます。 特定の日時のインターフェイスに関する動作ステータスをチャート形式で表示するには、インターフェイスの横にあるチェックボックスをオンにします。最大 5 つのインターフェイスを選択できます。デフォルトでは、テーブル内の最初のインターフェイスが選択されます。 [Interface Availability]、[Utilization]、[Error]、および [Link Discard] チャートがテーブルの下に表示されます。 [Tx Utilization] チャートと [Rx Utilization] チャートの値が [Percentage] と [Rate（bps）] に入力されます。[Percentage] と [Rate] を切り替えて使用状況の値を表示できます。 （注） ワイヤレスコントローラの場合、リンク破棄情報が別のチャートに表示されることはありません。リンク破棄情報は、他のデータとともに [Traffic Summary] テーブルに表示されます。[Traffic Summary] テーブルのデータは、ワイヤレスコントローラ上の物理インターフェイスとイーサネットインターフェイスについてのみ表示されます。 デジタル オプティカル モニタリング（DOM）をサポートするインターフェイスを選択した場合、[デジタルオプティカルモニタリング（Digital Optical Monitoring）] エリアに次のメトリックが表示されます。 • [送信電力（Transmit Power）]：電力が不足している場合、信号が低下し、ビットエラー率が上昇する可能性があります。電力が過剰な場合、光ファイバ内での受信側の飽和や非線形効果を引き起こす可能性があります。 • [受信電力（Receive Power）]：低 RxPower は、光ファイバの減衰、汚れたコネクタ、配置の不一致など、ネットワークのパフォーマンス低下につながる問題を示している可能性があります。

[Interfaces] タブ
• [温度監視（Temperature Monitoring）]：温度データのモニタリングは、ネットワーク管理者がオーバーヒートを防ぐための修正措置を講じるのに役立ちます。オーバーヒートは、光コンポーネントに永久的な損傷を与え、ネットワーク障害を引き起こす可能性があります。また、データセンター環境における冷却システムの障害を特定することもできます。 • [電流監視（Current Monitoring）]：過剰な電流は、コンポーネント障害やショートなどの潜在的な問題を示している可能性があります。電流レベルが常に高い場合、デバイスのオーバーヒートや早期障害が発生する可能性があります。 • [電圧監視（Voltage Monitoring）]：電圧が低すぎると、デバイスの電力が不足する可能性があります。その結果、パフォーマンスが低下したり、動作に失敗したりする可能性があります。逆に、電圧が高すぎると、トランシーバの電子コンポーネントが損傷する可能性があります。

[PoE] タブ

このタブは、PoE 対応スイッチおよび AP で使用できます。

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

スイッチ

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

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

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

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

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

この表は次のタスクを実行することでカスタマイズできます。

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

AP

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

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

[StackWise] タブ

このタブは、Cisco StackWise に対して表示されます。

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

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

[RF] タブ

[RF] タブ

このタブは、AP とワイヤレスクライアントに対して表示されます。

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

  3 種類の無線を使用する AP（Cisco Catalyst 9130 AP など）を 17.2 以降を実行中のワイヤレスコントローラに接続した場合、デバイスで 3 種類すべての無線がサポートされ、[RF] タブに 3 種類の無線（Radio 0、Radio 1、および Radio 2）が表示されます。

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

  ただし、AP を新しいバージョンを実行するワイヤレスコントローラから古いバージョンを実行するワイヤレスコントローラに移行した場合（17.2 以降から 17.1 以前）は、最初に検出された 3 種類の無線（Radio 0、Radio 1、Radio 2）が [RF] タブにそのまま表示されます。

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

- **AP 360**の場合、 [RF] タブに次の情報が表示されます。

  [Radio 2]（6GHz 帯）、 [STANDARD POWER MODE] セクションには 、**自動周波数調整（AFC）統合**に関する情報が表示されます。これには、AFC ステータス、最終応答時刻、期限切れ、および AFC 定義ロケーションの詳細（ロケーションタイプ、緯度、経度など）が含まれます。

  [Neighbors and Rogues] セクションには、[Band]（2 GHz および 5 GHz 無線周波数）、[Type]（All、Neighbor、Rogue）および [RSSI Range]（0 ～ 100 dBm）フィルタが含まれています。選択されたフィルタに応じて、AP テーブルが更新されます。

  AP テーブルには、AP の識別子、無線、RSSI（dBm）、チャネル、タイプ、SSID などの詳細情報が含まれています。AP デバイス、無線、または他の値を検索するには、検索バーを使用します。

  （注）
  Catalyst Center は、5 分間隔で RSSI が最大の 10 台のネイバーのみを保存します。

  ⚙ をクリックしてメニューを開き、[Edit Table Column] を使用して特定の列を有効または無効にできます。CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。
- [KPI] ドロップダウンリストをクリックし、表示するチャートの横にあるチェックボックスをオンにします。チャートには、スループット、クライアント数、チャネル使用率、クライアント/パケット数別の上位 SSID などのさまざまな情報が表示されます。選択したチャートが [RF] タブに表示されます。
- 選択されたフィルタに応じて、Wi-Fi Analyzer のグラフがテーブルの下に表示されます。Wi-Fi グラフでは、AP 360 タイムラインスライダの上部で選択された時間範囲について、集計された KPI の合計値と平均値の要約が示されます。

[RF] タブ

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

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

[Virtual Network] タブ

このタブは、SD-Access ファブリックで使用できます。

KPI は、[VN Services] カテゴリと [Fabric Control plane] カテゴリにグループ化されます。カテゴリを選択して、[Dynamic Default Border]、[Remote Internet Availability]、[Multicast (external RP)]、[Pub-Sub Session Status] の各 KPI を表示できます。これらのカテゴリをフィルタ処理して、接続先、IP アドレス、タイプなどの到達可能性情報を含むテーブルを表示できます。コントロールプレーンの到達可能性ステータス、LISP、およびPub/Subセッションのステータスチャートなどのステータスを表示するには、接続先の横にあるチェックボックスをオンにします。

[Transits and Peers Network] タブ

このタブは、SD-Access ファブリックで使用できます。

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

[Mesh] タブ

このタブは、メッシュ AP で使用できます。

[Mesh] タブには、デバイスのメッシュロール、メッシュプロファイル、ダウンストリーム MAP、メッシュ バックホール チャネル、RAP へのホップ、ブリッジグループ名、およびバックホール インターフェイスが表示されます。

また、無線固有の KPI である [Current Channel]、[Extended Channel（s）]、[Mode]、[RF Profile]、[Band]、[Tx Power]、[Clean Air Status]、[Admin State]、および [Current Channel Width] も表示されます。

[高度な分析（Advanced Analytics）] タブ

このタブは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラおよびワイヤレス対応 Catalyst スイッチ（eCA）で使用できます。

[高度な分析（Advanced Analytics）] タブには、次のようなプロセスレベルの詳細なテレメトリ KPI が表示されます。

- [プロセスごとのCPU使用率（%）（Per-Process CPU Utilization（%））]：選択した時間範囲において、ワイヤレスコントローラ上で実行されている各プロセスが消費した CPU リソースの割合を表示します。この KPI により、デバイスのパフォーマンスやクライアント エクスペリエンスに影響を与える可能性のある、過剰な CPU サイクルを消費しているプロセスを特定できます。
- [プロセスごとのメモリ使用率（%）（Per Process Memory Utilization（%））]：選択した時間範囲において、ワイヤレスコントローラ上で実行されている各プロセスが消費したメモリリソースの割合を表示します。この KPI により、メモリ枯渇やデバイスの不安定化につながる可能性のある異常なメモリ消費があるプロセスを特定できます。
- [クライアント削除カウント（Client Delete Count）]：選択した時間範囲における WNCD プロセス インスタンスごとのクライアント削除イベントの数を表示します。クライアントの削除は、関連付け解除、認証解除、セッションタイムアウト、または管理アクションが原因でクライアントセッションがコントローラから削除される場合に発生します。この KPI により、異常なクライアント チャーン パターンを特定できます。
- [KPI]：[KPI] ドロップダウンをクリックして、使用可能な高度な分析 KPI を表示して選択します。表示する KPI の横にあるチェックボックスをオンにし、[適用（Apply）] をクリックします。KPI は一度に複数選択できます。使用可能な KPI は次のとおりです。AP カウント、クライアント数、バンドごとのクライアント数、クライアント状態統計情報、クライアント関連付け統計情報、クライアントモビリティ統計情報、クライアントローミング統計情報、トラフィック、トラフィックエラー、データプレーン - パント、データプレーン - ソフトウェアドロップ、データプレーン - ハードウェアドロップ、mDNS 統計情報、AAA 統計情報 - 認証、AAA 統計情報 - 許可、AAA 統計情報 - アカウンティング、AAA 統計情報 - RADIUS
- [クライアント数（Client Count）]：選択した時間範囲において、ワイヤレスコントローラ上の各 WNCD プロセスインスタンスに現在関連付けられているワイヤレスクライアントの総数を表示します。この KPI により、WNCD プロセス間でのクライアント負荷分散を可視化でき、負荷の偏りを特定できます。

タイムスライダを使用して過去 3 時間、24 時間、または 7 日間の KPI データを表示する場合は、次の点に注意してください。

- 7 日間のタイムスライダは 60 分の時間枠を使用します。60 分の時間枠の開始時刻に基づいてデータを報告し、その 60 分の間隔内の最新のデータを返します。
- 3 時間および 24 時間のタイムスライダは、10 分の時間枠を使用します。10 分の時間枠の開始時刻に基づいてデータを報告し、その 10 分の間隔内の最新のデータを返します。

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

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

ステップ 17 [サイトの表示（View Site）] ドロップダウンリストから、AP 無線を比較するフロアを選択します。

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

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

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

ステップ 19 フロアマップ上の AP アイコンをクリックします。

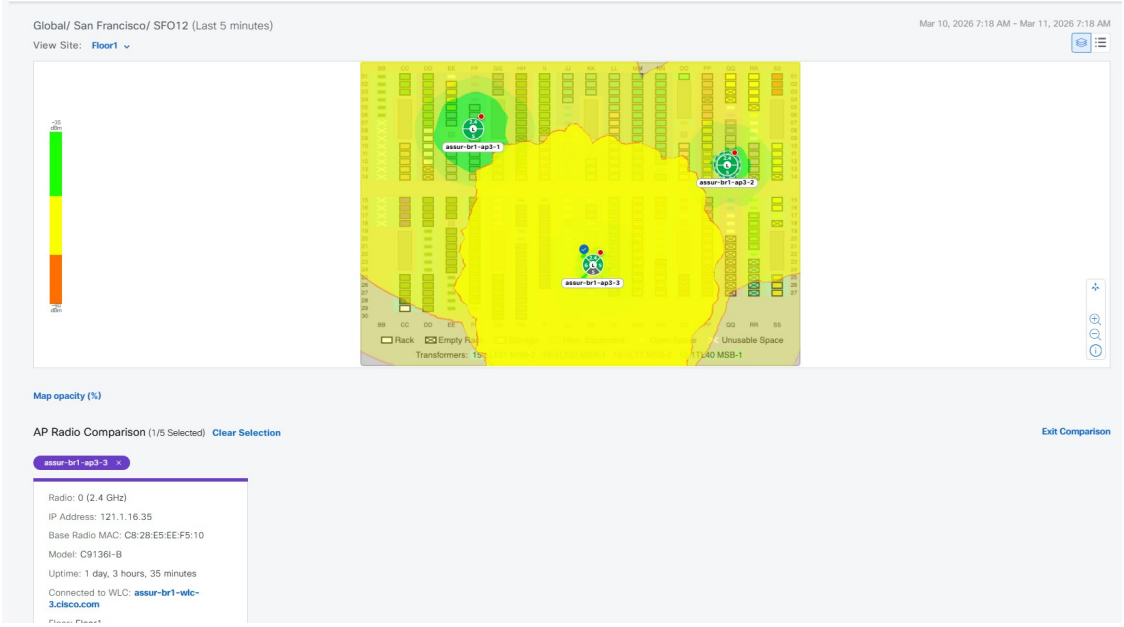
比較する無線を選択または選択解除するためのダイアログボックスが表示されます。

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

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

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

図 *11 : AP* 無線比較マップビュー



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

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

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

次の KPI から選択できます。

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

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

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

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

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

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

Cisco StackWise Virtual と制限事項について

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

StackWise Virtual 対応デバイス

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

デバイス	サポート対象 IOS-XE ソフトウェアの最小バージョン
Cisco Catalyst 9300 シリーズ スイッチ	16.11 +
Cisco Catalyst 9400 シリーズ スイッチ	16.11 +
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、次の手順を実行します。

  1. インベントリから 両方のスイッチを削除します。ネットワークデバイスの削除 （77 ページ）を参照してください。
  2. StackWise Virtual を設定します（2 つのスイッチを 1 つの仮想スイッチに設定します）。
  3. デバイスを検出します。IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 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、次の手順を実行します。

  1. 2 番目のスイッチで別の IP アドレスを設定します。

2. デバイスをもう一度検出します。IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 ページ）を参照してください。

Cisco StackWise と制限事項について

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

Cisco StackWise 対応デバイス

Cisco StackWise をサポートするデバイスを次に示します。

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

Cisco StackWise の制限事項

Cisco StackWise には、次の既知の制限事項があります。

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

ネットワークデバイスの正常性スコアの設定

ネットワークデバイスの正常性スコアを設定するには、次の手順を実行します。KPI のしきい値を変更し、計算に含める KPI を指定すると、ネットワークデバイスの正常性スコアの計算をカスタマイズできます。正常性スコア設定は、サードパーティ製デバイスには適用されません。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **[正常性（Health）]** > **[正常性スコア設定（Health Score Settings）]**。

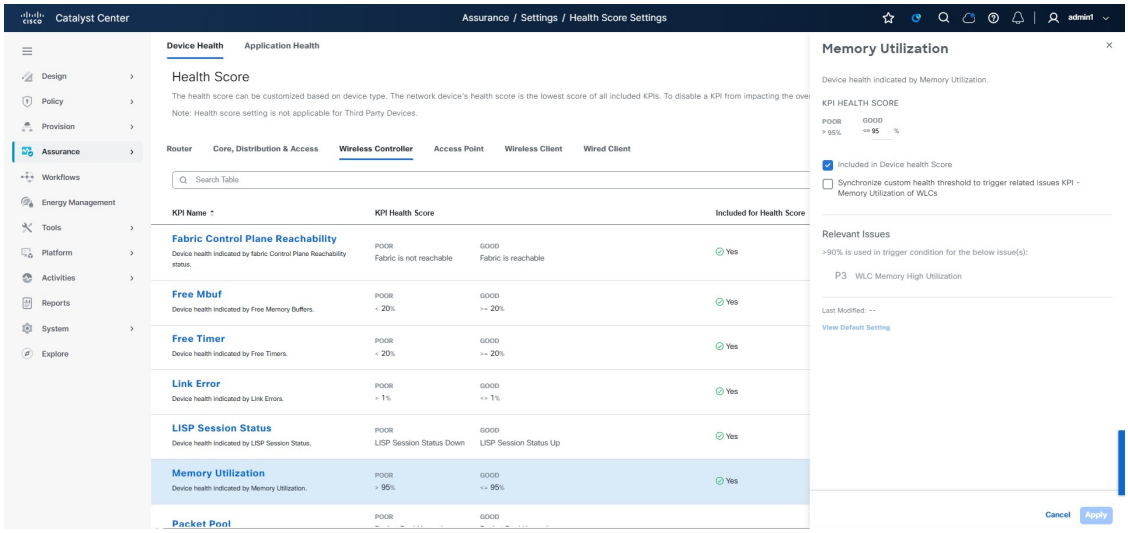
[Health Score] ウィンドウが表示されます。

ステップ 2 [デバイスの正常性（Device Health）] カテゴリをクリックして、正常性スコアの計算設定をカスタマイズします。

画面に、重要業績評価指標（KPI）テーブルが表示されます。このテーブルには、[KPI名（KPI Name）]、[KPI正常性スコア（KPI Health Score）]、[正常性スコアに含まれる（Included for Health Score）]、[現在の設定（Current Setting）]、および [最終更新日（Last Modified）] が含まれます。

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

KPI のスライドインペインが表示されます。



ステップ 4 KPI の正常性スコアを次のように設定します。

a) 定量的 KPI しきい値の場合は、良好な正常性スコアと見なすしきい値をカスタマイズできます。

b) 正常性と問題の設定の間で共通の KPI しきい値を同期または同期解除するには、[Synced] トグルボタンを使用します。正常性の設定ページまたは問題の設定ページから同期した場合、逆方向にも同期されます。これはワイヤレスコントローラにのみ適用されます。

c) 正常性スコアの計算から KPI を削除するには、[Included in Device health Score] チェックボックスをオフにします。

注：[同期（Synced）] トグルボタンを使用した正常性の設定と問題の設定間の共通 KPI しきい値の同期は、ワイヤレスコントローラ デバイス カテゴリにのみ適用されます。

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

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

ステップ 5 [Apply] をクリックします。

確認用のダイアログボックスが表示されます。

ファブリックデバイスの SNMP コレクタメトリックの有効化

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

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Data Platform]**。

ステップ 2 [Collectors] をクリックします。

コレクタのリストが表示されます。

ステップ 3 [COLLECTOR-SNMP] をクリックします。

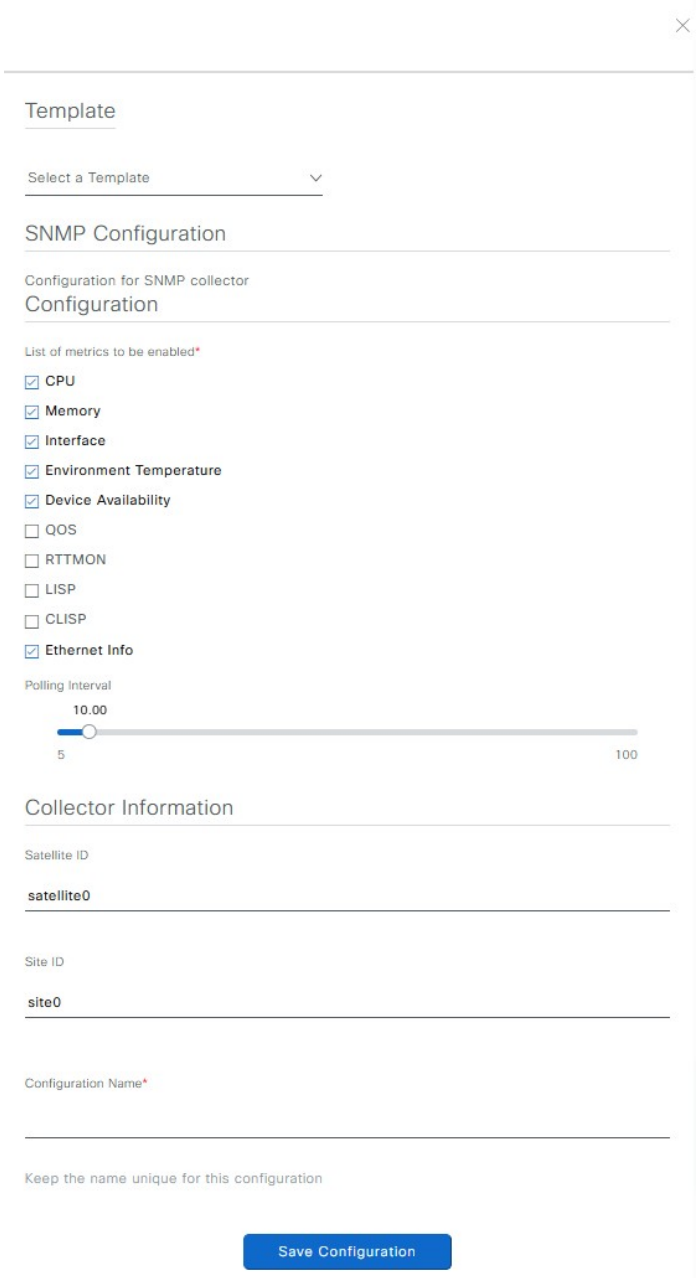
[COLLECTOR-SNMP] ウィンドウが開きます。

ステップ 4 **[+ Add]** をクリックします。

[SNMP Configuration] ダイアログ ボックスが開きます。

ステップ 5 [テンプレートの選択（Select a Template）] ドロップダウン リストからテンプレートを選択します。

図 *12 : SNMP* の設定



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

ステップ 7 [Save Configuration] をクリックします。

ネットワークの正常性スコアと KPI メトリックについて

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

ネットワークの正常性スコア

ネットワークの正常性スコアは、健全なネットワークデバイス（正常性スコアが 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（メンテナンスモードのデバイスを除く）。スコアは 5 分ごとに計算されます。

次に例を示します。

90%（正常性スコア）=90（正常性スコア 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 - メンテナンスモードのデバイス）

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（メンテナンスモードのデバイスを除く）。スコアは 5 分ごとに計算されます。

次に例を示します。

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 - メンテナンスモードのデバイス）

個別のデバイス正常性スコア

個別のデバイス正常性スコアは、KPI メトリックの正常性スコア（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）の中での最小スコアです。KPI メトリックスコアは、KPI ごとに定義されるしきい値に基づきます。

デバイス正常性スコア = MIN（システムの正常性、データプレーンの接続性、コントロールプレーンの接続性）

デバイスのタイプに応じて、メトリックは変わります。

システム ヘルス	
デバイス タイプ	**説明**
スイッチ（アクセスおよび配信）	CPU 使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。

システム ヘルス	
デバイス タイプ	**説明**
ワイヤレス	次のシステムモニターリングメトリックが含まれます。 • ワイヤレスコントローラの場合、メモリ使用率、空きタイマー、空き Mbuf が含まれます。 • AP については、CPU 使用率とメモリ使用率が含まれます。
ルータ	CPU使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。
ファブリック	CPU使用率やメモリ使用率などのシステムモニターリング メトリックが含まれます。

データプレーンの接続性	
デバイス タイプ	**説明**
スイッチ（アクセスおよび配信）	リンクエラーやリンクステータスなどのメトリックが含まれます。 スイッチの場合、デバイス間リンク可用性メトリックは、物理スタックポート、ネットワークデバイスに接続されたリンク、およびファブリックエッジ側のポートチャネルをカウントします。
ワイヤレス	次のメトリックが含まれます。 • ワイヤレスコントローラについては、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については、インターフェイス、ノイズ、電波品質、無線使用状況などの RF メトリックが含まれます。
ルータ	リンクエラーなどのメトリックが含まれます。

コントロールプレーンの接続性	
デバイス タイプ	**説明**
ワイヤレス	次の KPI が含まれます。 • ワイヤレスコントローラの場合、コントロール プレーン ノード サーバーへの接続性が含まれます。 • ファブリックデバイスの場合、コントロールプレーンノードへの接続性などのメトリックが含まれます。

スイッチの正常性スコア

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。

（注） メンテナンスモードのデバイスは、デバイスのヘルススコアの計算に含まれません。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 95 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 95 パーセント以上の場合、スコアは 1 です。
メモリ使用率	• メモリ使用率が 95 パーセント以下の場合、スコアは 10 です。 • メモリ使用率が 95 パーセント以上の場合、スコアは 1 です。
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）を接続するトポロジー型リンクを指します。Catalyst Center 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、スコアは 8 です。すべてのリンクがダウンしている場合、スコアは 1 です。それ以外の場合、スコアは 10 です。
リンク破棄	リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、APなど）を接続するトポロジー型リンクを指します。Catalyst Center 物理インフラストラクチャリンクにパケットドロップ（廃棄）がある場合、スコアは 8 です。すべてのリンクで破棄が発生した場合、スコアは 1 です。それ以外の場合、スコアは 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 などの、Catalyst Center 管理型デバイス）を接続するトポロジー型リンクを指します。 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、スコアは 8 です。すべてのインターフェイスがダウンしている場合、スコアは 1 です。それ以外の場合、スコアは 10 です。

パラメータ	スコアの計算
デバイス間リンク可用性	**デバイス間リンクの可用性** KPIは、ネットワークデバイス間の接続ステータスをモニターします。 • [良好（GOOD）]：このステータスは、すべてのデバイス間リンクが稼働している場合にトリガーされます。 . • [不良（POOR）]：このステータスは、すべてのデバイス間リンクがダウンしている場合にトリガーされます。
コントロールプレーンノードへの到達可能性。ファブリックデバイスのみ（エッジおよびボーダー）	• コントロール プレーン ノードが到達可能な場合、スコアは 10 です。 • コントロール プレーン ノードが到達不能な場合、スコアは 1 です。 （注） • ファブリックネットワークに 1 つを超える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。それ以外の場合、スコアは 1 です。 • CP を含む連結型エッジまたはボーダーの場合、CP への到達可能性は考慮されません。 • ヘルス スコアをファブリック デバイス向けに正しく入力するには、SNMP コレクタ メトリックを有効にします。ファブリックデバイスの SNMP コレクタメトリックの有効化 （141 ページ）を参照してください。

ルータの正常性スコア

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。

（注） メンテナンスモードのデバイスは、デバイスのヘルススコアの計算に含まれません。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 95 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 95 パーセント以上の場合、スコアは 1 です。
メモリ使用率	• メモリ使用率が 95 パーセント以下の場合、スコアは 10 です。 • メモリ使用率が 95 パーセント以上の場合、スコアは 1 です。

パラメータ	スコアの計算
WAN 接続	• WAN 接続がダウンした場合、スコアは 1 です。 • WAN 接続がアップしている場合、スコアは 10 です。
リンクエラー	リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、AP など）を接続するトポロジー型リンクを指します。Catalyst Center 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、スコアは 8 です。すべてのリンクがダウンしている場合、スコアは 1 です。それ以外の場合、スコアは 10 です。
リンク破棄	リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、APなど）を接続するトポロジー型リンクを指します。Catalyst Center 物理インフラストラクチャリンクにパケットドロップ（廃棄）がある場合、スコアは 8 です。すべてのリンクで破棄が発生した場合、スコアは 1 です。それ以外の場合、スコアは 10 です。
デバイス間リンク可用性	**デバイス間リンクの可用性** KPIは、ネットワークデバイス間の接続ステータスをモニターします。 • [良好（GOOD）]：このステータスは、すべてのデバイス間リンクが稼働している場合にトリガーされます。 . • [不良（POOR）]：このステータスは、すべてのデバイス間リンクがダウンしている場合にトリガーされます。
コントロールプレーンノードへの到達可能性。ファブリックデバイスのみ（エッジおよびボーダー）	• コントロール プレーン ノードが到達可能な場合、スコアは 10 です。 • コントロール プレーン ノードが到達不能な場合、スコアは 1 です。 （注） • ファブリックネットワークに 1 つを超える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。それ以外の場合、スコアは 1 です。 • CP を含む連結型エッジまたはボーダーの場合、CP への到達可能性は考慮されません。 • ヘルス スコアをファブリック デバイス向けに正しく入力するには、SNMP コレクタ メトリックを有効にします。ファブリックデバイスの SNMP コレクタメトリックの有効化 （141 ページ）を参照してください。

AP の正常性スコア

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。

（注） メンテナンスモードのデバイスは、デバイスのヘルススコアの計算に含まれません。

パラメータ	スコアの計算
CPU 使用率	• CPU 使用率が 90 パーセント以下の場合、スコアは 10 です。 • CPU 使用率が 90 パーセント以上の場合、スコアは 1 です。
メモリ使用率	• メモリ使用率が 90 パーセント未満の場合、スコアは 10 です。 • 利用可能メモリ率が 90 パーセント以上の場合、スコアは 1 です。
無線使用率スコア	スコアは無線ごとに個別に計算され、すべての無線で平均されて全体的な使用率スコアが得られます。 • 無線使用率が 70 パーセント未満の場合、スコアは 10 です。 • 無線使用率が 70 パーセント以上の場合、スコアは 1 です。
干渉スコア	スコアは無線ごとに個別に計算され、すべての無線で平均されて全体的な干渉スコアが得られます。 2.4 GHz 無線の場合： • 干渉が 50 パーセント以下の場合、スコアは 10 です。 • 干渉が 50 パーセントを超える場合、スコアは 1 です。 5 GHz 無線または 6 GHz 無線の場合： • 干渉が 20 パーセント以下の場合、スコアは 10 です。 • 干渉が 20 パーセントを超える場合、スコアは 1 です。

パラメータ	スコアの計算
RF ノイズスコア	スコアは無線ごとに個別に計算され、すべての無線で平均されて全体的なノイズスコアが得られます。 2.4 GHz 無線の場合： • RF ノイズが -81 dBm 未満の場合、スコアは 10 です。 • RF ノイズが -81 dBm 以上の場合、スコアは 1 です。 5 GHz 無線または 6 GHz 無線の場合： • RF ノイズが -83 dBm 未満の場合、スコアは 10 です。 • RF ノイズが -83 dBm 以上の場合、スコアは 1 です。
電波品質スコア	スコアは無線ごとに個別に計算され、すべての無線で平均されて全体的な電波品質スコアが得られます。 2.4 GHz 無線の場合： • 電波品質が 60 パーセント以上の場合、スコアは 10 です。 • 電波品質が 60 パーセント未満の場合、スコアは 1 です。 5 GHz 無線または 6 GHz 無線の場合： • 電波品質が 75 パーセント以上の場合、スコアは 10 です。 • 電波品質が 75 パーセント未満の場合、スコアは 1 です。
リンクエラースコア	スコアはイーサネットインターフェイスごとに個別に計算され、すべてのイーサネット インターフェイスで平均されて、全体的なリンクエラースコアが得られます。 • 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。

ワイヤレスコントローラの正常性スコア

ワイヤレスコントローラの正常性スコアは、次のパラメータの最小サブスコアです。

（注） メンテナンスモードのデバイスは、デバイスのヘルススコアの計算に含まれません。

パラメータ	スコアの計算
メモリ使用率	• メモリ使用率が 90 パーセント未満の場合、スコアは 10 です。 • 利用可能メモリ率が 90 パーセント以上の場合、スコアは 1 です。
空きタイマースコア	• 空きタイマーの数が 20 パーセント以上の場合、スコアは 10 です。 • 空きタイマーの数が 20 パーセント以下の場合、スコアは 1 です。
空きメモリバッファ（**MBufs**）	• 空きメモリ バッファの数が 20 パーセント以上の場合、スコアは 10 です。 • 空きメモリ バッファの数が 20 パーセント以下の場合、スコアは 1 です。
作業キュー要素（**WQE**）のプールスコア	• WQE プールが WQE プールのしきい値より大きい場合、スコアは 10 です。 • WQE プールが WQE プールのしきい値と同じレベルかこれより低い場合、スコアは 1 です。
パケットプール	• パケット プールがパケット プールのしきい値より大きい場合、スコアは 10 です。 • パケット プールがパケット プールのしきい値と同じレベルかこれより低い場合、スコアは 1 です。
Link Errors	• リンク エラーが 1 パーセント以下の場合、スコアは 10 です。 • リンク エラーが 1 パーセント以上の場合、スコアは 1 です。
コントロールプレーンノードへの接続 - ファブリック ワイヤレス コントローラのみ	• コントロール プレーン ノードが到達可能な場合、スコアは良好です。 • コントロール プレーン ノードが到達不能な場合、スコアは不良です。 （注） ファブリックネットワークに 1 つ以上のコントロールプレーンノードが存在し、すべてのコントロールプレーンノードに到達可能な場合、スコアは 10 です。そうでない場合、スコアは 1 です。

ネットワークの正常性スコアと KPI メトリックに対するメンテナンス モードの影響

ネットワークデバイス（ルータ、スイッチ、ワイヤレスコントローラ、またはアクセスポイント）がメンテナンスモードになると、そのクライアントもメンテナンスモードになります。たとえば、シスコ ワイヤレス コントローラ をメンテナンスモードにすると、ワイヤレスコントローラ に関連付けられている AP もすべてメンテナンスモードになります。Catalyst Center は、デバイスが管理アクションとして、またはデバイスとの関連付けの結果として、メンテナンスモードになったかに関係なく、メンテナンスモードのすべてのデバイスを同じように扱います。

ネットワークの正常性スコアと KPI メトリックには、メンテナンスモードのデバイスは含まれません。メンテナンスモードの間はデバイスのメトリックが信頼できないか利用できない可能性があるためです。

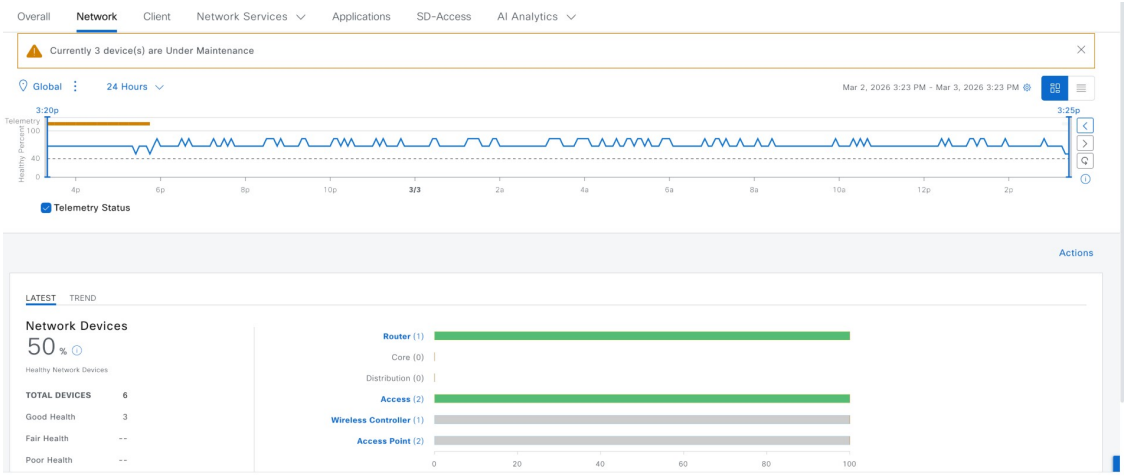
デバイスがメンテナンスモードの場合、Catalyst Center は次のことを行いません。

- 正常性データの収集
- 統計情報の収集
- デバイスの問題の報告

正常性および KPI の計算では、メンテナンスデータはスキップされます。ただし、デバイスの総数を示すレポートには、メンテナンスモードのデバイスも含まれます。

[Assurance] > **[Health]** > **[Network]** ウィンドウでデバイスがメンテナンスモードのときにネットワークの正常性スコアと KPI メトリックにアクセスすると、Catalyst Center にデバイスがメンテナンスモードであることを示すバナーが表示されます。さらに、メンテナンス期間の開始時刻と終了時刻が [device 360] ウィンドウに表示され、システムステータスログにイベントとして記録されます。ダッシュボードでは、メンテナンスモードのデバイスでフィルタリングできます。

図 *13* : メンテナンスバナー付きの *[Device 360]*



Catalyst Center は、メンテナンスモードのデバイスに対して次の操作の実行を継続します。

- 関連するイベントが引き続き生成され、メンテナンスモード中にイベントビューアに表示できます。
- イメージのアップグレード、一括プロビジョニングなどのメンテナンス関連の操作は、引き続きイベントをトリガーします。
- アシュアランスの可用性レポートは影響を受けません。
- トポロジは影響を受けません。

RF の計算について

チャネル使用率（無線使用率とも呼ばれます）は、Catalyst Center が Wi-Fi と非 Wi-Fi で検出する合計チャネル使用率です。

Catalyst Center は、次の式で AP 無線干渉を導出します。

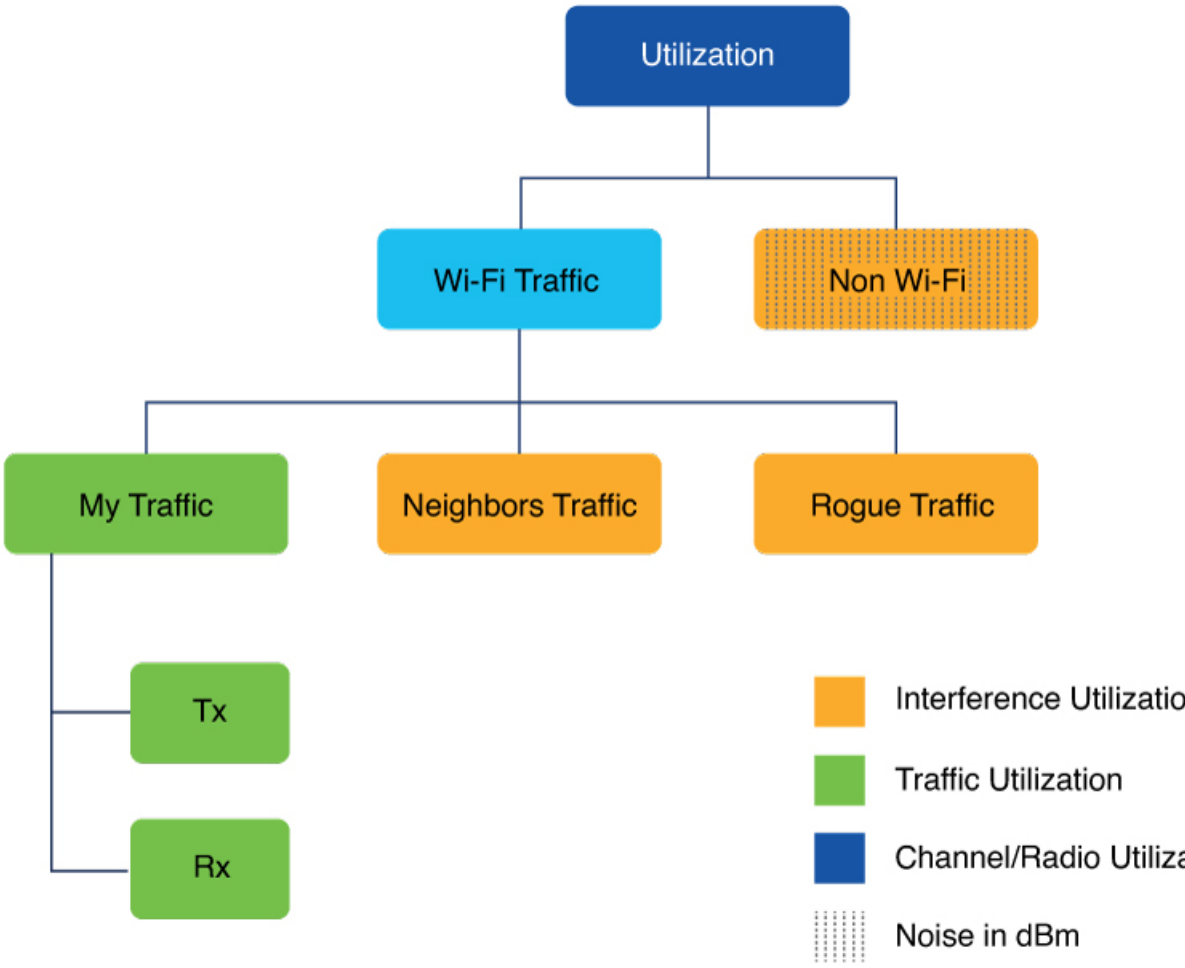
干渉 % = チャネル使用率 % – Rx トラフィック % – Tx トラフィック %

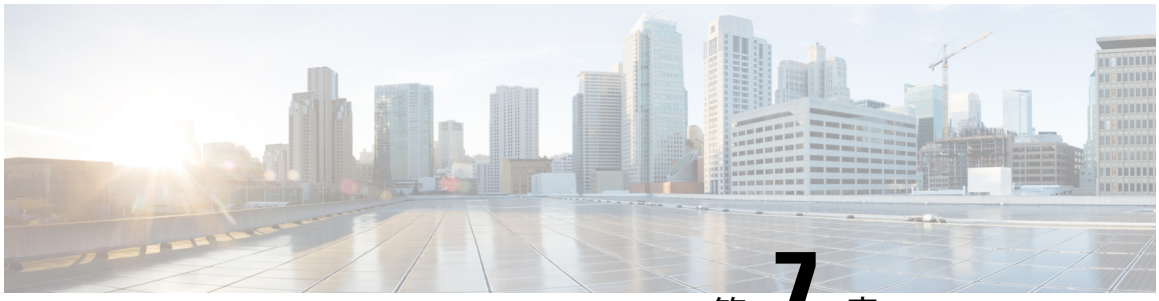
AP 干渉のこの定義には、不正トラフィック、ネイバートラフィック、および非 Wi-Fi トラフィックによって引き起こされる干渉が含まれます。

非 Wi-Fi 干渉（ノイズとも呼ばれる）は、% および dBm 単位で測定できます。

次の図は、AP 無線のさまざまなパラメータ間の関係を示しています。

図 *14 : Catalyst Center* の *RF* パラメータ





第 7 章

クライアント正常性のモニターとトラブルシューティング

- リモート LAN サポート （155 ページ）
- ワークグループ ブリッジ クライアントのサポート （155 ページ）
- すべてのクライアントデバイスの正常性のモニターとトラブルシューティング （156 ページ）
- クライアントデバイスの正常性のモニターとトラブルシューティング （173 ページ）
- クライアント追跡 （186 ページ）
- 除外クライアントの設定 （191 ページ）
- クライアントの正常性スコアと KPI メトリックについて （192 ページ）

リモート LAN サポート

Assurance は、リモート LAN（RLAN）または RLAN クライアントをサポートしていません。[Client 360] ウィンドウで、RLAN クライアントのデータが欠落しているか、不正確な可能性があります。[AP 360] ウィンドウで、RLAN クライアントを使用する AP の場合、RLAN ポートに RLAN 固有の情報は表示されません。AP および ワイヤレスコントローラ 上の RLAN クライアントは引き続き正常に動作しますが、Assurance のウィンドウでは RLAN クライアントは表示されなくなることに注意してください。詳細については、「*Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*」の「Remote LANs」を参照してください。

ワークグループ ブリッジ クライアントのサポート

Assurance はワークグループブリッジ（WGB）クライアントをサポートしていません。[Client 360] ウィンドウで、WGB クライアントのデータが欠落しているか、不正確な可能性があります。WGB 自体は Assurance 内にワイヤレスクライアントとして表示され、[Client 360] ウィンドウが表示されます。AP および ワイヤレスコントローラ 上の WGB および WGB クライアントは引き続き正常に動作しますが、Assurance ウィンドウでは WGB クライアントは表示されないことに注意してください。詳細については、「*Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*」の「Workgroup Bridges」を参照してください。

すべてのクライアントデバイスの正常性のモニターとトラブルシューティング

クライアントが、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。Catalyst Center は、有線クライアントと無線クライアントの両方をサポートしています。

Assurance は、ユーザーのアクセス範囲を制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。[Client Health] ダッシュボードを使用している間は、サイト、有線クライアント、および無線クライアントにアクセスできるようにしておく必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

この手順を使用して、すべての有線およびワイヤレスのクライアントの正常性の概要を把握し、対処する必要がある潜在的な問題があるかどうかを判断します。

Assurance機械学習（ML）アルゴリズムを使用してネットワーク内の動作パターンを抽出し、トレンドを予測します。これらのトレンドは、[Client Onboarding Time] ダッシュレットおよび [Client Count Per SSID] ダッシュレットに基準として表示されます。

（注） HA フェールオーバーが発生した場合、クライアントの正常性データの表示に 1 時間かかることがあります。

手順

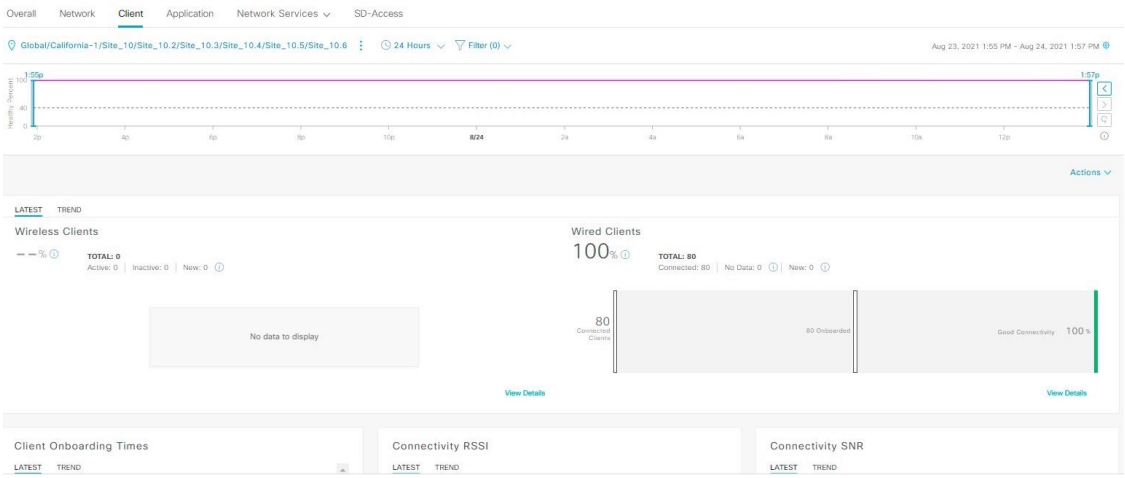
ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

図 *15 : [Client Health]* ダッシュボード



ステップ 3 次の機能には [Client Health] ダッシュボードの上部のメニューバーを使用します。

[Client Health] ダッシュボードの上部のメニューバー	
アイテム	説明
Global [Location] ペイン	クリックすると、次のアイコンが表示されます。 • 上部のメニューバーで場所オプション（Global）をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 ネットワーク階層からフロアを選択することはできません。 • ロケーションアイコンの横にある をクリックして、以下を切り替えます。 • [サイトマップ（Site Map）]：ネットワーク階層の地理的ビューを提供します。 • [サイトテーブル（Site Table）]：正常性スコアやデバイス数を含む、すべてのサイトのリストベースビューを提供します。 • トグルボタンをクリックすると、ネットワークのサイトと建物がリスト形式で表示されます。 ドロップダウンリストをクリックすると、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [建物/屋外エリアの表示（Building/Outdoor Area view）]：リストを建物レベルで並べ替えます。[Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • Export をクリックしてデバイス情報を CSV ファイルにエクスポートします。 • トグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。 • マップまたはテーブルビューを非表示にするには、閉じるアイコンをクリックします。

[Client Health] ダッシュボードの上部のメニューバー	
アイテム	説明
24 Hours **[Time Range] の設定**	上部のメニューバーにある時間範囲設定（ 24 Hours ）をクリックして、ダッシュボードに表示するデータの時間範囲を指定します。 **1.** ドロップダウンメニューで、[3 hours]、[24 hours]、[7 days] のいずれかの時間範囲を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。
[Filter] アイコン	[SSID] および [Band] オプションが含まれます。[SSID] および [Band] の横にあるチェックボックスをオンにしてドロップダウンリストでSSIDおよび帯域周波数選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。 （注） 複数の SSID を選択できます。たとえば、Class 1 の SSID と Class 2 の SSID を選択した場合、ダッシュボードには、Class 1 の SSID と Class 2 の 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	クライアントダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビューページを表示し、[Save] をクリックします。 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 （434 ページ）およびカスタムダッシュボードの作成 （431 ページ）を参照してください。

ステップ 4 **タイムラインスライダ**を使用すると、正常なクライアント比率をより詳細な時間範囲で表示できます。

タイムライン内でマウスのカーソルを合わせると、特定の時点のワイヤレスおよび有線クライアントの正常性スコアのパーセンテージが表示されます。

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、ダッシュボード ダッシュレットに表示されるクライアントデータのコンテキストが設定されます。

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

点線の横線は、正常なクライアントのしきい値を表します。デフォルトでは、40% に設定されています。

しきい値を変更するには、次の手順を実行します。

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

（注） [Client Summary] の [Health Score] が赤色で表示される場合、カスタムしきい値の変更に影響が出ます。カスタムしきい値によって、正常または異常なデバイスの数が変わることはありません。

ステップ 5 次の機能には [Client Health Summary] ダッシュレットを使用します。

[Client Health Summary] ダッシュレット	
アイテム	説明
[Client Health Summary] エリア	次の 2 つのタブがあります。 • [Latest]：デフォルトで表示されます。次のオプションがあります。 • [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。クライアントの正常性スコア （192 ページ） を参照してください。 • [Total Devices]：クライアントの合計数、およびアクティブ、非アクティブ、新しいクライアントの数が表示されます。Cisco Catalyst Center は、5 分間の正常性スコア計算ウィンドウ内のアクティビティに基づいて、アクティブなクライアント、非アクティブなクライアント、および新しいクライアントを次のように定義します。 • [Active]：正常にオンボードし、データしきい値を満たすのに十分なデータを送信しているクライアント、正常にオンボードしたが切断されたクライアント、オンボードを試行したが失敗したクライアント、オンボードを試行したが除外されたクライアント。 • [Inactive]：データしきい値を満たすのに十分なデータを送信していないクライアント。ユーザーアイドル タイムアウト期間が経過すると、ワイヤレスコントローラは非アクティブなクライアントの認証を解除します。 • [New]：オンボーディング中のクライアント。これらのクライアントの正常性スコアは、次回の 5 分間の計算ウィンドウに含まれます。 • [Charts]：このスナップショットビューチャートでは、過去 5 分間でオンボードに成功または失敗したクライアントの分布が示されます。次に、正常にオンボードしたクライアントの数を使用して、このチャートでは接続性が良好または中程度のクライアントの割合が示されます。 • [Trend]：一定の期間にわたるクライアントの健全性を示すトレンドチャートを表示します。 オンボードに失敗したクライアントの場合、オンボーディング失敗の理由が示されます。例には、AAA、DHCP、およびその他が含まれます。 チャート内の色は、クライアントデバイスの正常性を示しています。 ●：クライアントデバイスが不適切です。ヘルス スコアの範囲は 1 ～ 3 です。 ●：クライアントデバイスが適切です。ヘルス スコアの範囲は 4 ～ 7 です。 ●：クライアントデバイスが良好です。ヘルス スコアの範囲は 8 ～ 10 です。 ●：クライアントデバイスが非アクティブです。ヘルス スコアは 0 です。

[Client Health Summary] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 有線クライアントと無線クライアントの両方について、[LATEST] タブと [TREND]タブを表示できます。 • [LATEST]タブ：オンボーディングアクティビティによってクライアントの正常性を要約する棒グラフが表示されます。 • [TREND]タブ：クライアントの正常性を経時的に追跡するための 2 つのチャートが表示されます。 • [Radial Bar chart]：オンボーディングに失敗したクライアントの分布と、オンボーディング失敗の理由が表示されます。 • [Line chart]：オンボーディングの失敗が 5 分単位で表示されます。 （注） 有線クライアントおよび無線クライアントで AAA 管理に Cisco ISE が使用されていて、認証に失敗すると、上位のオンボーディング AAA および Cisco ISE の失敗理由を [TREND] タブで確認できます。AAA 失敗情報は ワイヤレスコントローラ からのものであり、Cisco ISE 情報は Cisco ISE からのものです。 • 有線クライアントの場合は、折れ線グラフをクリックしてから [Top Authentication Failure Reasons] をクリックすると、失敗の理由の詳細が表示されます。 • 無線クライアントの場合は、放射状棒グラフの横にある [AAA] をクリックすると、失敗の理由の詳細が表示されます。 無線クライアントまたは有線クライアントのタブでは、次の操作を行うことができます。 • チャート内のセグメントをクリックすると、特定のセグメントに関する詳細が表示されます。 • チャートの下に表示されているデータタイプカテゴリをクリックすると、テーブルデータをフィルタ処理できます。 • テーブル内で、検索バーを使用して特定のデータを検索できます。 • テーブル内で、デバイスの識別子または名前をクリックすると、関連する [Client 360] ウィンドウまたは [Device 360] ウィンドウに移動します。

ステップ 6 ネットワーク内のクライアントの特定の KPI とメトリックを表示するには、KPI ダッシュレットを使用します。[KPI] ダッシュレットについて、次の表で説明します。

（注） チャートデータは 5 分ごとに更新されます。

[Client Onboarding Times] ダッシュレット	
アイテム	**説明**
[Client Onboarding Times] チャート	すべてのサイトまたは選択したサイトでの、すべてのクライアントオンボード試行の時系列分布。このダッシュレットには、10秒以内にオンボードに成功したクライアントの割合が示されます。クライアントのオンボーディングは、関連付け、認証、アドレッシング、Web 認証、および DNS の各フェーズを対象としています。 チャートには、次の 2 種類があります。 • [Latest]：デフォルトで表示されます。このスナップショットビューチャートでは、過去 5 分間オンボードに成功または失敗したクライアントの分布が示されます。次に、正常にオンボードしたクライアントの数を使用して、このチャートでは接続性が良好または中程度のクライアントの割合が示されます。 • [Trend]：[Client Count] タブと [Baseline] タブがあります。[Baseline] タブをクリックすると、機械学習によって生成されるオンボーディング時間のチャートが表示されます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics の設定 （95 ページ）およびCisco AI Network Analytics の概要 （7 ページ）を参照してください。 **重要** 基準チャートを表示するには、[Filter] のオプションでサイトと SSID を選択する必要があります。 基準チャートの詳細は、異なる色で表示されます。 • **緑色のバンド**：予測基準値。 • **青色の実線**：実際の値。 オンボードに失敗したクライアントの場合、オンボーディング失敗の理由が示されます。例には、AAA、DHCP、およびその他が含まれます。

[Client Onboarding Times] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 • 左側のペインには、[Overall]、[Association]、[Authentication]、[DHCP] タブが表示されます。タブをクリックすると、右側のペインにチャートが表示されます。 • 右側のペインには [Charts] が表示され、次のタブがあります。 • [Latest]：全体の平均オンボーディング時間が表示されます。 [Authentication] および [DHCP] の場合、[Latest] タブには、[Avg Latency Time]、[Authentication] の [Avg Authentication Time]、および [DHCP] の [Avg DHCP Time] に基づいてデータをフィルタリングするためのドロップダウンリストが表示されます。 • [Trend]：[Baseline] タブが含まれます。このタブでは、機械学習の基準チャートを表示できます。 左側のペインで選択しているタブに応じて、**[Trend]** > **[Baseline]** 内に追加のタブが表示されます。たとえば、[Association]、[Authentication]、または [DHCP] データの [Authentication]、[Time Baseline]、または [Failure Baseline] タブが表示されます。 （注） [Failure Baseline] データは、グローバルサイトの場合にのみ表示されます。 （注） [Baseline] 、[Time Baseline]、および [Failure Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics の設定 （95 ページ）およびCisco AI Network Analytics の概要 （7 ページ）を参照してください。 • チャートの上にマウスカーソルを合わせると、選択した時点の情報が同期化されたツールチップに表示されます。 • チャート内の色付きセグメントをクリックすると、次のオプションが表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Connectivity RSSI] ダッシュレット	
アイテム	説明
[Connectivity RSSI] チャート	すべてのサイトまたは選択したサイト内に配置されたすべてのクライアントの受信信号強度表示（RSSI）分布。このダッシュレットには、RSSI 測定値が -72 dBm（しきい値）より大きいすべてのクライアントの RSSI 測定値の割合が示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Connectivity SNR] ダッシュレット	
アイテム	説明
[Connectivity SNR] チャート	すべてのサイトまたは選択したサイト内に配置されたすべてのクライアントの信号対雑音比（SNR）分布。このダッシュレットには、SNR 測定値が 10 dBm（しきい値）より大きいすべてのクライアントの SNR 測定値の割合が示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Roaming Times] ダッシュレット	
アイテム	説明
[Client Roaming Times] チャート	ローミング時間および障害別のクライアント分布。このダッシュレットには、ローミング時間が 3000 ミリ秒未満のクライアントの割合が表示されます。

[Client Roaming Times] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Access Points]、[Top SSIDs]、[Top Host Device Types]、[Top Bands]、[Top Locations]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Count per SSID] ダッシュレット	
アイテム	説明
[Client Count per SSID] チャート	すべてのサイトまたは選択したサイトにおけるSSID別のクライアント数の時系列分布。 チャートには、次の 2 種類があります。 • [Latest]：デフォルトで表示されます。このスナップショットビューチャートには、SSID または選択したサイトごとのクライアントの分布が表示されます。 • [Trend]：[Client Count] タブと [Baseline] タブがあります。[Baseline] タブをクリックすると、機械学習によって生成される SSID 基準チャートが表示されます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AIネットワーク分析の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics の設定 （95 ページ）およびCisco AI Network Analytics の概要 （7 ページ）を参照してください。 **重要** SSID機械学習の基準チャートを表示するには、**[Filter]** オプションでサイトと SSID を選択する必要があります。 • 基準チャートの詳細は、異なる色で表示されます。 • **緑色のバンド**：予測基準値。 • **青色の実線**：実際の値。

[Client Count per SSID] ダッシュレット	
アイテム	説明
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。 次の 2 種類のチャートから構成されます。 • **Latest** • [Trend]：[Baseline] タブが含まれます。このタブでは、機械学習の基準チャートを表示できます。 （注） [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析 の機能については、AI ネットワーク分析 を有効にする必要があります。Cisco AI Network Analytics の設定 （95 ページ）およびCisco AI Network Analytics の概要 （7 ページ）を参照してください。 チャートの上にマウスカーソルを合わせると、選択した時点の情報が同期化されたツールチップに表示されます。 チャート内の色付きセグメントをクリックすると、次の情報が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のワイヤレスクライアントの詳細データが格納されたテーブル。

[Connectivity Physical Link] ダッシュレット	
アイテム	説明
[Connectivity Physical Link] チャート	有線クライアントデバイスのリンクステートの分布。これは、物理リンクがアップ、ダウン、およびエラーであるクライアントデバイスの数です。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Switches]、[Top Host Device Types]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Count per Band] ダッシュレット	
アイテム	説明
[Client Count per Band] チャート	2.4 GHz 帯域または 5 GHz 帯域に接続されたワイヤレスクライアントの分布。 セグメントの上にカーソルを合わせると、特定の帯域に接続されているクライアントの割合と数が表示されます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

[Client Data Rate] ダッシュレット	
アイテム	説明
[Client Data Rate] チャート	クライアントのデータレートの分布。 使用しているクライアントプロトコルに基づいてクライアントをフィルタ処理するには、[Client Protocol] ドロップダウンリストを使用します。[802.11 n/ac/ax] または [802.11 a/b/g] を選択できます。
[View Details]	[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでチャート内の色付きセグメントをクリックすると、次が表示されます。 • クライアント数別のデータタイプカテゴリ：[Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

ステップ 7 ネットワーク内のクライアントに関する詳細情報を表示するには、[Client Devices] ダッシュレットを使用します。このダッシュレットは次の機能を提供します。

[Client Devices] ダッシュレット	
アイテム	説明
Type	クライアントのタイプに基づいてテーブルをフィルタ処理します。オプションは、[Wired] および [Wireless] クライアントです。

[Client Devices] ダッシュレット	
アイテム	説明
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、データタイプに基づいてテーブルをフィルタ処理します。 • [Onboarding Time >= 10 s]：オンボーディング時間が 10 秒（しきい値）以上。 • [Association >= 5 s]：関連付け時間が 5 秒（しきい値）以上。 • [DHCP >= 5 s]：DHCP 時間が 5 秒（しきい値）以上。 • [Authentication >= 5 s]：認証時間が 5 秒以上。 • [RSSI <= -72 dBm]：RSSI が -72 dBm（しきい値）以下。 • [SNR <= 9 dB]：SNR が 9 dB（しきい値）以下。

[Client Devices] ダッシュレット	
アイテム	説明
[Client Device] テーブル	

[Client Devices] ダッシュレット	
アイテム	説明
	詳細なクライアントデバイス情報を表形式で表示します。デフォルトでは、[Client Device] テーブルに次の情報が表示されます。 • [Identifier]：クライアントのユーザー ID、ホスト名、または MAC アドレスが、可用性に基づいてこの順序で表示されます。たとえば、ユーザー ID が使用不可能な場合は、ホスト名が表示されます。ユーザー ID とホスト名が使用不可能な場合は、MAC アドレスが表示されます。 [Identifier] 列には、クライアントデバイスが有線と無線のどちらであるかを判別できる固有のアイコンも表示されます。ワイヤレスデバイスの場合、クライアントが接続している間、およびクライアントが新しく接続されると、アイコンに青い点が表示されます。 • [MAC Address]：デバイスの MAC および Randomized and Changing MAC Address（RCM）を含む MAC アドレスが表示されます。プライベート MAC アイコンが RCM の前に表示されます。MAC アドレスのタイプ（すべて、デバイス MAC、RCM など）に基づいてテーブルをフィルタ処理できます。 • [IPv4 Address]：クライアントの IPv4 アドレスが、可用性に基づいて表示されます。 （注） メニューで [IPv6 Address] チェックボックスをオンにすると、クライアントの IPv6 アドレスを表示できます。 • [Device Type]：デバイスタイプが表示されます。 • [Health]：オンボーディングスコアと接続済みスコアの平均が表示されます。クライアント ヘルス スコアは 5 分ごとに計算されます。 （注） スコアが -- の場合、これはクライアントが直近でオンボーディングした（新規）ことを示します。新しいクライアントは、健全性スコア計算ウィンドウの開始 5 分後に、オンボードを試行するクライアントです。これらの新規クライアントのヘルススコアは、次回の 5 分間の計算ウィンドウに含まれます。 • [Trust Score]：AI エンドポイント分析の信頼レベルに基づいて、ネットワークに接続されているエンドポイントの信頼スコアが表示されます。 • [Tracked]：クライアントのトラッキングステータスが表示されます。 • **Last Seen** • [AP Name]（ワイヤレスクライアントの場合のみ）：アクセスポイントの名前が表示されます。 • [Switch]（有線クライアントの場合のみ）

[Client Devices] ダッシュレット	
アイテム	説明
	• [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。 • [Security Group (Tag Value)]：有線クライアントの場合のみ、セキュリティグループタグ値が表示されます。 • [Bridge-Mode Virtual Machine]：ワイヤレスクライアントの場合のみ、ブリッジモード仮想マシンが表示されます。 • [Average Latency By Access Category]：平均ビデオ、平均音声、平均ベストエフォート、および平均バックグラウンド遅延が含まれます。 • [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。
[Tracked Clients]	[Tracked Clients] をクリックするとスライドインペインが表示されます。このペインには、[MAC Address]、[Last Detected]、[Tracking Duration]、[Description]、および [Randomized MACs] を含むテーブルが表示されます。
[Excluded Clients]	[Excluded Clients] をクリックするとスライドインペインが表示されます。このペインには、[Excluded MAC address]、[Excluded Since]、[Impacted Wireless Controllers]、および [Description] を含むクライアント除外リストが表示されます。 クライアントの除外の詳細については、「除外クライアントの設定（191 ページ）」[英語] を参照してください。
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。
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。

[Client Devices] ダッシュレット	
アイテム	説明
	テーブルの表示をカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 3. [Apply] をクリックします。

クライアントデバイスの正常性のモニターとトラブルシューティング

[Client 360] ウィンドウを使用して、ネットワーク管理者は、クライアントに発生した問題を簡単に特定できます。利用可能な情報により、クライアントの問題に関する次のインサイトが得られます。

- **問題の内容**：[Summary] カテゴリを使用して、オンボーディング、ローミング、接続の問題など、クライアントに発生した問題についてのインサイトをすばやく得ることができます。
- **時期**：正常性タイムラインスライダを使用して、問題が発生した時期を特定します。問題がいつ発生したかがわかっている場合は、問題を設定の変更と関連付けることが可能な場合があります。
- **原因**：問題の原因となったイベントと KPI を表示します。
- **影響**：問題が 1 人のユーザーに限定されているか、多数のユーザーに広がっているかを判定します。

これらすべての機能により、IT 組織は、ネットワークをより効率的に運用し、ユーザーにより良いエクスペリエンスを提供できます。

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を表示し、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できます。Assurance は、ユーザーのアクセス範囲を特定の Client 360 に制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。[Client 360] ウィンドウで、サイト、有線および無線のクライアントにアクセスできるようにしておく必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

（注） ベストプラクティスとして、アンカーと外部 ワイヤレスコントローラ の両方を Catalyst Center に追加して、ゲストアンカーまたは L3 モビリティクライアントのセッションを完全に可視化します。

HA フェールオーバーが発生した場合、クライアントの正常性データの表示に最大 1 時間かかることがあります。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

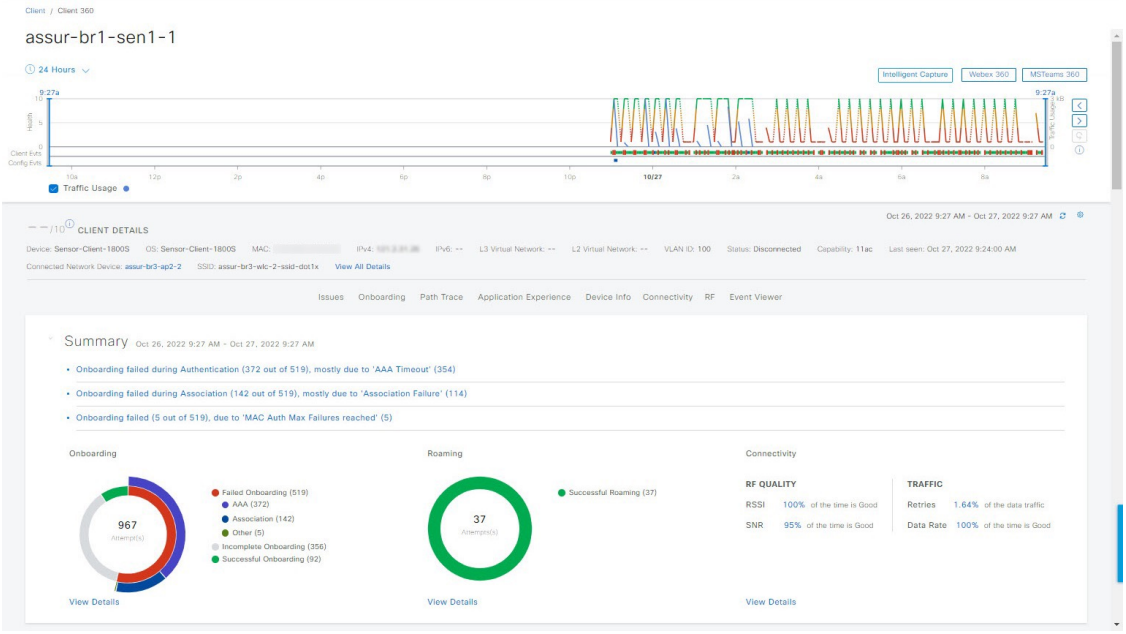
[Client Health] ダッシュボードが表示されます。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- [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] フィールドに、次のいずれかの要素を入力します。
  - ユーザー ID（Cisco ISE により認証）
  - 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 *16 : [Client 360]* ウィンドウ



ステップ 4 上部のメニューバーにある時間範囲設定（ 24 Hours ）をクリックして、 ダッシュボードに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューで、[3 hours]、[24 hours]、[7 days] のいずれかの時間範囲を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 5 右上隅にある [Intelligent Capture] をクリックすると、特定のクライアントデバイスのキャプチャされたオンボーディングやデータパケットを表示、モニター、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。クライアントデバイスのライブオンボーディング パケット キャプチャ セッションの実行 （482 ページ）を参照してください。

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

ステップ 6 タイムラインスライダの右上隅にある [MS Teams 360] をクリックして、クライアントの MS Teams ミーティングを表示し、監視します。

[Application Experience for MS Teams] スライドインペインが表示されます。

Microsoft Teams の統合を設定するには、*Cisco Catalyst Center Administrator Guide* の「*Configure MS Teams Integration*」を参照してください。

[Application Experience] スライドインペインでは次の機能を利用できます。

- [Search bar]：表示されたテーブルでミーティングを検索できます。
- [Time Range filter]：時間フィルタをクリックして、表示するデータの時間範囲を指定します。
- [Client Meetings] テーブルには、[Meeting Name]、[MS Teams Score]、[Network APM Score]、[Duration]、[Start Time]、[End Time]、[Status]、[Meeting Type]、[Participants] が表示されます。

（注） [Network APM Score] は、管理対象ネットワークデバイスからエクスポートされた NetFlow データに基づいて計算されます。データは 5 分ごとに集約されます。通話時間が 5 分未満の場合、一致する NetFlow レコードがない可能性があるため、そのような短時間の通話では、APM スコアに「利用可能なデータがありません」と表示されます。APM の詳細については、「サポートされるプラットフォーム （199 ページ）」[英語] を参照してください。

会議品質 KPI データを表示する会議を選択するには、次のように操作します。

- [Audio Quality] タブをクリックすると、[MS Teams Score] と [Network APM Score] が表示されます。[Packet loss]、[Jitter]、[Media Bitrate] などのメトリックをグラフビューで確認できます。
- [Video Quality] タブをクリックすると、[MS Teams Score] と [Network APM Score] が表示されます。[Packet loss]、[Jitter]、[Media Bitrate] などのメトリックをグラフビューで確認できます。
- [Share Quality] タブをクリックすると、[MS Teams Score] と [Network APM Score] が表示されます。[Packet loss]、[Jitter]、[Media Bitrate] などのメトリックをグラフビューで確認できます。

ステップ 7 タイムラインスライダの右上隅にある [Webex 360] をクリックして、クライアントの Webex ミーティングを表示し、監視します。[Search Meetings] ポップアップウィンドウが表示されます。

Webex 統合を設定するには、*Cisco Catalyst Center Administrator Guide* の「*Configure Webex Integration*」を参照してください。

a) クライアントの Webex ミーティングに関連付けられた電子メールアドレスを入力します。
b) [Search Meetings] をクリックします。[Application Experience for Webex] スライドインペインが表示されます。
c) 次の機能には [Application Experience] スライドインペインを使用します。
   - **検索バー**：表示されたテーブルでミーティングを検索できます。
   - **時間範囲フィルタ**：時間フィルタをクリックして、テーブルに表示するデータの時間範囲を指定します。
   - [Client Meetings] テーブルには、[Meeting Number]、[Meeting Name]、[Application]、[Network Duration]、[Start Time]、[End Time]、[Status] が表示されます。

     ミーティングを選択して、ミーティングの品質 KPI データを表示できます。これは、アプリケーション（Webex API を使用して取得されたデータ）とネットワーク（NetFlow を使用して取得されたデータ）の遅延に基づくオーディオ品質、ビデオ品質、および共有品質を示す水平バーとしてテーブルの下に表示されます。ドロップダウンリストを使用して、送信および受信オプショ

ンに基づいてデータをフィルタ処理し、パケット損失、ジッターなどのメトリックに関連するアプリケーションとネットワークの遅延グラフを表示できます。

ステップ 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の機能を次の表に示します。

実行する操作	結果
クライアントのテレメトリステータスの表示	**1.** タイムラインスライダで、[Telemetry Status] チェックボックスをオンにします。 テレメトリステータス行がタイムラインスライダに表示されます。 **2.** タイムラインスライダにカーソルを合わせると、ネットワークデバイスのテレメトリステータス（[Good]、[Fair]、[Poor] など）がツールチップに表示されます。 **3.** [Client Health] で、[Telemetry Status] をクリックすると、テレメトリステータスの概要が スライドインペイン に表示されます。 （注） テレメトリステータスは 15 分間隔で計算されます。現在の期間が 15 分未満の場合、またはデータ収集間隔が計算周期と一致しない場合、次の間隔が完了するまでステータスは「緑色」で表示されることがあります。
クライアントトラフィック使用状況の表示	**1.** タイムラインスライダで、[Traffic Usage] チェックボックスをオンにします。 トラフィック使用状況の行がタイムラインスライダに表示されます。 **2.** タイムラインスライダにカーソルを合わせると、クライアント使用状況情報が表示されます。

実行する操作	結果
クライアントの正常性と KPI の詳細の表示	タイムラインスライダにカーソルを合わせると、5分の時間枠でのクライアントの正常性と KPI の詳細が表示されます。 （注） • 色付きの円が付いている各 KPI は、個々のクライアントの正常性スコアに寄与します。 • [Data Rate] KPI では、インターフェイスまたは物理ポートのデータレート容量が表示されます。ポートが特定のレートにネゴシエートされた場合、そのネゴシエートされたレートが表示されます。
1 時間の期間がタイムラインに表示されます。	タイムラインをダブルクリックします。 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。 （注） 1 時間を超えて情報を表示するには、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。
オンボーディングの詳細の表示	タイムラインスライダにカーソルを合わせると、クライアントのオンボーディングの成否の詳細が表示されます。 • クライアントのオンボーディングに成功した場合は、関連付けや認証などのオンボーディング時間が表示されます。 • クライアントオンボーディングに失敗した場合は、失敗のタイプと理由（取得可能な場合は Cisco ISE の失敗の理由を含む）が表示されます。
接続性の詳細の表示	タイムラインスライダにカーソルを合わせると、RSSI や SNR などの接続性の詳細が表示されます。
接続の詳細の表示	タイムラインスライダにカーソルを合わせると、IP アドレスやステータスなどの接続の詳細が表示されます。

実行する操作	結果
主要イベントの詳細の表示	1. タイムラインスライダにカーソルを合わせると、クライアントの主要イベントが表示されます。 それらの詳細を覚えておきます。 • 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表し、赤の垂直バーは失敗したイベントを表します。 • 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。 2. [See Full List] をクリックすると、[Event Viewer] ダッシュレットに移動してクライアントのすべての主要イベントが表示されます。

ステップ 9 タイムラインの下にある [Client Details] 領域で、個々のクライアントの正常性スコアを確認します。

個々のクライアントの正常性スコアは、クライアントのオンボーディングステータス、RSSI、および SNR を集約したものです。

ユーザー ID で検索する場合、表示される個別のクライアント ヘルス スコアは、そのユーザーに関連付けられているすべての監視対象クライアント デバイスの最も低いスコアです。詳細については、「個別のクライアント正常性スコア （195 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 10 タイムラインの下にある [Client Details] エリアに、次の情報が表示されます。

- ワイヤレスクライアントの場合、このエリアには、その OS バージョン、MAC アドレス（デバイス MAC と RCM を含む）、IPv4 および IPv6 アドレス、ブリッジモードの仮想マシン、接続された VLAN ID、接続ステータス、平均遅延、最終検出タイムスタンプ、接続されたネットワークデバイス、SSID、最後の既知のロケーションなど、クライアントデバイスに関する情報が表示されます。

  Wi-Fi 7 対応のワイヤレスクライアントとアクセスポイントは、2.4 GHz または 5 GHz または 6 GHz 帯域の任意の組み合わせに接続します。MLO（Multiple Link Operational）クライアントは、異なる帯域への接続を同時に確立することで、データ転送速度が向上します。ワイヤレスクライアントが Wi-Fi 7 対応 AP または Zelland AP に接続されている場合、Catalyst Center はリンクごとに 4 つの KPI（RSSI、SNR、特殊ストリーム、およびチャンネル）をサポートします。Wi-Fi 7 対応クライアントの場合、タイムラインにカーソルをホバーすると、5 分間、複数のリンクで動作する接続 KPI（チャンネル、SNR、および RSSI）が表示されます。ただし、データ転送は、クライアントに基づいて単一のリンクまたは複数のリンクで発生する可能性があります。

- 有線クライアントの場合、このエリアには、MAC アドレス、IPv4 および IPv6 アドレス、セキュリティグループ（タグ値）、接続された VLAN ID、接続ステータス、最終検出タイムスタンプ、接続されたネットワークデバイス、ポート、最後の既知のロケーションなどのクライアントデバイスに関する情報が表示されます。

- PoE 対応デバイスの場合は、[IEEE Class]、[Negotiated Power Level]、[PoE Status] の各要素も [Client Details] エリアに表示されます。

ステップ 11 [Client Details] エリアで [View All Details] をクリックすると、クライアントデバイスに関する追加の詳細を含む スライドインペイン が開きます。

クライアントデバイスの分類情報（デバイスタイプ、ユーザー名、ホスト OS、ホスト名など）を表示するには、Catalyst Center を Cisco ISE と統合するか、Cisco AI エンドポイント分析 を Catalyst Center で展開して有効にする必要があります。

ステップ 12 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。

[Summary] カテゴリ

選択したタイムフレームにおける選択したクライアントのオンボーディング、ローミング、および接続情報が人間が判読可能な要約とグラフの形式で表示されます。情報には、カテゴリ（ビデオ、音声、ベストエフォート、およびバックグラウンド）別のトラフィックの削除数、データレート、平均遅延が含まれます。

リスト内の問題をクリックすると、スライドインウィンドウが表示され、クライアントが最後にアクセスした場所で遭遇した性能上の問題に関する詳細が見られます。このスライドインウィンドウには、クライアント、場所、および問題に基づく情報が表示されます。

問題に応じて、スライドインペイン に次の詳細が表示されます。

- [Location]：クライアントが過去 24 時間に訪れた建物またはフロアをドロップダウンフィールドで選択します。その場所でクライアントが遭遇した問題の詳細が表示されます。
- [Issue radial bar chart]：問題の概要がグラフィックチャートに表示されます。
- [Top Failure Reasons]：クライアントがこの問題に遭遇した回数が表示されます。たとえば、オンボーディングの問題は、DHCP タイムアウトの回数を示す場合があります。

  （注）
  オンボーディングカテゴリの場合は、放射状棒グラフの横にある [AAA] をクリックすると、上位の AAA または Cisco ISE の失敗理由が表示されます。AAA の失敗情報は ワイヤレスコントローラからのものであり、Cisco ISE の失敗情報は Cisco ISEからのものです。

  [Top ISE Failure Reasons] をクリックすると、[Event Viewer] テーブルに Cisco ISE 認証イベント、および ワイヤレスコントローラ からの該当する認証イベントが表示され、データを比較できます。なお、ワイヤレスコントローラ と Cisco ISE で報告される失敗イベントの数は、ワイヤレスコントローラ からのクライアント再試行回数および Cisco ISE からの失敗レポートのスロットリングが原因で、一致しない場合があります。

- [Timeline Slider]：タイムラインスライダには、クライアントの失敗の期間が表示されます。放射状棒グラフ内の色付きのセグメントをクリックすると、そのセグメントに基づいてタイムラインスライダがフィルタ処理されます。タイムラインスライダのバーの上の線は、選択したロケーションにある他のクライアントを含めて、ネットワークで同じ問題が発生したタイミングを表しています。クライアントが接続を試行した AP も示されます。
- [Event Viewer]タブ：この問題に関する情報を表示します。
- [Impact Analysis]タブ：上位の AP、SSID、帯域など、影響を受けるコンポーネントの上位を表示します。各コンポーネントの下にある括弧の数字は、そのコンポーネントの影響を受けたその他のクライアントの数です。
- [Correlation]タブ：クライアントが遭遇した KPI の失敗をタイムラインのチャートを表示します。デフォルトでは、接続されたワイヤレスコントローラとスイッチを含め、クライアントが問題に遭遇した AP の上位 3 つが表示されます。デフォルトの KPI に加えて、KPI ドロップダウンリストからもさらに選択できます。

[Issues] 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 が開いて、該当する詳細情報（問題の説明、同じタイプの問題が発生している関連クライアント、推奨処置 など）が表示されます。 （注） Cisco ISE の認証エラーの問題が発生している無線クライアントに対して、次の操作を行うことができます。 • [Relevant Clients] タブの スライドインペイン で、同じタイプの問題が発生している他のクライアントでの Cisco ISE の上位の失敗理由を確認できます。 • [Suggested Actions] タブの スライドインペイン で、失敗の問題に対処するための推奨処置を確認できます。 スライドインペイン で、次の操作を行うことができます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （299 ページ）を参照してください。

[Onboarding] 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、および AAA や DHCP などのサービスに関する情報があります。

有線クライアントのトポロジの例：**[Client]** > **[Switch]** > **[Router]**

無線クライアントのトポロジの例：**[Client]** > **[SSID]** > **[Access Point]** > **[Wireless Controller]**

トポロジでは、次の操作を行うことができます。

- 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。Wi-Fi 7 対応クライアントが複数の帯域に接続されている場合は、帯域値（2.4 GHz、5 GHz、6 GHz）がトポロジリンクの上部に表示されます。
- 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。

[Event View] 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。この一覧により、どのサブイベントの間に問題が発生したかを特定できます。

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。

For Wired Clients：ISE サーバーイベント、スイッチシステムレベルの syslog、スイッチポートまたはインターフェイス固有のイベント、およびクライアント固有のイベントがリストされますCisco ISE。

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。

（注）
Cisco ISE の認証失敗イベントの詳細を表示するには、赤い円で示されている [ISE Authentication] イベントをクリックすると、右側のペインに詳細が表示されます。右側のペインで [Show ISE Events] クリックすると、RADIUS サーバーによって完了した Cisco ISE の認証手順が表示されます。各手順には、Cisco ISE から収集されたコード番号とその説明が記載されています。

[Path Trace] カテゴリ
[Run New Path Trace] をクリックすると、指定した送信元デバイスと接続先デバイス間のネットワークトポロジが表示されます。トポロジには、パスの方向とパスに沿ったデバイスが、その IP アドレスを含めて含まれます。ディスプレイには、パスに沿ったデバイスのプロトコル（**Switched**、**STP**、**ECMP**、**Routed**、**Trace Route**）や、その他のソース タイプも表示されます。 パストレースの実行 （528 ページ）を参照してください。

[Application Experience] カテゴリ
クライアント デバイスで実行中のアプリケーション、およびその質的および量的なメトリック。 メトリックをチャート形式で表示するには、テーブル内のアプリケーションの横にあるオプションボタンをクリックします。関連する情報を示すスライドインペインが開きます。 アプリケーション エクスペリエンスとアプリケーションの可視性について （197 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 （206 ページ）を参照してください。

[Detail Information] カテゴリ

次のいずれかのタブをクリックすると、対応する情報が表示されます。

- [Device Info]：デバイスについての基本情報が表示されます。

  Samsungデバイスについては、このタブに、ビルド番号、製造元、国番号、デバイスタイプ（モバイル、タブレットなど）、ホストのオペレーティングシステムといった詳細情報が表示されます。

  Wi-Fi 7 対応クライアントの場合、接続情報にはチャネルと帯域の値が表示されます。

  ネットワークに接続されているエンドポイントの場合、このタブには、[Hardware Manufacturer]、[Device Type]、[OS]、および [Endpoint Type] などの [Manufacturing] の詳細が表示されます。

  このタブには、デバイスの [Tracked] および [Exclusion] のステータスも表示されます。必要に応じて、対応するハイパーリンクをクリックして、デバイスの追跡ステータスおよび除外ステータスを更新します。

  クライアントを追跡する方法については、「既知のクライアントの追跡（187ページ）」を参照してください。

  [Exclude clients] スライドインペインで次の手順を実行します。

  1. トグルボタンを使用して、デバイスの除外ステータスを設定します。
  2. トグルボタンを有効にする場合は、[Description for Exclusion] フィールドに説明を入力し、デバイスを除外する ワイヤレスコントローラ の横にあるチェックボックスをオンにします。
  3. [Save] をクリックします。

  表示される利用可能なセキュリティ情報（認証タイプ、セキュリティポリシータイプなど）は、クライアント接続およびCisco ISE がCatalyst Center と統合されているかどうかによって異なります。

  ステーション情報（HW モデル、SW バージョン、AC/DC 電圧など）の詳細が表示されるのは、Intel デバイスに対してのみです。

- [RF]：ワイヤレスデバイスでのみ使用できます。
- [User Defined Network]：UDN 対応のネットワークデバイスでのみ使用できます。このタブには、登録済みの UDN、接続された UDN の詳細、デバイスの MAC アドレス、デバイスの所有者、デバイス名、デバイスタイプ、および現在のステータスが表示されます。
- [Connectivity]：Rx/Tx データレート、Tx/Rx パケット数、無線の Rx 再試行接続、DNS 要求と応答数、および Tx ドロップ（パケットドロップの割合）に関するそれぞれの KPI チャートが表示されます。
- [PoE]：PoE 対応クライアントでのみ使用できます。
- [iOS Analytics]：Apple デバイスでのみ使用できます。
- [Intel Connectivity Analytics]：Intel ワイヤレスアダプタでサポートされているデバイスでのみ使用できます。サポートされているクライアントによって報告されたローミングイベント、報告されたエラー、一時的な切断レポート、および低 RSSI レポートが表示されます。

クライアント追跡

クライアント追跡は、Assurance の機能であり、

- クライアントがネットワークにいつ接続および切断するかを追跡およびモニターし、
- 既知および新規のクライアントを追跡し、
- クライアントのトラッキングイベントの通知を受信できるようにします。

この機能は、指定された重要クライアントの接続をプロアクティブにモニターおよび追跡することにより、接続ステータスをリアルタイムで可視化します。これらの機能により、中断の可能性を迅速に特定して対応することができるため、最も重要なデバイスやユーザーの接続および運用可能な状態を維持できるようになります。

クライアントのタイプ

既知のクライアントまたは新規クライアントを追跡できます。

- 既知のクライアント：以前にネットワークに接続したことがあるクライアント。
- 新規クライアント：以前にネットワークに接続したことがないクライアント。

トラッキング通知のタイプ

2 つのタイプ（接続および切断）のトラッキング通知を設定できます。

- 接続通知：クライアントがネットワークに接続したときに通知されます。クライアントがネットワークに最初に接続したときにのみ通知するか、ネットワークに接続するたびに通知するかを選択できます。
- 切断通知：クライアントがネットワークから切断されるたびに通知されます。

切断通知の動作

クライアントの切断通知を設定する場合は、以下の切断通知の動作を確認します。

- クライアントが切断されてから 5 分以内に再接続された場合、切断通知は送信されません。このアプローチにより、すぐに解決する短い中断または通常のクライアントローミングに対するアラートが通知されなくなります。
- スパムを防ぐために、切断通知の頻度は次のように制限されています。
  - ワイヤレスクライアントの場合：クライアントが同じ理由で1時間にわたって切断した場合、通知は1つだけ送信されます。その時間内に切断の理由が変更されると、新しい通知が送信されます。
  - 有線クライアントの場合は、切断通知が 1 時間ごとに送信されます。

既知のクライアントの追跡

特定の既知のクライアントを追跡してモニターし、ネットワークに接続または切断するタイミングを示すには、この手順を使用します。追跡対象クライアントが接続または切断したときに通知されるように追跡通知を設定できます。

Before you begin

次の要件を満たしている必要があります。

- この手順を実行することができるのは、NETWORK-ADMIN-ROLE または SUPER-ADMIN-ROLE 権限を持つユーザーだけです。
- 「ネットワークで検出されたクライアントアクティビティの追跡」イベント（イベント ID：NETWORK-CLIENTS-4-370）が有効になっていることを確認します。これにより、クライアントが接続または切断されたときに通知を受信できます。このイベントが有効になっていないと、クライアント追跡が設定されていても、追跡対象クライアントに関する通知を受信しません。なお、このイベントは、以前は「ネットワーク上で接続を検出されたクライアント」と呼ばれていました。

  イベント通知を作成する手順については、『*Cisco Catalyst Center User Guide*』の「構築と展開のワークフロー」章の「イベント通知の作成」を参照してください。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

ステップ 3 1 つのクライアントのみを追跡する場合は、次の手順を実行します。

a) [Client Devices] ダッシュレットで、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。

b) [Client 360] ページの [Detail Information] で、[Tracked] フィールドにある [No] をクリックします。

c) [Track Client] スライドインペイン で、[Not Tracking] トグルボタンをクリックします。

d) [Notification Frequency] で、チェックボックスをオンにして通知タイプを登録します。

- [Connect Notification]：クライアントがネットワークに接続すると通知されます。
- [Disconnect Notification – On every detection]：クライアントがネットワークから切断されるたびに通知されます。

e) [Connect Notification] チェックボックスをオンにした場合に、この通知を受信する頻度を指定します。

- [On First Detection]：クライアントがネットワークに最初に接続されたときにのみ通知されます。
- [On Every Detection]：クライアントがネットワークに接続するたびに通知されます。

f) [Notification Expiration] で、これらの通知を期限切れにする時間を指定します。
g) [Save] をクリックします。

クライアントは追跡され、追跡対象クライアントリストに追加されます。

ステップ 4 複数のクライアントを追跡する場合は、次の手順を実行します。

a) [Client Devices] ダッシュレットで、トラッキング対象とするクライアントの横にあるチェックボックスをオンにします。
b) [Actions] ドロップダウンリストから、[Track Client] を選択します。
c) [Track Client] スライドインペインで [Not Tracking] トグルボタンが表示されている場合はクリックします。
d) [Notification Frequency] で、チェックボックスをオンにして通知タイプを登録します。
   - [Connect Notification]：クライアントがネットワークに接続すると通知されます。
   - [Disconnect Notification – On every detection]：クライアントがネットワークから切断されるたびに通知されます。
e) [Connect Notification] チェックボックスをオンにした場合に、この通知を受信する頻度を指定します。
   - [On First Detection]：クライアントがネットワークに最初に接続されたときにのみ通知されます。
   - [On Every Detection]：クライアントがネットワークに接続するたびに通知されます。
f) [Notification Expiration] で、これらの通知を期限切れにする時間を指定します。
g) [Save] をクリックします。

選択したクライアントが追跡され、追跡対象クライアントリストに追加されます。

新しいクライアントの追跡

新しいクライアントがネットワークに接続または切断したことを追跡およびモニターするには、次の手順に従います。新しいクライアントが接続または切断したときに通知されるように、通知を設定できます。

Before you begin

次の要件を満たしている必要があります。

- この手順を実行することができるのは、NETWORK-ADMIN-ROLE または SUPER-ADMIN-ROLE 権限を持つユーザーだけです。
- 「ネットワークで検出されたクライアントアクティビティの追跡」イベント（イベント ID：NETWORK-CLIENTS-4-370）が有効になっていることを確認します。これにより、クライアントが接続または切断されたときに通知を受信できます。このイベントが有効になっていないと、クライアント追跡が設定されていても、追跡対象クライアントに関する

通知を受信しません。なお、このイベントは、以前は「ネットワーク上で接続を検出されたクライアント」と呼ばれていました。

イベント通知を作成する手順については、『*Cisco Catalyst Center User Guide*』の「構築と展開のワークフロー」章の「イベント通知の作成」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Health]**

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

ステップ 3 [Client Devices] ダッシュレットで、[Tracked Clients] をクリックします。

[Tracked Client] スライドインペイン が開いて、現在のすべての追跡対象クライアントと期限切れの追跡対象クライアントが MAC アドレスで一覧表示されます。

ステップ 4 追跡対象の新しいクライアントを追加するには、次のいずれかの方法に従います。

実行する操作	[Tracked Client] スライドインペイン で行う操作
クライアントを一括追加する	[Import Client List (CSV)] をクリックして ステップ 5 （189 ページ） に進む
MAC アドレスを指定してクライアントを手動で追加する	[+ Add New] をクリックして ステップ 6 （189 ページ） に進む

ステップ 5 クライアントを一括で追加する場合は次の手順を実行します。

a) [CSV Sample] をクリックして、サンプルファイルをダウンロードします。
b) サンプルファイルを編集して、必要なクライアント情報をすべて含めます。
c) 編集した CSV ファイルをファイルアップロードエリアにドラッグアンドドロップします。

または、[Choose a File] をクリックし、CSV を選択してから、[Upload] をクリックします。

d) [Save] をクリックします。

新しいクライアントがシステムにインポートされ、追跡対象クライアントリストに追加されます。

ステップ 6 手動でクライアントを追加する場合は、[Add New Clients] スライドインペイン で次の手順を実行します。

a) [MAC Address] フィールドに MACアドレスを入力します。
b) [Description for Tracking] フィールドに、クライアントの簡単な説明を入力します。
c) （任意） 複数のクライアントを追加するには [+] アイコンをクリックします。次に、クライアントの MAC アドレスと説明を入力します。
d) [Notification Frequency] で、チェックボックスをオンにして通知タイプを登録します。

- [Connect Notification]：クライアントがネットワークに接続すると通知されます。

- [Disconnect Notification - On every detection]：クライアントがネットワークから切断されるたびに通知されます。

e) [Connect Notification] チェックボックスをオンにした場合に、この通知を受信する頻度を指定します。
   - [On First Detection]：クライアントがネットワークに接続したときにのみ通知されます。
   - [On Every Detection]：クライアントがネットワークに接続するたびに通知されます。

f) [Notification Expiration] で、これらの通知を期限切れにする時間を指定します。
g) [Save] をクリックします。

新しいクライアントが追跡され、追跡対象クライアントリストに追加されます。

クライアントの追跡の停止

次の手順を使用して、クライアントの追跡を停止し、それらのクライアントがネットワークに接続したとき、またはネットワークから切断したときの通知の受信を停止します。

単一のクライアントまたは複数のクライアントの追跡を停止できます。

Before you begin

この手順を実行することができるのは、NETWORK-ADMIN-ROLE または SUPER-ADMIN-ROLE 権限を持つユーザーだけです。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Health]**

[Overall Health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

ステップ 3 単一のクライアントの追跡を停止する場合は、以下の手順を実行します。

a) [Client Devices] ダッシュレットで、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。
b) [Client 360] ページの [Detail Information] で、[Tracked] フィールドにある [Yes] をクリックします。
c) [Tracked Client] スライドインペイン で、[Tracking] トグルボタンをクリックします。[Save] をクリックすると、このクライアントの追跡が無効になります。

   選択したクライアントは追跡されなくなり、追跡対象クライアントリストで期限切れとマークされます。

ステップ 4 複数クライアントの追跡を停止する場合は、以下の手順を実行します。

a) [Client Devices] ダッシュレットで、[Tracked Clients] をクリックします。

b) 追跡を停止するクライアントデバイスのチェックボックスをオンにします。
c) [Actions] ドロップダウンリストで、[Stop Tracking Client] を選択して [OK] をクリックします。

選択したクライアントは追跡されなくなり、追跡対象クライアントリストで期限切れとマークされます。

除外クライアントの設定

この手順に従ってシスコ ワイヤレス コントローラの除外クライアントを設定します。[Excluded Clients] オプションを使用して、次を設定を行うことができます。

- クライアントを除外リストに追加する。
- 除外リストのクライアントを編集する。
- クライアントを除外する ワイヤレスコントローラ を追加する。
- 除外リストからクライアントを削除する。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

ステップ 3 [Client Devices] ダッシュレットで、[Excluded Clients] をクリックします。

ステップ 4 [Excluded Clients] スライドインペインでは、次のいずれかの方法で除外リストにクライアントを追加できます。

- ドロップダウンリストでクライアントを選択するには、[Add] をクリックして次のように設定します。
  1. [MAC Address] ドロップダウンリストで MAC アドレスを選択します。または、検索フィールドに有効な MAC アドレスを入力し、プラスアイコンをクリックして MAC アドレスを追加することもできます。
  2. [Description for Exclusion] フィールドに説明を入力します。
  3. （オプション）別の MAC アドレスを追加するには、プラスアイコンをクリックします。
  4. [Next] をクリックします。
  5. クライアントを除外する ワイヤレスコントローラ の横にあるチェックボックスをオンにします。
  6. [Save] をクリックします。

- クライアントのリストを CSV 形式でインポートするには、[Import Client List (CSV)] をクリックし、次の手順に従います。
  1. [CSV Sample] をクリックして、サンプル CSV ファイルをダウンロードします。
  2. サンプル CSV ファイルを編集してクライアントの情報を含めます。
  3. CSV ファイルをファイルアップロードエリアにドラッグアンドドロップします。または、[Choose a file] をクリックして CSV ファイルの場所に移動し、[Upload] をクリックすることもできます。
  4. [Next] をクリックします。
  5. クライアントを除外する ワイヤレスコントローラ の横にあるチェックボックスをオンにします。
  6. [Save] をクリックします。

ステップ 5 除外リスト内のクライアントを編集するには、次の手順を実行します。

a) 編集する除外 MAC アドレスの横にあるチェックボックスをオンにします。
b) [Actions] にカーソルを合わせて [Edit] を選択します。
c) 説明を編集し、[Save] をクリックします。

ステップ 6 クライアントを除外する ワイヤレスコントローラ を追加するには、次の手順を実行します。

a) ワイヤレスコントローラを追加する除外 MAC アドレスの横にあるチェックボックスをオンにします。
b) [Actions] にカーソルを合わせて [Add WLC] を選択します。
c) クライアントを除外する ワイヤレスコントローラ の横にあるチェックボックスをオンにします。
d) [Save] をクリックします。

ステップ 7 除外リストからクライアントを削除するには、次の手順を実行します。

a) 削除する除外 MAC アドレスの横にあるチェックボックスをオンにします。
b) [Actions] にカーソルを合わせて [Delete] を選択します。
c) [Yes] をクリックします。

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。

クライアントの正常性スコア

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。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、認証および認可が成功し、IP アドレスを受信しています。リンク破棄、リンクエラー、リンク使用率など、正常性スコアに含まれる KPI。クライアントスコアは 10 です。

[ワイヤレスクライアント（Wireless Client）]：クライアントがネットワークに参加しており、RSSI、SNR、データレート、および再試行 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。

クライアントの接続スコア

クライアントの接続スコアは、クライアントデバイスがネットワークに接続された後のエクスペリエンスを表します。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、接続スコアとその結果の全体的な正常性スコアが次のように決まります。

- 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。

再試行主導の正常性スコア	
クライアントの再試行回数	**再試行主導の正常性スコア**
再試行回数が 50% を超えている場合。	クライアントの正常性は不良と見なされます。
再試行回数が 50% 以下の場合。	クライアントの正常性は良好と見なされます。

データレートによって示されるワイヤレスクライアントの正常性	
プロトコル	**データレート主導の正常性スコア**
802.11 a/b/g	クライアントのデータレートしきい値が 5 Mbps 未満の場合は正常性が不良と見なされ、5 Mbps 以上の場合は正常性が良好と見なされます。
802.11 n/ac	クライアントのデータレートしきい値が 24 Mbps 未満の場合は正常性が不良と見なされ、24 Mbps 以上の場合は正常性が良好と見なされます。
802.11 ax/ax6/be	クライアントのデータレートしきい値が 54 Mbps 未満の場合は正常性が不良と見なされ、54 Mbps 以上の場合は正常性が良好と見なされます。

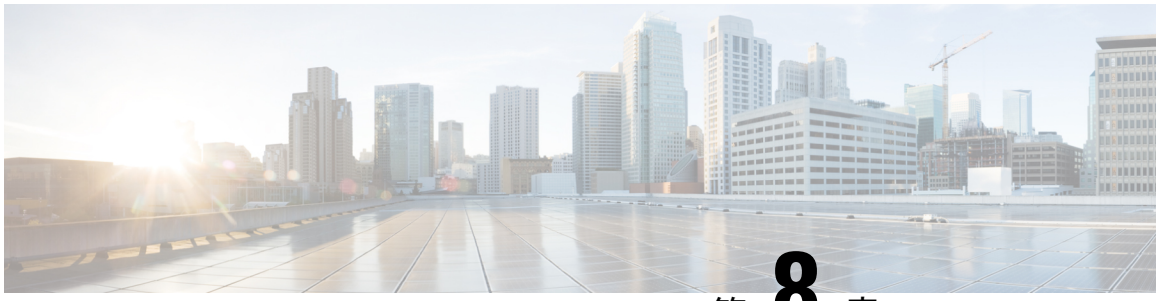
個別のクライアント正常性スコア

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。クライアント正常性スコアの範囲は 1 ～ 10 であり、非アクティブなクライアントのスコアは 0 です。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、認証および認可が成功し、IP アドレスを受信しています。クライアントスコアは 10 です。

ワイヤレスクライアント：クライアントがネットワークに参加しており、RSSI および SNR KPI の観点から接続が良好な状態です。

クライアントのオンボーディングと接続性	クライアント正常性スコアの結果
クライアントがオンボーディングに失敗した場合。	クライアントの正常性スコアは 1 で、不良な状態であると見なされます。
クライアントの RSSI と SNR がしきい値を下回っている場合。	クライアントの正常性スコアは 4 で、正常性が中程度であると見なされます。
クライアントの RSSI と SNR のいずれかがしきい値を下回っている場合。	クライアントの正常性スコアは 7 で、正常性が中程度であると見なされます。
クライアントの RSSI と SNR がしきい値を超えている場合。	クライアントの正常性スコア 10 で、正常性が良好であると見なされます。



第 8 章

アプリケーション健全性のモニター

- アプリケーションエクスペリエンスとアプリケーションの可視性について （197 ページ）
- サポートされるプラットフォーム （199 ページ）
- デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）
- アプリケーションの正常性の前提条件 （203 ページ）
- アプリケーションテレメトリ設定のプロビジョニング （205 ページ）
- ホストのアプリケーション エクスペリエンスの表示 （206 ページ）
- 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 （208 ページ）
- すべてのアプリケーションの正常性のモニター （210 ページ）
- アプリケーションの正常性をモニター （226 ページ）
- アプリケーションの正常性スコアの設定 （239 ページ）
- 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 （240 ページ）

アプリケーションエクスペリエンスとアプリケーションの可視性について

Assuranceは、複雑なアプリケーションデータを処理し、その結果をAssurance正常性ダッシュボードで提示することで、アプリケーションのパフォーマンスに関するインサイトを提供します。

正常性データは、デバイスの観点（[Device 360] ウィンドウ）、ユーザーの観点（[Client 360] ウィンドウ）、アプリケーションの観点（[Application 360] ウィンドウ）でそれぞれ提供されます。

データの収集元に応じて、次の一部またはすべての情報を確認できます。

- アプリケーション名
- スループット
- DSCP マーキング
- パフォーマンスメトリック（遅延、ジッター、パケット損失）

アプリケーション名とスループットを総称して定量的メトリックと呼びます。定量的メトリックのデータは、アプリケーション可視性を有効にすることで得られます。

DSCP マーキングとパフォーマンスメトリック（遅延、ジッター、パケット損失）は、総称して定性的メトリックと呼ばれます。定性的メトリックのデータは、アプリケーションエクスペリエンスを有効にすることで得られます。

アプリケーションの可視性

[Application Visibility] のデータは、IOS-XE を実行しているスイッチ、および AireOS を実行しているワイヤレスコントローラから取集されます。

IOS-XE を実行しているスイッチについては、物理レイヤのアクセススイッチポートに双方向（入力および出力）で適用される事前定義された NBAR テンプレートを使用してアプリケーション可視性のデータが収集されます。

AireOS を実行しているワイヤレスコントローラについては、ワイヤレスコントローラでアプリケーション可視性のデータが収集され、そのデータがストリーミングテレメトリを使用して Catalyst Center に送られます。

ワイヤレスデバイスの場合、管理インターフェイスとワイヤレス管理インターフェイスの両方が存在する場合があります。デバイス検出に使用されるインターフェイスは、Application Visibility and Control（AVC）設定の送信元インターフェイスを決定します。AVC の設定にネットワーク管理インターフェイスの代わりにワイヤレス管理インターフェイスを使用することが予想される場合は、ワイヤレス管理インターフェイスを使用して Catalyst Center でデバイスを検出する必要があります。

Application Experience

アプリケーションエクスペリエンスのデータは、Cisco IOS-XE ルータプラットフォームから、Cisco Performance Monitor（PerfMon）機能とシスコのアプリケーション応答時間（ART）メトリックを使用して収集されます。

ルータプラットフォームの例には、ASR 1000、ISR 4000、CSR 1000v などがあります。Catalyst Center とのデバイスの互換性については、「*Cisco Catalyst Center Compatibility Matrix*」を参照してください。

Cisco Performance Monitor 機能が使用可能かどうかを確認するには、Cisco Feature Navigator ツールを使用します。[Research Features] をクリックし、フィルタフィールドで [Easy Performance Monitor Phase II] を追加します。

最適化アプリケーション パフォーマンス モニタリング

最適化アプリケーションパフォーマンスモニタリング（APM）は、デバイスでの NetFlow データの収集に関連するオーバーヘッドを軽減する機能です。APM は、Cisco IOS-XE ルータ、Cisco 9800 シリーズ ワイヤレス コントローラ、および Catalyst Center トラフィック テレメトリ アプライアンスでサポートされています。最小ソフトウェアバージョンについては、サポートされるプラットフォーム （199 ページ）を参照してください。

サポートされるプラットフォーム

次の表に、サポートされるプラットフォーム、データ収集のタイプ、およびソフトウェアとライセンスの要件を示します。

（注） Catalyst Center とのデバイスの互換性については、「*Cisco Catalyst Center Compatibility Matrix*」を参照してください。

Catalyst Center におけるアプリケーション エクスペリエンスとアプリケーションの可視性に対するシスコのプラットフォームのサポート		
プラットフォーム	**データ収集**	**注記**
Cisco IOS XE ルータ	アプリケーションエクスペリエンスのデータ収集。	• アクティブな NBAR2 ライセンスが必要。 • Cisco IOS XE 16.3 以上のソフトウェアバージョン。 • 最適化 APM の場合：Cisco IOS XE 17.3 以上のソフトウェアバージョン。
Catalyst 9000 シリーズ スイッチ	9200、9300、9400 のアプリケーション可視性のデータ収集	• Advantage ライセンスが必要です。 • Cisco IOS XE 16.10.1 以上のソフトウェアバージョン。 • IP ルーティングが有効にされている必要があります。
Cisco C9350 シリーズ スマートスイッチ	9200、9300、9400 のアプリケーション可視性のデータ収集	• Advantage ライセンスが必要です。 • Cisco IOS XE 26.1.1 以上のソフトウェアバージョン。
Cisco AireOS ワイヤレスコントローラ	アプリケーション可視性のデータ収集	• Advantage ライセンスが必要です。 • 8.8 MR2 ソフトウェアが必要：8.8.114.130 以上のバージョン。

Catalyst Center におけるアプリケーション エクスペリエンスとアプリケーションの可視性に対するシスコのプラットフォームのサポート		
プラットフォーム	データ収集	注記
Cisco 9800 シリーズ ワイヤレス コントローラ	Flex/Fabric SSID のアプリケーション可視性のデータ収集。 中央スイッチング/ローカル SSID および Flex/Fabric SSID のアプリケーション エクスペリエンスのデータ収集。	• アプリケーションの可視性：最適化 APM の場合、Cisco IOS XE 16.12.1 以上のソフトウェアバージョン。 • アプリケーションエクスペリエンス：ローカルモードの場合、Cisco IOS XE 16.12.1 以上のソフトウェアバージョン。 Flex/Fabric モードの場合、Cisco IOS XE 17.10.1 以上のソフトウェアバージョン。
Catalyst Center トラフィック テレメトリ アプライアンス	アプリケーションエクスペリエンスのデータ収集。	• Advantage ライセンスが必要です。 • 最適化 APM の場合：Cisco IOS XE 17.3 以上のソフトウェアバージョン。

デバイスでのアプリケーションテレメトリ有効化の基準

Catalyst Center では、新しい自動選択アルゴリズムに基づいてインターフェイスと WLAN を選択し、該当するすべてのインターフェイスと WLAN でアプリケーションテレメトリを自動的に有効にします。

（注）
- 従来のタギングベースのアルゴリズムがサポートされ、インターフェイスまたは WLAN の新しい自動選択アルゴリズムよりも優先されます。
- 自動選択アルゴリズムからタギングベースのアルゴリズムに切り替える場合は、タグ付き SSID をデバイスに対してプロビジョニングする前にテレメトリを無効にする必要があります。
- タグ付けベースのアルゴリズムは、グリーンフィールド展開とブラウンフィールド展開の両方に適用されます。

サポートされているすべてのプラットフォームに対して、従来のタグ付けベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムの両方を使用した、インターフェイスと WLAN の選択基準を次の表に示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
ルータ	• インターフェイスの説明に **lan** キーワードが含まれている。[1]、[2] • インターフェイスに管理 IP アドレス以外の IP アドレスがある。	• インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれのタイプでもない。 • WAN （注） インターフェイスにパブリック IP アドレスがあり、パブリック IP アドレスがインターフェイスを経由するルートルールがある場合、そのインターフェイスは WAN 側インターフェイスとして扱われます。 このコンテキストでは、パブリック IP アドレスはプライベート範囲にない（たとえば、192.168.x.x、172.16.y.y、10.z.z.z にない）か、システムの IP プールにない IP アドレスです。 ルートルールは動的に学習できます。このコンテキストでは、**show ip route** コマンドでこのインターフェイスを通過するパブリック IP アドレスへのルートは表示されません。 • ループバック • 管理インターフェイス：GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、FASTETHERNET1

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
スイッチ	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • スイッチポートがアクセスポートとして設定されている。 • スイッチポートに **switch-mode access** コマンドが設定されている。	• インターフェイスが物理インターフェイスである。 • アクセスポートにネイバーがない。 • インターフェイスが次のいずれのタイプでもない。 • 管理インターフェイス：FASTETHERNET0、FASTETHERNET1、GIGABITETHERNET0/0、MGMT0 • LOOPBACK0、Bluetooth、App Gigabit、WPAN、Cellular、Async • VSL インターフェイス
Cisco AireOS コントローラ	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合、Wireless Service Assurance（WSA）の処理が有効になります。すべての SSID がローカルモードの場合、NetFlow が有効になります。
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと最適化アプリケーション パフォーマンス モニタリング（APM）プロファイルおよび IOS 16.12.1 以降	WLAN プロファイル名が **lan** キーワードでタグ付けされている。[1、2]	SSID が混在している場合、つまり中央スイッチング、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control（AVC）の基本レコードが設定されます。すべての SSID で中央スイッチングを使用している場合、最適化 APM レコードが設定されます。 IOS 17.10 以降を備える Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Catalyst Center は、フレックスおよびファブリック SSID に対して、AVC 基本プロファイルではなく、APM プロファイルをプッシュします。
	（注） NetFlow 設定は、WLAN プロファイルに直接プッシュされるのではなく、「lan」キーワードを使用してポリシープロファイルにプッシュされます。ブラウンフィールド展開では、回避策は、「lan」キーワードを使用して新しいポリシープロファイルを作成し、既存のポリシープロファイルを削除して、新しいポリシープロファイルを既存の WLAN プロファイルと関連付けることです。ポリシープロファイルの名前を直接変更することはできません。	

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Catalyst Center トラフィックテレメトリアプライアンスと最適化APMプロファイルおよびIOS 17.3 以降	• インターフェイスの説明に **lan** キーワードが含まれている。[1、2] • インターフェイスが物理インターフェイスである。	• インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス（GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1）ではない。

[1] **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。
[2] ネットワークデバイスを再同期して、**lan** キーワードを読み取ります。

たとえば、従来のタグベースのアルゴリズムを使用してアプリケーションテレメトリを有効にする場合は、次の条件を満たす必要があります。

- この Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の WLAN プロファイル名 *test-lan* に **lan** キーワードが含まれている。

```
WLAN Profile Name              SSID                    VLAN Status
-------------------------------------------------------------------------------
1    test-lan                  test1-ssid              137   UP
```

- このスイッチのインターフェイスの説明の *wired-lan* に **lan** キーワードが含まれている。

```
interface GigabitEthernet1/0/1
description wired-lan
```

アプリケーションの正常性の前提条件

ここでは、ルータ、Cisco AireOS ワイヤレスコントローラ、スイッチのアプリケーションの正常性に関連する前提条件を示します。

ルータのアプリケーション エクスペリエンスの前提条件

- Cisco IOS XE ソフトウェアのアクティブな NBAR2 ライセンスが必要です。
- レイヤ 3 ネットワーク内のアプリケーションフローは可視化されません。
- 管理インターフェイスに関連付けられたトラフィックは、アプリケーションエクスペリエンスに含まれません。
- ポートは ETA に対して有効にできません。
- Assurance でアプリケーションの正常性データを表示するには、Catalyst Center とデバイスの間でクロックを同期する必要があります。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスと WLAN の新しい自動選択アルゴリズムにより、キーワード「**lan**」

でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）を参照してください。

スイッチのアプリケーション可視性の前提条件

- Cisco IOS XE ソフトウェアが必要です。
- Advantage ライセンスが必要です。
- **switchport mode access** コマンドが含まれているアクセスポートにのみ実装されます。
- L2 論理インターフェイスのサポートは使用できません。
- スイッチポートが AP に接続されて **switchport mode access** が設定されている場合、可視性が制限されます。
- ポートは ETA に対して有効にできません。
- IPv4 フローのみがモニターされます。
- これらの管理インターフェイスは、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。
  - GIGABITETHERNET0/0
  - MGMT0
  - FASTETHERNET0
  - FASTETHERNET1
  - GIGABITETHERNET0
- Assurance でアプリケーションの正常性データを表示するには、Catalyst Center とデバイスの間でクロックを同期する必要があります。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスと WLAN の新しい自動選択アルゴリズムにより、キーワード「**lan**」でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）を参照してください。

AireOS ワイヤレスコントローラのアプリケーション可視性の前提条件

- Advantage ライセンスが必要です。
- AireOS ソフトウェアを搭載したワイヤレスコントローラでのみサポートされ、IOS XE ソフトウェアを搭載したワイヤレスコントローラではサポートされません。
- Cisco AireOS ワイヤレスコントローラでは NetFlow を有効にする必要があります。

- Assurance でアプリケーションの正常性データを表示するには、Catalyst Center とデバイスの間でクロックを同期する必要があります。
- Flexible NetFlow（FNF）フローモニターは実装されません。代わりに、Client-app-stat-events チャネルに登録することにより、ストリーミングテレメトリを使用してアプリケーション可視性のデータが収集されます。
- 従来のタギングベースのアルゴリズム（キーワード「**lan**」を使用）もサポートされますが、インターフェイスとWLANの新しい自動選択アルゴリズムにより、キーワード「**lan**」でタグ付けしなくても、インターフェイスと WLAN でアプリケーションテレメトリを有効にできます。使用される基準については、デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）を参照してください。

Cisco 9800 シリーズ ワイヤレス コントローラのアプリケーション可視性の前提条件

- 最適化 APM には IOS XE ソフトウェアが必要です。デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）を参照してください。
- Assurance でアプリケーションの正常性データを表示するには、Catalyst Center とデバイスの間でクロックを同期する必要があります。

トラフィック テレメトリ アプライアンスでのアプリケーション エクスペリエンスの前提条件

- Advantage ライセンスが必要です。
- 最適化 APM には IOS XE ソフトウェアが必要です。デバイスでのアプリケーションテレメトリ有効化の基準 （200 ページ）を参照してください。
- Assurance でアプリケーションの正常性データを表示するには、Catalyst Center とデバイスの間でクロックを同期する必要があります。
- CAPWAP でカプセル化されたワイヤレストラフィックの可視性を有効にするには、アプライアンスで **ip nbar Classification tunneled-traffic CAPWAP** コマンドを手動で入力します。

アプリケーションテレメトリ設定のプロビジョニング

デバイスで NetFlow アプリケーションテレメトリ設定を設定できます。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、サイト、ビルディング、またはフロアを選択します。

ステップ 2 プロビジョニングするデバイスを選択します。

ステップ 3 [Actions] ドロップダウンリストから、[Telemetry] を選択し、次の手順のいずれかを実行します。

（注） [Enable Application Telemetry] および [Disable Application Telemetry] オプションは、デバイスで Catalyst Center からのアプリケーションテレメトリがサポートされている場合のみ有効です。

a) [アプリケーションテレメトリの有効化（Enable Application Telemetry）]：選択したデバイスでアプリケーションテレメトリを設定します。

b) [アプリケーションテレメトリの無効化（Disable Application Telemetry）]：選択したデバイスからアプリケーションテレメトリ設定を削除します。

ステップ 4 [Apply] をクリックします。

[Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で

[Application Telemetry] 列が表示されない場合は、列見出しの右端にある省略記号アイコン（⋮）をクリックし、[Application Telemetry] チェックボックスをオンにします。

ホストのアプリケーション エクスペリエンスの表示

ホストで稼働しているアプリケーションの質的および量的なメトリックを確認するには、次の手順を実行します。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （205 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （203 ページ）を参照してください。

手順

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、次の手順を実行できます。

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**] です。

（注） 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]、[7 Days] です。デフォルトは、[24 Hours] です。

b) テーブルでアプリケーション エクスペリエンス データを表示します。

- [Name]：アプリケーション名。
- [Health]：正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。詳細については、個別アプリケーションの正常性スコア （240 ページ）を参照してください。
- [Usage Bytes]：このアプリケーションに対してクライアントが転送したバイト数。
- [Average Throughput]：クライアントとサーバー間を流れているアプリケーション トラフィックのレート（Mbps 単位）。
- [DSCP]：アプリケーションの現在（[Observed]）とデフォルト（[Expected]）の DSCP 値。

（注） このメトリックは、最適化 APM については提供されません。

- [Packet Loss]：パケット損失のパーセンテージ（最小と平均）。
- [Network Latency]：ネットワーク遅延時間（最大と平均）（ミリ秒単位）。
- [Jitter]：ネットワーク上のデータパケット間の時間遅延のバリアンス（ミリ秒単位）（最大と平均）。

c) アプリケーション エクスペリエンス メトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、および [Application Server Latency] です。

（注） Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレスコントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

ネットワークデバイスのアプリケーションエクスペリエンスの表示

この手順を使用して、ネットワークデバイスで稼働しているアプリケーションの質的および量的なメトリックを表示できます。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （205 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （203 ページ）を参照してください。

手順

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、次の手順を実行できます。

a) [NetFlowエクスポータのサマリ（Netflow Exporter Summary）] には、Netflow パケット数、データレコード数、パケットドロップ、レコードドロップ、および合計バイト数が表示されます。

b) 対応するタブ（[Business Relevant]、[Business Irrelevant]、[Default]）をクリックして、特定のビジネスとの関連性グループからアプリケーション エクスペリエンス データを表形式で表示します。

（注） 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]（デフォルト）、または [7 Days] です。

c) 適切なフィルタ（[All VRFs] および [All Interfaces]）を使用して、特定の VRF または特定のルータインターフェイスのアプリケーション エクスペリエンス データをフィルタ処理します。



（注） [All VRFs] および [All Interfaces] フィルタは、ルータでのみ使用できます。

d) テーブルでアプリケーション エクスペリエンス データを表示します。

- [Name]：アプリケーション名。
- [Health]：正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。



（注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。

- [Usage Bytes]：このアプリケーションに対してクライアントが転送したバイト数。
- [Average Throughput]：クライアントとサーバー間を流れているアプリケーション トラフィックのレート（Mbps 単位）。
- [DSCP]：アプリケーションの現在（[Observed]）とデフォルト（[Expected]）の DSCP 値。



（注） このメトリックは、最適化 APM については提供されません。

- [Packet Loss]：パケット損失のパーセンテージ（最小と平均）。
- [Network Latency]：ネットワーク遅延時間（最大と平均）（ミリ秒単位）。
- [Jitter]：ネットワーク上のデータパケット間の時間遅延のバリアンス（ミリ秒単位）（最大と平均）。

e) アプリケーション エクスペリエンス メトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、[Application Server Latency]、および [Application Response Time] です。

（注） Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレスコントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

すべてのアプリケーションの正常性のモニター

サイトでアプリケーションのグローバルビューを取得するには、次の手順を使用します。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲または CIDR を使用したネットワークの検出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 ページ）を参照してください。
- ネットワークデバイスでアプリケーション テレメトリ プロファイルを有効にし、設定します。アプリケーションテレメトリ設定のプロビジョニング （205 ページ）を参照してください。
- アプリケーションの正常性の前提条件 （203 ページ）を参照してください。

手順

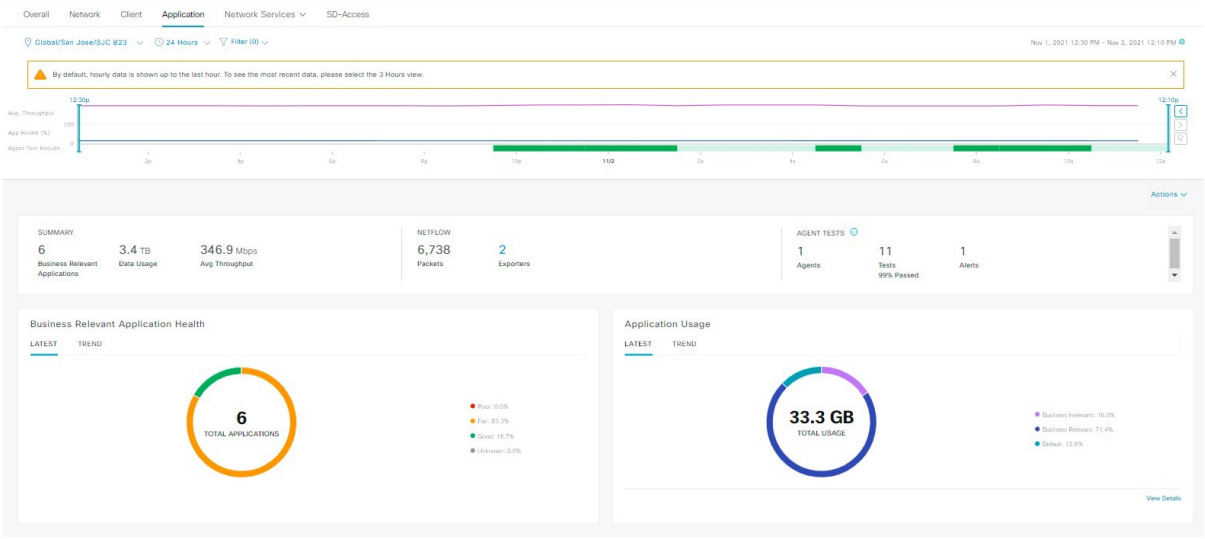
ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

図 *17 : [Application Health]* ダッシュボード



ステップ 3 次の機能には、[Application] 正常性ダッシュボードの上部のメニューバーを使用します。

[Application] 正常性ダッシュボードの上部のメニューバー	
アイテム	**説明**
Global [Location] ドロップダウン リスト	クリックすると、ロケーションアイコンが表示されます。ロケーションアイコンをクリックすると、[Site List View] が表示されます。特定のサイトまたは建物からアプリケーション情報を表示するには、適切な行で [Go to Site] 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。
[Time Range] の設定	ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 1. ドロップダウンメニューで範囲の長さ（[3 Hours]、[24 Hours]、または [7 days]）を選択します。 2. [Start Date] と時刻、[End Date] と時刻を指定します。 3. [Apply] をクリックします。
Filter	ドロップダウンリストから SSID を選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。
[Actions] ドロップダウン リスト	ドロップダウンリストから [Edit Dashboards] を選択すると、ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （434 ページ）およびカスタムダッシュボードの作成 （431 ページ）を参照してください。

[Application] 正常性ダッシュボードの上部のメニューバー	
アイテム	説明
アプリケーションの正常性タイムラインスライダ	健全なビジネス関連アプリケーションの割合、スループット、およびエージェントテスト結果を、より詳細な時間範囲で表示できます。タイムライン内でマウスカーソルを合わせると、特定の時刻の正常性スコアパーセンテージが表示されます。 時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。これにより、ダッシュボードダッシュレットに表示されるアプリケーションデータのコンテキストが設定されます。 タイムラインの右側にある矢印ボタンを使用して、最大 30 日間のデータを表示できます。

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

[Summary] ダッシュレット	
アイテム	説明
Summary	ネットワーク全体または選択したサイトにおけるビジネス関連アプリケーションの総数、データ使用量、および平均スループットを表示します。
ThousandEyes Tests	サポートされている Cisco Catalyst 9300 または 9400 シリーズ スイッチで実行されている ThousandEyes エンタープライズ エージェント、テスト、およびアクティブなアラートの総数を表示します。 次のタイプの ThousandEyes エージェントテストがサポートされています。 • ネットワークエージェントからサーバーへのテスト：ジッター、パケット損失、遅延などのネットワークデータを収集します。 • Web HTTP サーバーテスト：応答時間を含む HTTP サーバーデータを収集します。 • ネットワークエージェントからエージェントのテスト：ジッター、パケット損失、遅延などのネットワークデータを収集します。 • Voice RTP テスト：平均オピニオンスコア（MOS）、パケット損失、遅延、およびパケット遅延変動（PDV）を収集します。 ThousandEyes 統合を設定するには、『*Cisco Catalyst Center Administrator Guide*』の「*Configure ThousandEyes Integration*」を参照してください。

ステップ 5 次の機能については、[Application Health] ダッシュレットを使用します。

[Application Health] ダッシュレット	
アイテム	説明
[Business Relevant Application Health]	ビジネス関連アプリケーションの正常性スコアが含まれています。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 （240 ページ）を参照してください。 [最新（LATEST）] および [傾向（TREND）] タブをクリックして、ビジネス関連アプリケーションの正常性をその正常性スコアで表示します。 次のチャートが表示されます。 • 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。 • 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。 • [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は、次の操作を実行できます。 • グラフ内の特定の正常性カテゴリをクリックしてアプリケーションリストをフィルタ処理すると、[アプリケーション（Application）] テーブルに詳細情報が表示されます。 • 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。

[Application Health] ダッシュレット	
アイテム	説明
[Application Usage]	[最新（Latest）] をクリックすると、アプリケーションのビジネス関連グループ（ビジネス関連、ビジネス非関連、およびデフォルト）別に分類されたアプリケーション使用状況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。 [傾向（Trend）] をクリックすると、各カテゴリの帯域幅使用率が 24 時間にわたってどのように変化したかを示す積み上げ面グラフが表示されます。 （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。 • [傾向（Trend）] タブから [詳細の表示（View Details）] をクリックすると、スライドインペインが開き、アプリケーションの使用状況ごとのすべてのアプリケーションのグラフが [最新（Latest）] および [傾向（Trend）] タブとともに表示されます。スライドインペインでは、次の操作を実行できます。 • [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。 • 右上にある [内訳（Breakdown by）] 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（Application Group）] または [トラフィッククラス（Traffic Class）] 別にグラフをフィルタ処理できます。 • グラフ内の特定のアプリケーションをクリックすると、[アプリケーション（Application）] テーブル内のアプリケーションとその詳細情報（名前、正常性、ビジネス関連性、使用状況、平均スループット、パケット損失、遅延、ジッターなど）がフィルタ処理されます。

[Application Health] ダッシュレット	
アイテム	説明
[Top Applications by Throughput]	[LATEST] タブおよび [TREND] タブをクリックして、平均スループット値で上位 5 つのアプリケーションを表示します。各アプリケーション名をクリックすると、関連するアプリケーション 360 のページにリダイレクトされます。 • [詳細の表示（View Details）] をクリックすると、スライドインペインが開き、スループットで上位のアプリケーションのグラフが、[最新（Latest）] および [傾向（Trend）] タブとともに表示されます。スライドインペインでは、次の操作を実行できます。 • グラフ内の特定のアプリケーションをクリックすると、アプリケーションテーブル内のスループットで上位のアプリケーションとその詳細情報（名前、正常性、ビジネス関連性、使用状況、平均スループット、パケット損失、遅延、ジッターなど）がフィルタ処理されます。
[Top Endpoints by Throughput]	[最新（LATEST）] および [傾向（TREND）] タブをクリックすると、平均スループット値で上位 5 つのエンドポイントが表示されます。各エンドポイント識別子（IP アドレス）をクリックすると、関連するクライアント 360 のページにリダイレクトされます。 • [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでは、次の操作を実行できます。 • グラフ内の特定のエンドポイント/バーをクリックすると、[クライアントデバイス（Client Devices）] テーブル内のスループットで上位のエンドポイントとその詳細情報（識別子、IP アドレス、デバイスタイプ、正常性、ロケーション、最新の確認日時、スイッチ、VLAN ID など）がフィルタ処理されます。

[Application Health] ダッシュレット	
アイテム	説明
[Worst Applications]	[LATEST] タブおよび [TREND] タブをクリックして、正常性スコアで下位 5 つのアプリケーションを表示します。ドロップダウンメニューを使用して、[正常性スコア（Health Score）]、[ジッター（Jitter）]、[パケット損失（Packet Loss）]、[クライアントネットワーク遅延（Client Network Delay）]、[サーバーネットワーク遅延（Server Network Delay）]、[アプリケーション遅延（Application Delay）]などの特定のパフォーマンス基準でアプリケーションをフィルタ処理します。各アプリケーション名をクリックすると、関連するアプリケーション 360 のページにリダイレクトされます。 • [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインでは、次の操作を実行できます。 • グラフ内の特定のアプリケーションをクリックすると、アプリケーションテーブル内の下位アプリケーションで上位のエンドポイントとその詳細情報（名前、正常性、ビジネス関連性、使用状況、平均スループット、パケット損失、遅延、ジッターなど）がフィルタ処理されます。 詳細の表示：[View Details] をクリックすると、パケット損失やジッターなど、さまざまな正常性 KPI ごとに下位のアプリケーションに関する追加の詳細を含むスライドインペインが開きます。

ステップ 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	
アイテム	説明
Type	ビジネス関連グループに基づいてテーブルをフィルタリングします。オプションには、[Business Relevant]、[Business Irrelevant]、[Default]、[All] があります。
[Health]	アプリケーションの正常性スコアに基づいてテーブルをフィルタリングします。次のオプションがあります。 • [Poor]：正常性スコアが 1 ～ 3 のアプリケーション。 • [Fair]：正常性スコアが 1 ～ 3 のアプリケーション。 • [Good]：正常性スコアが 8 ～ 10 のアプリケーション。 • [All]：すべてのアプリケーション。 • [Unknown]：アプリケーションに正常性スコアを決定するための定性的なメトリックがありません。

[Application] ダッシュレット	
アイテム	説明
[Applications] テーブル	

[Application] ダッシュレット	
アイテム	説明
	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。 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。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。 • アプリケーションが NBAR の標準アプリケーションでない場合は、その HTTP ホスト名または SSL 共通名が表示されます（使用可能な場合）。これらのアプリケーションは、[Default] ビジネス関連性グループに割り当てられています。 アプリケーション名をクリックして、アプリケーションの 360 度ビューを表示することもできます。アプリケーションの正常性をモニター（226 ページ）を参照してください。 • アプリケーションの表には、新しいアプリケーションが一覧表示されます。 ms-teams-video、ms-teams-app-sharing、ms-teams-audio、ms-teams-media、および ms-teams アプリケーションは、関連するデータを収集する microsoft-teams の下にグループ化されています。 **microsoft-teams** をクリックして、Microsoft Teams アプリケーションの MS Teams 360 ビューを表示します。Microsoft Teams アプリケーションの正常性のモニターとトラブルシューティング （235 ページ）を参照してください。 webex-video、webex-audio、および webex-app-sharing は、関連するデータを収集する webex の下にグループ化されています。 [Webex] をクリックして、Webex アプリケーションの Webex 360 ビューを表示します。Webex アプリケーション正常性のモニターとトラブルシューティング （231 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]：有効な値は、[All]、[Business Relevant]、[Business Irrelevant]、および [Default] です。 • [使用量（Usage）]：このアプリケーションで転送されたバイト数。 • [Average Throughput]：クライアントとサーバー間のアプリケーショントラフィックのフローレート（Mbps 単位）。

[Application] ダッシュレット	
アイテム	説明
	• [Packet Loss（%）]：パケット損失の割合。 • [Network Latency]：Transmission Control Protocol（TCP）ベースのアプリケーションのネットワーク遅延時間（ミリ秒）。 • [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）。ジッターは、Real-time Transport Protocol（RTP）ベースのアプリケーションの場合です。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします。 3. [Apply] をクリックします。
	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。

ステップ 7 [ThousandEyes Enterprise Agent Tests] ダッシュレットには、次の機能が用意されています。

ThousandEyes Enterprise Agent Tests	
アイテム	説明
[Enterprise Agent Tests] テーブル	詳細な [ThousandEyes Enterprise Agent Tests] 情報を表形式で表示します。エージェントテーブルには、次の詳細情報が表示されます。 • [Test Name]：Enterprise エージェントテストの名前を表示します。 名前をクリックして、ThousandEyes エージェントページに移動します。 • [Test Type]：テストの種類の名前を表示します。 • [Target]：エージェントテストに使用する対象サーバーを表示します。 • [Device Name]：デバイス名を表示します。 • [Average Packet Loss（%）]：エージェントとサーバー間のデータ収集中のパケット損失の平均パーセンテージ。 • [Average 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）。ジッターはRTPベースのアプリケーション用です。 • [Average Latency]：TCPベースのアプリケーションのネットワーク遅延時間（ミリ秒）。 • [# of Active Alerts]：エージェントテスト中のアクティブなアラートの数を表示します。 • [# of Alerts]：エージェントテスト中のアラートの総数を表示します。 • [# of Failed Tests]：失敗したエージェントテストの数を表示します。 • MOS：平均オピニオン評点の平均値と最新値を表示します。 • PDV（ms）：パケット遅延変動の平均値と最新値を表示します。
[Install Agents]	[Install Agents] をクリックして、ThousandEyes Enterprise Agentsをインストールします。Cisco Catalyst 9000 シリーズスイッチ（Catalyst 9300 および 9400 など）では、スイッチ上でアプリケーションとして ThousandEyes Enterprise Agents を直接実行できます。ThousandEyes Enterprise Agent のインストール（221 ページ）を参照してください。
[Manage Agents]	[Manage Agents] をクリックして、インストールされているすべてのエンタープライズエージェントを管理し、エージェントの管理ウィンドウでアンインストール、アップグレード、開始、停止、再同期、テストの割り当て、または新しいテストの追加を実行します。実行中、停止、失敗、および進行中のエージェントなどの、グローバルエージェントの統計を表示できます。企業エージェントとテストの管理 （224 ページ）を参照してください。

ThousandEyes Enterprise Agent Tests	
アイテム	説明
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします。 3. [Apply] をクリックします。
	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。

ThousandEyes Enterprise Agent のインストール

次の手順を使用して、Catalyst 9300 および 9400 シリーズ スイッチと IE3500 および IE9300 シリーズ スイッチに ThousandEyes Enterprise エージェントをインストールします。以前にエージェントをインストールしている場合は、エージェントを管理し、エージェントで実行するテストを追加することができます。

Catalyst Center は、CPU アーキテクチャ全体で ThousandEyes のマルチバリアント アプリケーション パッケージをサポートしています。ThousandEyes の場合、Catalyst Center は、x86_64 や aarch64 など、同じアプリケーションファミリのアーキテクチャ固有のバリアントを認識できます。インストールまたはアップグレード中にデバイスごとに適切なバリアントを自動的に解決し、バリアントを認識したライフサイクル運用を提供します。

始める前に

- ThousandEyes エージェントアカウントが Catalyst Center に接続されていることを確認してください。詳細については、『Cisco Catalyst Center Administrator Guide』の「*Configure ThousandEyes Integration*」を参照してください。

手順

ステップ 1 [Connect ThousandEyes] ウィンドウで、[ThousandEyes Account Group] ドロップダウンリストから [ThousandEyes] アカウントグループを選択し、[Next] をクリックします。

ステップ 2 [Select Applications] ウィンドウで、エージェントをインストールし、拡張アプリケーション モニタリングを実行するアプリケーションを次のオプションから選択します。

- Microsoft 365

- Slack
- Webex
- Salesforce
- Zoom
- AWS コンソール
- カスタムアプリケーション。

ステップ 3 [Configure Application] ウィンドウでは、選択したアプリケーションに基づいてアプリケーションを設定できます。

選択内容	解決策
Microsoft 365	次の Microsoft 365 パラメータとテストを設定します。 • **サブドメイン名** - Microsoft 365 サブドメイン名を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • 追加するテストを選択するには、[Test included] チェックボックスをオンにします。使用可能なテストは、 **M365: OneDrive Web**、 **M365: ログインWeb**、 **M365: アプリケーションポータルWeb**、 **M365: Sharepoint Web**、 **M365: Outlook Web**。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。
Slack	次の Slack パラメータとテストを設定します。 • **サブドメイン名** - Slack サブドメイン名を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは **Slack - Web** および **Slack - api.slack.com**です。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。
Webex	次の Webex パラメータおよびテストを設定します。 • **Webex サイト ID**：Webex サイト ID を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは **Webex - Server**です。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。

選択内容	解決策
Salesforce	次の Salesforce パラメータとテストを設定します。 • **サブドメイン名**：Salesforce のサブドメイン名を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは **Salesforce - Classic**、**Salesforce - Lighting**、**Salesforce - ログイン**、**Salesforce - Files**、および **Salesforce - Static Assets** です。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。
Zoom	次の Zoom パラメータとテストを設定します。 • **サブドメイン名**：Zoom のサブドメイン名を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは **Zoom - Web** です。アプリケーションでテストを実行するには、少なくとも1 つのテストを設定する必要があります。
AWS コンソール	次の AWS コンソールパラメータとテストを設定します。 • **テンプレート**：AWS テンプレート名を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは **AWS - Web** です。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。
カスタムアプリケーション	カスタム アプリケーション パラメータおよびテストを設定します。 • **ターゲットドメイン**：ターゲットドメイン URL または IP アドレスを入力します。 • **ターゲットポート**：ターゲットポート番号を入力します。 • **テスト間隔**：[Test interval] ドロップダウンリストからテスト間隔を選択します。テスト間隔の値は、1 分、2 分、5 分、10 分、15 分、30 分、1 時間です。 • **テンプレート名**：AWS テンプレート名を入力します。 • テストを追加するには、[Test included] チェックボックスをオンにします。使用可能なテストは、**カスタムアプリケーション - ネットワーク** です。アプリケーションでテストを実行するには、少なくとも 1 つのテストを設定する必要があります。最大 10 個のカスタムアプリケーションを作成できます。

または

（オプション）アプリケーションの設定をスキップする場合は、[Continue without an application] を選択し、[Next] をクリックします。

ステップ 4 [Select Locations] ウィンドウで、ロケーション ドロップダウン リストからロケーションを選択し、[Next]をクリックします。

ステップ 5 [Select Switches] で、スイッチを選択し、**スイッチ設定**と **プロキシ設定**を設定します。

ステップ 6 [Summary] ウィンドウで、アプリケーション モニタリング設定を確認し、[Complete setup] をクリックします。

次のタスク

企業エージェントとテストを管理できるようになりました。「Manage Enterprise Agents and Tests」を参照してください。

企業エージェントとテストの管理

この手順を使用して、インストールされているすべてのエンタープライズエージェントを管理します。[Manage Agents] ページで、アンインストール、アップグレード、起動、停止、再同期、テストの割り当て、または新しいテストの追加を行うことができます。

始める前に

ThousandEyes Enterprise エージェントとテストがインストールされていることを確認します。エージェントをインストールしてテストを追加する場合は、ThousandEyes Enterprise Agent のインストール （221 ページ）を参照してください。

手順

ステップ 1 Catalyst Center のホームページで、**Assurance** タブをクリックし、**[Health]** > **[Applications]** の順に選択します。

[Applications] ページが表示されます。

ステップ 2 [ThousandEyes Enterprise Agent Tests] テーブルから、[Manage Agents] をクリックします。[ThousandEyes Integration Enterprise Agents] ウィンドウが表示されます。ThousandEyes が展開されているスイッチとハブのみを表示できます。

グローバルエージェントの統計エリアには、[All Agents] テーブルの実行中、停止、失敗、および進行中のエージェントのステータスが表示されます。

ステップ 3 [Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用して、サイト、ビルディング、またはエリアを見つけます。

ステップ 4 [Enterprise Agents] ページを使用して、次の情報を表示します。

Enterprise Agents	
アイテム	説明
グローバルエージェント統計値	アプリケーション内の実行中、停止、失敗、および進行中のエージェントの数を表示します。
[All Agents] テーブル	エージェントのステータス、ホスト名、テスト、テストタイプなどを表示します。 • [All Agents] テーブルから、チェックボックスをオンにしてエージェント名を選択し、次のタスクを実行します。 • アンインストール • アップグレード • Start • 停止 • Resync • テストの割り当て • 新しいテストの追加 • [All Agents] テーブルで、ホスト名をクリックするとスライドインペインが開き、エージェントの詳細タブには、リソース、ネットワーク、およびDockerランタイムオプションなどのエージェントデータが表示されます。テクニカルサポートログをダウンロードするには、[Tech Support Logs] をクリックします。 • スライドインペインの [Tests] タブをクリックすると、エージェントに追加されたテスト名、テストタイプ、間隔、およびターゲット値が表示されます。エージェントからテストを切り離すには、テスト名の列の横にあるチェックボックスをオンにして、 [Detach from this agent] をクリックします。

ステップ 5 エージェントをアップグレードするには、次の手順に従います。

a) [すべてのエージェント（All Agents）] リストで、アップグレードするエージェントの横にあるチェックボックスをオンにします。

b) **[Upgrade]** をクリックします。[エージェントのアップグレード（Agent(s) Upgrade）] スライドインペインが表示されます。

c) [プロキシタイプ（Proxy type）] ドロップダウンからプロキシタイプを選択して、プロキシを設定します。

- [直接（Direct）] : 追加設定は必要ありません。
- [静的（Static）] : [プロキシのロケーション（Proxy location）] と [プロキシバイパスリスト（Proxy bypass list）] を入力し、必要に応じて [プロキシ認証タイプ（Proxy Auth type）] を選択します。

- [PAC]：[PACファイルURL（PAC File URL）] を入力し、必要に応じて [プロキシ認証タイプ（Proxy Auth type）] を選択します。
- （オプション）Docker ランタイムオプションをカスタマイズするには、[以下のDockerランタイムオプションでのアップグレード（Upgrade with below docker runtime options）] スイッチを「オン」の位置に切り替え、[追加のDockerランタイムオプション（Additional Docker runtime options）] フィールドに必要な設定を入力します。
- [アップグレード（Upgrade）] をクリックしてプロセスを開始します。[ステータス（Status）] 列をモニターして、エージェントが更新されたバージョンに正常に移行したことを確認します。

アプリケーションの正常性をモニター

この手順を使用して、特定のアプリケーションの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

ステップ 3 [Application] テーブルで、アプリケーション名をクリックします。

[Application 360] ウィンドウが開き、アプリケーションの 360 度ビューが表示されます。

ステップ 4 左上隅にある時間範囲設定（  ）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

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

ステップ 5 特定のロケーションのアプリケーション情報を表示するには、[Location] ドロップダウンリストからロケーションを選択します。

ステップ 6 [Filter] ドロップダウンリストから SSID を選択し、[Apply] をクリックして特定の SSID の情報を表示します。

ステップ 7 アプリケーションの正常性タイムラインスライダを使用して、より詳細な時間範囲のアプリケーションの正常性スコアやアプリケーションの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Health Score]：特定の時点の正常性スコアが表示されます。[Quality] 領域のメトリックの色分けは正常性スコアに対応しています。

[Quality]：[Quality] 情報領域には、遅延、ジッター、およびパケット損失に関する情報が表示されます。遅延については、クライアントとアプリケーションの間の遅延に関する次の情報が表示されます。

- LAN の遅延：クライアントとルータの間の遅延（ミリ秒）。
- WAN の遅延：ルータとサーバーの間の遅延（ミリ秒）。
- アプリケーションの遅延：サーバーとアプリケーションの間の遅延（ミリ秒）。

[Under Maintenance]：デバイスが特定の期間にメンテナンスモードになっている場合、特定のデバイス名が [Under Maintenance] バナーの下に表示されます。

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、[Application 360] ウィンドウに表示されるアプリケーションデータのコンテキストが設定されます。

ステップ 8 タイムラインの下にある [Application Details] 領域で、次の情報を確認します。

Application details	
アイテム	**説明**
[Health Score]	アプリケーションの正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、およびジッター）の加重平均に基づいて計算されます。 （注） 正常性スコアは、Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。
[Time and Date] 範囲	[Application 360] ウィンドウに表示されているデータの時刻と日付の範囲が表示されます。
[Business Relevance [Traffic Class] **Category**	アプリケーションの次世代 Network-Based Application Recognition（NBAR）分類情報を表示します。
[Issues] タブ	クリックすると、問題のリストが表示されます。
[Exporters] タブ	クリックすると、NetFlow トラフィックを Catalyst Center に送信するデバイスのリストとその他の詳細情報が表示されます。

ステップ 9 [Issues] をクリックして、次の情報を確認します。

ISSUES
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、次のタスクを実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （299 ページ）を参照してください。

ステップ 10 [Exporters] をクリックして、次の情報を確認します。

Exporters	
アイテム	説明
[Device]	NetFlow トラフィックを Catalyst Center に送信しているデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アプライアンスなど）のリストが表示されます。 （注） 特定の時間範囲で、メンテナンスモードのデバイスに対して次の警告メッセージが表示されます。 「警告アイコンが付いたエクスポータは、選択した期間中、メンテナンスモードになっていました。（The exporters with warning icon were in maintenance mode during the selected period of time.）」

Exporters	
アイテム	説明
[Health Score]	直近の 5 分間の正常性スコア。正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、ジッターなど）に基づいて計算されます。 （注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよびCisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。
[Traffic Class]	該当する場合にアプリケーションの NBAR 分類情報が表示されます。
[Go to Device 360]	クリックすると、特定のデバイスの [Device 360] ウィンドウが開きます。

ステップ 11 メトリックチャートを表示するには、次の手順を実行します。

- ルータおよびアプライアンスの場合は、エクスポータの行をクリックします。その行の下に、使用状況、平均スループット、パケット損失、ジッター、および遅延のメトリックについてのチャートが表示されます。
- スイッチおよびワイヤレスコントローラの場合は、デバイス名をクリックします。スライドインペインが開き、使用状況および平均スループットのメトリックについてのチャートが表示されます。

  また、スライドインペインで [Device 360] をクリックして、特定のデバイスの [Device 360] ウィンドウを開くこともできます。

メトリックチャート	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Thoughput]	クライアントとサーバーの間のアプリケーション トラフィックのレート（Mbps）。
[Packet Loss]	パケット損失のパーセンテージ（最大と平均）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。

メトリックチャート	
チャート	説明
[Latency]	ネットワークの遅延時間（最大と平均）（ミリ秒単位）。次の遅延のチャートが提供されます。 • ネットワーク遅延 • クライアントネットワークの遅延 • サーバーネットワークの遅延 • アプリケーション ネットワークの遅延 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Jitter]	ネットワーク上のデータ パケット間の時間遅延（最大および平均）の差異（ミリ秒単位）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[DSCP]	• [Observed]：アプリケーションの現在の DSCP 値。 • [Expected]：NBAR によって割り当てられたデフォルトの DSCP 値。 （注） このメトリックは、最適化 APM については提供されません。

ステップ 12 [Application Endpoint] のテーブルで、アプリケーションにアクセスしているクライアントのリストを確認します（メトリックチャートの後に表示されます）。

Catalyst Center で管理されるクライアントのみを表示する場合は、[Managed Clients] タブをクリックします。

このテーブルには、各クライアントの詳細が表示されます。これには、識別子（ユーザー ID、ホスト名、IP アドレス、MAC アドレスのうち、この順序で使用可能なもの）、クライアント、クライアントの正常性、アプリケーションの正常性、使用状況、デバイスタイプ、MAC アドレス、VLAN ID などの情報が含まれます。

アクティブクライアントについては、[Identifier] 列をクリックして [Client 360] ウィンドウを開くことができます。

このテーブルには、クライアントが最大 100 個まで表示されます。追加のクライアントを表示するには、[Show More] をクリックします。

Webexアプリケーション正常性のモニターとトラブルシューティング

この手順を使用して、Webex アプリケーションの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

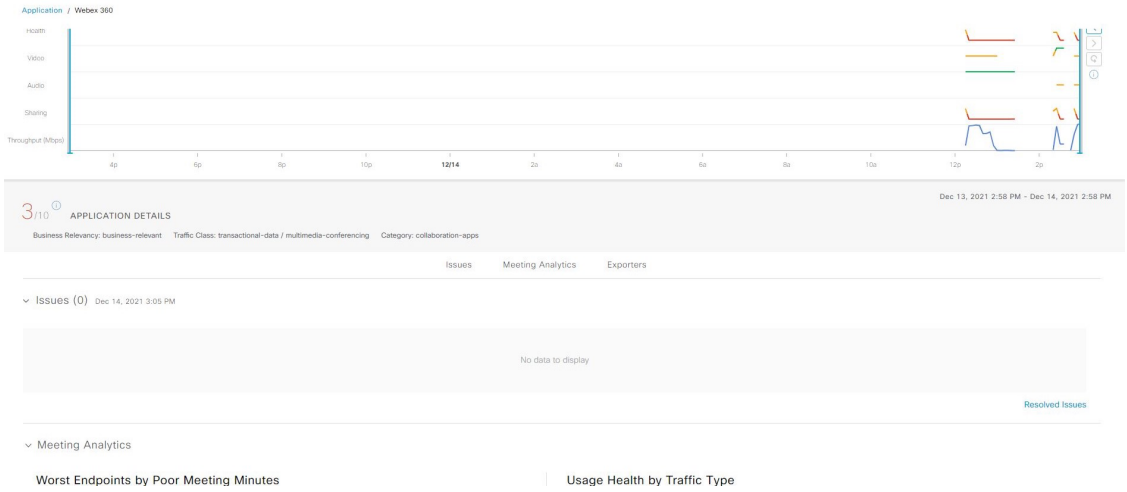
ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

ステップ 3 [Application] テーブルで、[Webex] アプリケーションをクリックします。

[Webex 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。

図 *18 : [Webex 360]* ウィンドウ



ステップ 4 [Summary] ダッシュレットを使用して、ネットワーク全体または選択したサイト内のデータ使用量、平均スループット、およびアクティブなクライアントの総数を表示します。

ステップ 5 左上隅にある時間範囲設定（）をクリックして、ウィンドウに表示するアプリケーションデータの時間範囲を指定します。

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

ステップ 6 特定のロケーションのアプリケーション情報を表示するには、[Location] ドロップダウンリストからロケーションを選択します。

ステップ 7 アプリケーションの正常性タイムラインスライダを使用して、より詳細な時間範囲のアプリケーションの正常性スコア、サブアプリケーション、ネットワーク品質やアプリケーションの品質情報を確認します。

タイムライン内で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。

ステップ 8 タイムラインの下にある [Application Details] 領域で、次の情報を確認します。

Application details	
アイテム	**説明**
[Health Score]	アプリケーションの正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、およびジッター）の加重平均に基づいて計算されます。
[Time and Date] 範囲	[Webex 360] ウィンドウに表示されているデータの時間と日付の範囲が表示されます。
[Business Relevance [Traffic Class] **Category**	アプリケーションの次世代 Network-Based Application Recognition（NBAR）分類情報を表示します。
[Issues] カテゴリ	クリックすると、問題のリストが表示されます。
[Meeting Analytics]	クリックして、ミーティング分析データを表示します。
[Exporters] タブ	クリックすると、NetFlow トラフィックを Catalyst Center に送信するデバイスのリストとその他の詳細情報が表示されます。

ステップ 9 [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、次のタスクを実行できます。

- 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 （299 ページ）を参照してください。

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

不良な会議時間の比較による下位エンドポイント
[Latest] および [Trend] グラフをクリックして、不良な会議時間の比較による下位エンドポイントのステータスを表示します。[By Percentage] または [By Total Poor Minutes] に基づいてデータをフィルタリングできます。

トラフィックタイプ別の使用状況正常性
[Latest] をクリックして、オーディオ、共有、およびビデオのトラフィックタイプに基づいた使用状況正常性を確認するグラフを表示します。 [Trend] をクリックして、オーディオ、共有、ビデオのトラフィックタイプに基づいた使用状況正常性を示すグラフを表示します。 グラフの色のセグメントにカーソルを合わせると、正常性のパーセンテージを表示できます。

ステップ 11 [Exporters] をクリックして、次の情報を確認します。

Exporters	
アイテム	**説明**
[Device]	NetFlow トラフィックを Catalyst Center に送信しているデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アプライアンスなど）のリストが表示されます。 （注） 特定の時間範囲で、メンテナンスモードのデバイスに対して次の警告メッセージが表示されます。 「警告アイコンが付いたエクスポータは、選択した期間中、メンテナンスモードになっていました。（The exporters with warning icon were in maintenance mode during the selected period of time.）」
[Health Score]	直近の 5 分間の正常性スコア。正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、ジッターなど）に基づいて計算されます。 （注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。
[Traffic Class]	該当する場合にアプリケーションの NBAR 分類情報が表示されます。
[Go to Device 360]	クリックすると、特定のデバイスの [Device 360] ウィンドウが開きます。

ステップ 12 オーディオ、ビデオ、共有のメトリックチャートを表示するには：

メトリックチャート	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Thoughput]	クライアントとサーバーの間のアプリケーショントラフィックのレート（Mbps）。チャートにカーソルを合わせると、オーディオ、ビデオ、および共有のスループット値を表示できます。
[Packet Loss]	パケット損失のパーセンテージ（最大と平均）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Latency]	ネットワークの遅延時間（最大と平均）（ミリ秒単位）。次の遅延のチャートが提供されます。 • ネットワーク遅延 • クライアントネットワークの遅延 • サーバーネットワークの遅延 • アプリケーション ネットワークの遅延 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Jitter]	ネットワーク上のデータ パケット間の時間遅延（最大および平均）の差異（ミリ秒単位）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。

ステップ 13 [Application Endpoint] のテーブルで、アプリケーションにアクセスしているクライアントのリストを確認します（メトリックチャートの後に表示されます）。

このテーブルには、各クライアントの詳細が表示されます。これには、識別子（ユーザー ID、ホスト名、IPアドレス、MACアドレスのうち、この順序で使用可能なもの）、クライアント、クライアントの正常性、アプリケーションの正常性、使用状況、デバイスタイプ、MAC アドレス、VLAN ID などの情報が含まれます。

アクティブクライアントについては、[Identifier] 列をクリックして [Client 360] ウィンドウを開くことができます。

このテーブルには、クライアントが最大100個まで表示されます。追加のクライアントを表示するには、[Show More] をクリックします。

Microsoft Teamsアプリケーションの正常性のモニターとトラブルシューティング

この手順を使用して、**Microsoft Teams** アプリケーションの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall Health] ダッシュボードが表示されます。

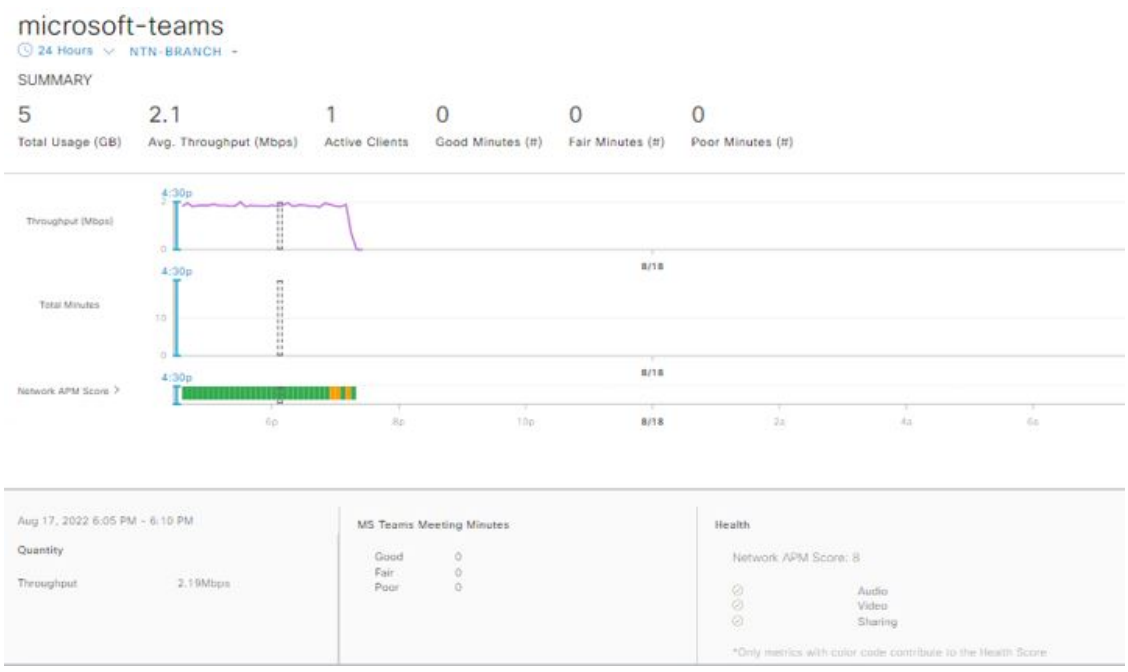
ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

ステップ 3 [Applications] テーブルで、[microsoft-teams] アプリケーションをクリックします。

アプリケーションの 360° ビューを提供する [MS Teams 360] ウィンドウが表示されます。

図 *19 : [MS Teams 360]* ウィンドウ



ステップ 4 [Summary] ダッシュレットを使用して、ネットワーク全体または選択したサイト内のデータ使用量、平均スループット、アクティブなクライアント、良好だった時間、普通だった時間、不良だった時間の総数を表示します。

ステップ 5 左上隅にある時間範囲設定（）をクリックして、ウィンドウに表示するアプリケーションデータの時間範囲を指定します。

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

（注） デフォルトでは、アプリケーションダッシュボードで選択したサイトと時間範囲が MS Teams 360 に表示されます。

ステップ 6 アプリケーションの正常性タイムラインスライダーを使用して、**スループット**、**合計分**、および**ネットワーク APM スコア**を表示します。

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。

（注） ネットワーク APM スコアは、管理対象ネットワークデバイスからエクスポートされた NetFlow に基づいて計算される正常性スコアです。APM の詳細については、「サポートされるプラットフォーム （199 ページ）」[英語] を参照してください。

ステップ 7 タイムラインの下にある [Application Details] 領域で、次の情報を確認します。

Application details	
アイテム	**説明**
[Time and Date] 範囲	[MS Teams 360] ウィンドウに表示されているデータの時間と日付の範囲が表示されます。
[Health]	**オーディオ**、**ビデオ**、および**共有**の正常性スコアを表示します。
[Quantity]	**スループット**データを表示します。
[MS Teams Meeting Minutes]	**良好だった時間**、**普通だった時間**、**不良だった時間**に関する情報を表示します。
[Business Relevance [Traffic Class] **カテゴリ**	アプリケーションの次世代 Network-Based Application Recognition（NBAR）分類情報を表示します。
[Issues] カテゴリ	クリックすると、問題のリストが表示されます。
[Meeting Analytics]	クリックして、ミーティング分析データを表示します。

Application details	
アイテム	説明
[Exporters] タブ	クリックすると、NetFlow トラフィックを Catalyst Center に送信するデバイスのリストとその他の詳細情報が表示されます。

ステップ 8 [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、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、次のタスクを実行できます。

- 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 （299 ページ）を参照してください。

ステップ 9 次の機能には、[Meeting Analytics] ダッシュレットを使用します：

Meeting Analytics	
アイテム	説明
上位アクセスデバイス	[Latest] および [Trend] チャートをクリックすると、上位アクセスデバイスのステータスを良好だった時間および不良だった時間別に表示します。 [By Poor Meeting Minutes]、[By Total Meeting Minutes]、[By Total Usage]、および [By Poor Network APM Score] に基づき、データをフィルタリングできます。
Top Endpoints	[Latest] および [Trend] チャートをクリックすると、上位エンドポイントのステータスを良好だった時間および不良だった時間別に表示します。 [By Poor Meeting Minutes]、[By Total Meeting Minutes]、[By Total Usage]、および [By Poor Network APM Score] に基づき、データをフィルタリングできます。

ステップ 10 [Exporters] をクリックして、次の情報を確認します。

Exporters	
アイテム	説明
[Device]	NetFlow トラフィックを Catalyst Center に送信しているデバイスを表示します。 （注） 特定の時間範囲で、メンテナンスモードのデバイスに対して次の警告メッセージが表示されます。 「警告アイコンが付いたエクスポータは、選択した期間中、メンテナンスモードになっていました。（The exporters with warning icon were in maintenance mode during the selected period of time.）」
[Health Score]	直近の 5 分間の正常性スコア。正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、ジッターなど）に基づいて計算されます。 （注） 正常性スコアは、 Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。
[Traffic Class]	該当する場合、アプリケーションの NBAR 分類情報が表示されます。

ステップ 11 オーディオ、ビデオ、共有のメトリックチャートを表示するには：

メトリックチャート	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Thoughput]	クライアントとサーバーの間のアプリケーショントラフィックのレート（Mbps）。チャートにカーソルを合わせると、オーディオ、ビデオ、および共有のスループット値を表示できます。
[Packet Loss]	パケット損失のパーセンテージ（最大と平均）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。
[Jitter]	ネットワーク上のデータ パケット間の時間遅延（最大および平均）の差異（ミリ秒単位）。 （注） このメトリックは、スイッチおよびワイヤレスコントローラについては提供されません。

ステップ 12 [Application Endpoint] のテーブルで、アプリケーションにアクセスしているクライアントのリストを確認します（メトリックチャートの後に表示されます）。

このテーブルには、各クライアントの詳細が表示されます。これには、識別子（ユーザー ID、ホスト名、IP アドレスまたは MAC アドレス）、クライアントの正常性、ネットワーク APM スコア、Microsoft Teams スコア、使用状況、デバイスタイプ、MAC アドレス、VLAN ID などが含まれます。

アクティブクライアントについては、[Identifier] カラムをクリックして [Client 360] ウィンドウを開くことができます。

このテーブルには、クライアントが最大 100 個まで表示されます。追加のクライアントを表示するには、[Show More] をクリックします。

アプリケーションの正常性スコアの設定

アプリケーションの正常性スコアを設定するには、次の手順を実行します。トラフィッククラスごとに KPI のしきい値を変更し、計算に含める KPI を指定すると、アプリケーションの正常性スコアの計算をカスタマイズできます。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **[Settings]** > **[Health Score Settings]**の順に選択します。

ステップ 2 [Application Health] タブをクリックします。

ステップ 3 アプリケーションカテゴリのタブをクリックして、正常性スコアの計算設定をカスタマイズします。

このタブには、アプリケーションの正常性スコアの計算に影響する KPI が表示されます。

ステップ 4 [KPI Name] 列で、KPI 名のリンクをクリックします。

KPI のスライドインペインが表示されます。

ステップ 5 KPI の正常性スコアを次のように設定します。

a) [Poor]、[Fair]、および [Good] 正常性スコアの KPI しきい値をカスタマイズします。
b) [Weight]：有効な重みは 1 ー 10 です。重みが大きいほど、KPI がアプリケーションの正常性に及ぼす影響は大きくなります。
c) この KPI を正常性スコアの計算に含める場合は、[Include for health score] チェックボックスをオンにします。
d) デフォルトの KPI 設定を復元するには、[Reset to Default] をクリックします。

ステップ 6 [Apply] をクリックします。

アプリケーションのヘルススコアと KPI メトリックスの理解

ここでは、アプリケーションのヘルス スコアと KPI メトリックの計算方法について説明します。

全体的なアプリケーション正常性スコア

アプリケーション正常性スコアは、正常なビジネス関連アプリケーションの数（正常性スコアが 8 ～ 10）をビジネス関連アプリケーションの総数で割ったパーセンテージです。このスコアは直近の 5 分間に対して計算されます。

例：90％（正常性スコア）=90（正常性スコアが 8 ～ 10 のビジネス関連アプリケーション数）÷ 100（ビジネス関連アプリケーションの総数）

個別アプリケーションの正常性スコア

個別アプリケーションの正常性スコアは、アプリケーションの定性的メトリック（パケット損失、ネットワーク遅延、およびジッター）の加重平均に基づいて計算されます。

個別アプリケーションの正常性は 1 ～ 10 のスケールで測定され、10 が最高スコアになります。個別アプリケーションの正常性スコアを計算するには、次の式を使用します。

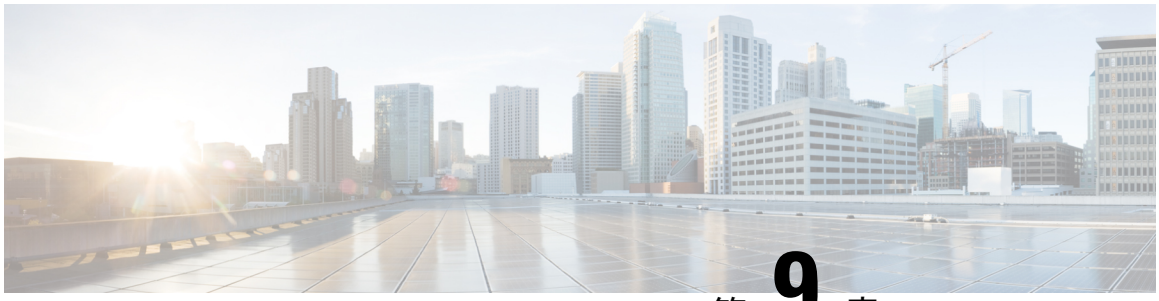
個別アプリケーションの正常性スコア = (Latency_Weight * Latency_VoS_Score + Jitter_Weight * Jitter_VoS_Score + PacketLoss_Weight * PacketLoss_VoS_Score) ÷ (Latency_Weight + Jitter_Weight + PacketLoss_Weight)

（注） 正常性スコアは、Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。

個別アプリケーションの正常性スコアを計算するためのワークフローには次のようなものがあります。

1. KPI（ジッター、遅延、パケット損失）を取得します。
2. フローレコードの DSCP 値に基づいて、アプリケーションのトラフィッククラスを決定します。
3. 各トラフィッククラスと KPI メトリックの Cisco Validated Design（CVD）しきい値を使用して、KPI 番号をサービススコア検証（VoS スコア）に変換します。
4. アプリケーションのトラフィッククラスと許容度レベルに基づいて、KPI の重み付けを行います。重み付けは RFC4594 に基づきます。

5. アプリケーションの正常性スコアを計算します。これは、パケット損失、ネットワーク遅延、およびジッターの加重平均です。



第 9 章

ネットワークサービスの監視

- AAA ネットワークサービスのモニター （243 ページ）
- DHCP ネットワークサービスの監視 （247 ページ）
- DNS ネットワークサービスの監視 （252 ページ）

AAA ネットワークサービスのモニター

この手順に従って、ネットワーク内の ワイヤレスコントローラ およびスイッチから報告されたすべての AAA サーバートランザクションを表示およびモニターします。

（注） **AAA 制約事項**

- AAAネットワークサービスは、ワイヤレスクライアント、有線クライアント、およびローカルモードをサポートします。
- AAA ネットワークサービスでは、次のことはサポートされていません。
  - Cisco AireOS ワイヤレスコントローラ、
  - フレックスモードまたはファブリックモード

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ バージョン 17.6.1 以降がインストールされていて、ローカルモード AP を使用して展開されていることを確認します。Assurance は、ユーザーのアクセス範囲を特定のネットワークサイトに制限する、サイトベースのロールベースアクセスコントロール（SRBAC）をサポートしています。サイトとデバイス、および関連する AAA ネットワークサービスにアクセスできるようにする必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

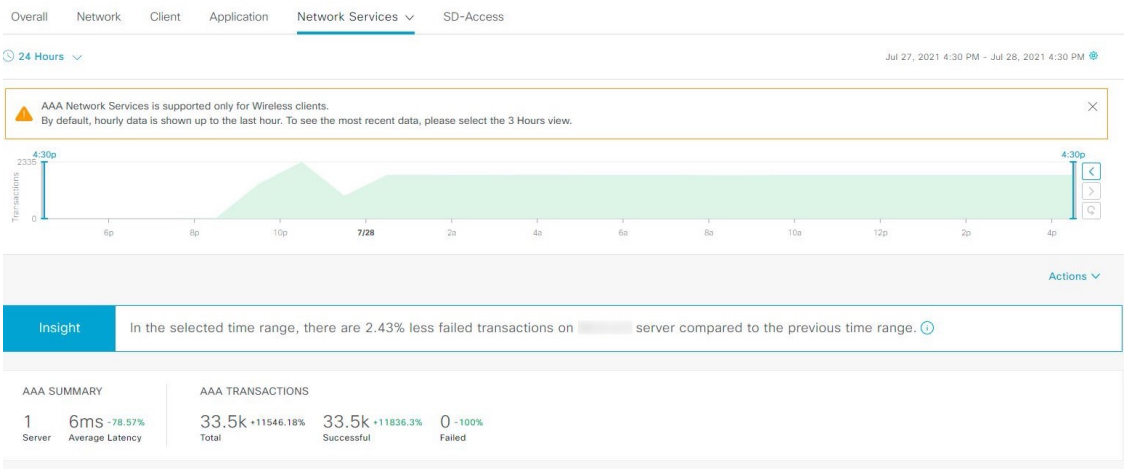
手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

ステップ 2 **[Network Services]** > **[AAA]**を選択します。

[AAA] ダッシュボードが表示されます。

図 *20 : [AAA]* ダッシュボード



ステップ 3 左上隅にある時間範囲設定（）をクリックして、表示するデータの時間範囲を指定します。

a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 4 右上隅にある自動更新設定（）をクリックして、サポートされている Assurance ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 5 タイムラインスライダを使用して、一定期間における AAA サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の AAA サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 6 タイムラインスライダの下にある **Actions** ドロップダウンリストをクリックして、次の機能を実行できます。

- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （434 ページ） およびカスタムダッシュボードの作成 （431 ページ） を参照してください。

ステップ 7 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した AAA サーバートランザクションの割合を表示します。

ステップ 8 [AAA Summary] ダッシュレットを使用して、次の情報を確認できます。

AAA サマリー	
アイテム	**説明**
AAA の概要	ネットワークの AAA サーバーの数と平均遅延（ミリ秒単位）を表示します。
AAA トランザクション	ネットワーク内の AAA トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合を表示します。

ステップ 9 次の機能には AAA サーバーダッシュレットを使用します。

最も大きい遅延が発生した上位サイト

チャートには、AAA サーバーの遅延（ミリ秒単位）が最も大きい上位サイトが表示されます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャート内のサイトにカーソルを合わせると、ロケーションの詳細、および該当する AAA サーバーの最大遅延が表示されます。
- チャート内のサイトをクリックすると、そのサイト内の AAA サーバーの最大遅延、およびそれらの遅延に関連する最も影響の大きいデータが表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位の AAA サーバーやサイトなど）をクリックすると、クライアントテーブルをフィルタ処理できます。

トランザクションエラーが発生した上位サイト

チャートには、AAA サーバーのトランザクションエラーが最も多い上位サイトが表示されます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャート内のサイトにカーソルを合わせると、ロケーションの詳細、および該当するトランザクション失敗数が表示されます。
- チャート内のサイトをクリックすると、サーバートランザクションのエラー、およびそのエラーに関連する最も影響の大きいデータが表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位 AAA サーバー、Cisco ISE 失敗数、SSIDなど）をクリックすると、クライアントテーブルをフィルタ処理できます。

AAA サーバーの遅延

このチャートには、各 AAA サーバーにおける AAA 平均遅延が表示されます。[All]、[MAB]、または [EAP] に基づいて遅延をフィルタ処理できます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャートの上にカーソルを合わせると、サーバーの IP アドレス、および該当する平均遅延が表示されます。
- チャートのエリアをクリックすると、AAA サーバーの遅延、およびそれらの遅延に関連する最も影響の大きいデータが表示されます。グラフに複数のサーバーが表示されている場合は、グラフの下の凡例でサーバーの IP アドレスをクリックすると、そのサーバーの詳細が表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位サイト、SSID など）をクリックすると、クライアントテーブルをフィルタ処理できます。

（注）
クライアントリストに表示される情報は、クライアントの最新のアクティビティおよびトランザクションに基づいています。

AAA サーバートランザクション

このグラフには、ワイヤレスコントローラおよびスイッチによって報告された各 AAA サーバーの平均 AAA サーバー トランザクション ステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャートの上にカーソルを合わせると、サーバーの IP アドレスとそれに該当するトランザクション数が表示されます。
- チャートのエリアをクリックすると、AAA サーバートランザクションと、それらのトランザクションに関連する最も影響の大きいデータが表示されます。

  チャートに複数のサーバーが表示されている場合は、チャートの下の凡例でサーバーの IP アドレスをクリックすると、そのサーバーの詳細が表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位の Cisco ISE 失敗数、サイトなど）をクリックすると、クライアントテーブルをフィルタ処理できます。

ステップ 10 次の機能には、ワイヤレスコントローラおよびスイッチ別AAAサーバーダッシュレットを使用します。

ワイヤレスコントローラ およびスイッチ別 AAA サーバーダッシュレット	
アイテム	説明
[デバイス別AAAサーバー（AAA Servers By Device）] テーブル	AAA サーバーの IP アドレス、デバイス名、デバイスのロケーション、デバイスファミリ（スイッチおよび ワイヤレスコントローラ）、トランザクション数、失敗数、平均遅延などが含まれているテーブル形式で AAA サーバー情報が表示されます。 AAA サーバーの IP アドレスをクリックすると、スライドインペイン が開いて、AAA サーバーの平均遅延およびトランザクションチャートが表示されます。 スライドインペイン では次のことができます。 • チャートにカーソルを合わせると、詳細情報が表示されます。 • チャートのエリアをクリックすると、サーバーの遅延とトランザクションの詳細、およびこれらのトランザクションに関連する最も影響の大きいデータが表示されます。 • 横棒で表示されているデータタイプカテゴリ（上位の Cisco ISE 失敗数、サイトなど）をクリックすると、クライアントテーブルをフィルタ処理できます。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします 3. [Apply] をクリックします。

DHCP ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラおよびスイッチから報告されたすべての DHCP サーバートランザクションを表示および監視します。

（注） **DHCP の制限事項**

- DHCP ネットワークサービスは、ワイヤレスクライアント、有線クライアント、およびローカルモードをサポートします。
- DHCP ネットワークサービスは、以下をサポートしていません。
  - SD-Access ファブリッククライアント
  - AireOS ワイヤレスコントローラ
  - フレックスモードまたはファブリックモード

始める前に

- バージョン 17.6.1 以降の Cisco Catalyst 9800 シリーズ ワイヤレスコントローラがインストールされていることを確認します。
- バージョン 26.01.02 以降の Cisco Catalyst 9000 IOS_XE シリーズ スイッチがインストールされていることを確認します。
- Assurance は、ユーザーのアクセス範囲を制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。サイトとデバイス、および関連する DHCP ネットワークサービスにアクセスできることを確認する必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

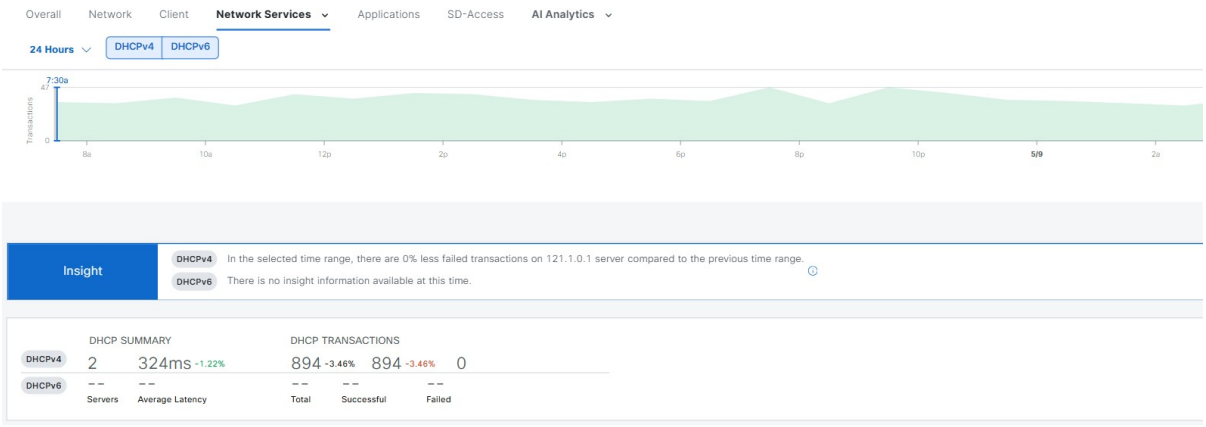
手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

ステップ 2 **[Network Services]** > **[DHCP]**を選択します。

[DHCP] ダッシュボードが表示されます。

図 *21 : [DHCP]* ダッシュボード



ステップ 3 左上隅にある時間範囲設定（）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 4 目的の [DHCP] プロトコル（[DHCPv4] および/または [DHCPv6]）を選択してダッシュボードをフィルタ処理します。この処理により、[インサイト（Insight）]、[DHCPの概要（DHCP Summary）]、および [DHCPトランザクション（DHCP Transactions）] セクションが自動的に更新され、選択項目に固有のメトリックが表示されます。

ステップ 5 右上隅にある自動更新設定（）をクリックして、サポートされている Assurance ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 6 タイムラインスライダを使用して、一定期間における DHCP サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の DHCP サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 7 タイムラインスライダの下にある **Actions** ドロップダウンリストをクリックして、次の機能を実行できます。

- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （434 ページ） およびカスタムダッシュボードの作成 （431 ページ） を参照してください。

ステップ 8 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した DHCP サーバートランザクションの割合を表示します。

ステップ 9 [DHCP Summary] ダッシュレットを使用して、次の情報を確認できます。

DHCP Summary	
アイテム	説明
DHCP 4 および DHCP 6 の概要（DHCP 4 and DHCP 6 Summary）	ネットワークの DHCP サーバーの数と平均遅延（ミリ秒単位）が表示されます。
DHCP 4 および DHCP 6 トランザクション（DHCP 4 and DHCP 6 Transactions）	ネットワーク内の DHCP トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合が表示されます。

ステップ 10 次の機能には、DHCP サーバーダッシュレットを使用します：

最も大きい遅延が発生した上位サイト
チャートには、DHCP サーバーの遅延（ミリ秒単位）が最も大きい上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントにカーソルを合わせると、DHCP サーバーの遅延が最も大きいサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

トランザクションエラーが発生した上位サイト
チャートには、DHCP サーバーのトランザクションエラーが最も多い上位サイトが表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントまたはそれに対応する凡例にカーソルを合わせると、DHCP サーバーのトランザクションエラーが最も多いサイトを表示できます。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

DHCP サーバーの遅延

このチャートには、各 DHCP サーバーにおける DHCP 平均遅延が表示されます。[All]、[Discover-offer]、または [Request-Ack] に基づいて遅延をフィルタ処理できます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャートの上にカーソルを合わせると、サーバーの IP アドレス、および該当する平均遅延が表示されます。
- グラフのエリアをクリックすると、DHCP サーバーの遅延、およびそれらの遅延に関連する最も影響の大きいデータが表示されます。グラフに複数のサーバーが表示されている場合は、グラフの下の凡例でサーバーの IP アドレスをクリックすると、そのサーバーの詳細が表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位サイト、SSID など）をクリックすると、クライアントテーブルをフィルタ処理できます。

DHCP サーバートランザクション

このチャートには、ワイヤレスコントローラによって報告された各 DHCP サーバーの平均 DHCP サーバー トランザクション ステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペイン では次のことができます。

- チャートの上にカーソルを合わせると、サーバーの IP アドレスとそれに該当するトランザクション数が表示されます。
- グラフのエリアをクリックすると、DHCP サーバートランザクションと、それらのトランザクションに関連する最も影響の大きいデータが表示されます。

  チャートに複数のサーバーが表示されている場合は、チャートの下の凡例でサーバーの IP アドレスをクリックすると、そのサーバーの詳細が表示されます。
- 横棒で表示されているデータタイプカテゴリ（上位サイト、SSID など）をクリックすると、クライアントテーブルをフィルタ処理できます。

ステップ 11 次の機能には、ワイヤレスコントローラおよびスイッチ別DHCP サーバーダッシュレットを使用します。

ワイヤレスコントローラおよびスイッチ別 DHCP サーバーダッシュレット	
アイテム	説明
DHCP サーバーテーブル	DHCP サーバー IP、デバイス名、デバイスの場所、トランザクション、障害、平均遅延などを含むテーブル形式で DHCP サーバー情報を表示します。[DHCP Server IP] をクリックしてスライドインペインを開き、サーバーの平均遅延およびトランザクションチャートを表示します。 水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします。 3. [Apply] をクリックします。

DNS ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラ、スイッチ、ルーターから報告された DNS サーバートランザクションを監視します。

（注） **DNS の制限事項**

- DNS ネットワークサービスは、ローカルモードまたはセントラルモードの AP でのみサポートされています。Flex モードの AP またはファブリックモードの AP ではサポートされていません。DHCP ネットワークサービスは、ワイヤレスクライアント、有線クライアント、およびローカルモードをサポートします。
- UI にクライアントごとの DNS データが表示されません。

始める前に

- 監視する予定のネットワークデバイスで NetFlow が有効になっていることを確認します。

- Catalyst Centerのアプリケーションテレメトリを有効にします。詳細については、テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 （93 ページ）を参照してください。
- DNS テレメトリのサポートでサポートされる最小バージョン：
  - Cisco IOS XE ルータ - 17.9
  - トラフィック テレメトリ アプライアンス - 17.9
  - Cisco Catalyst 9200/9300/9400 シリーズ スイッチ - 17.9.2
  - Cisco Catalyst 9800 シリーズワイヤレスコントローラ - 17.10.1

Assurance は、ユーザーのアクセス範囲を制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。サイトとデバイス、および関連する DNS ネットワークサービスへのアクセスを確認する必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

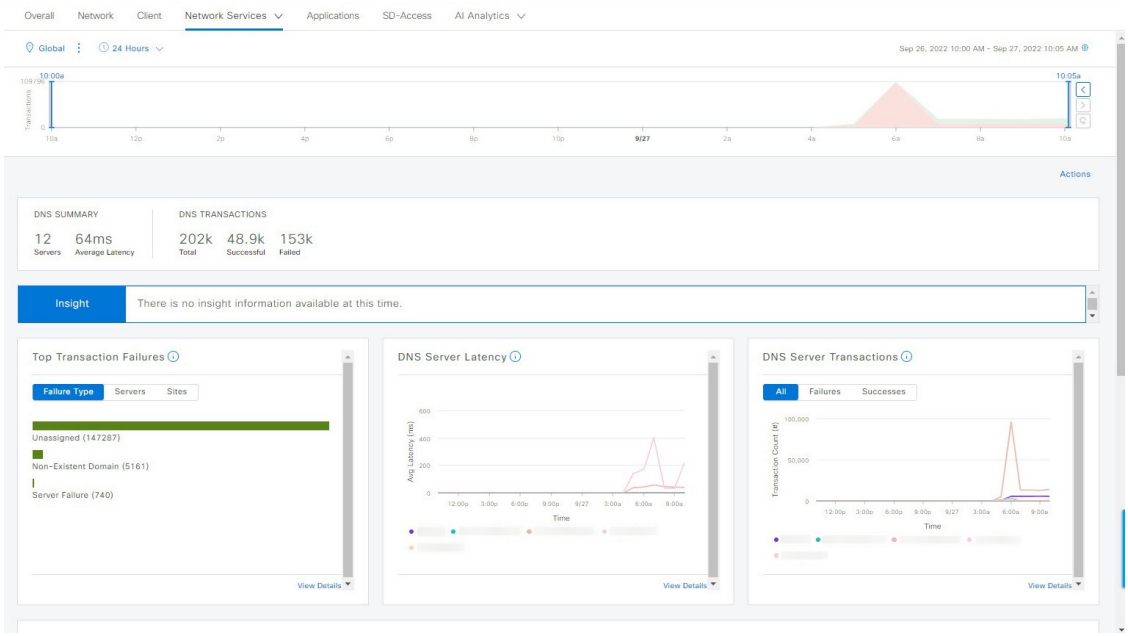
手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

ステップ 2 **Network Services** > **DNS**を選択します。

[DNS] ダッシュボードが表示されます。

図 *22 : DNS* ダッシュボード



ステップ 3 左上隅にある時間範囲設定（）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

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

ステップ 4 右上隅にある自動更新設定（）をクリックして、サポートされている Assurance ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 5 タイムラインスライダを使用して、一定期間における NDS サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の DNS サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 6 ダッシュボードの表示をカスタマイズするには、タイムラインスライダーの下にある [Actions] ドロップダウンリストをクリックし、[Edit Dashboard] を選択します。ダッシュレットの位置の変更 （434 ページ）およびカスタムダッシュボードの作成 （431 ページ）を参照してください。

ステップ 7 DNS の [Summary] ダッシュレットを使用して、次の情報を確認できます。

DNS Summary	
アイテム	**説明**
[DNS Summary]	ネットワークの DNS サーバーの数と平均遅延（ミリ秒単位）が表示されます。
DNS Transactions	ネットワーク内の DNS トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合が表示されます。

ステップ 8 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した DNS サーバートランザクションの割合を表示します。

ステップ 9 次の機能には、DNSサーバーダッシュレットを使用します。

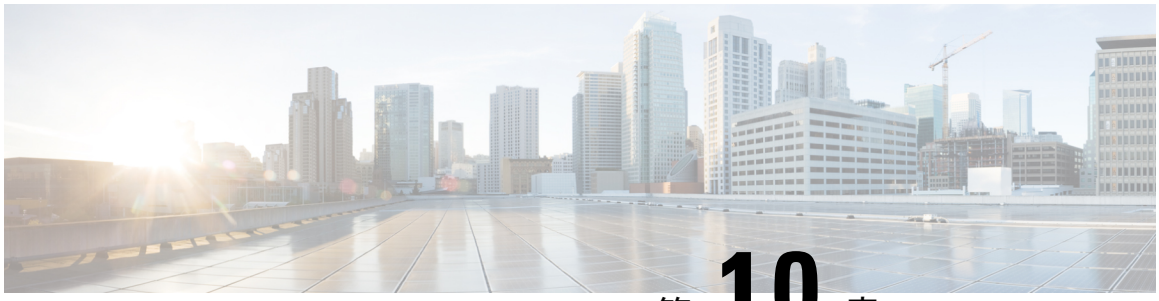
Top Transaction Failures
チャートには、DNS サーバーのトランザクションエラーが最も多いタイプ、サーバー、サイトがグラフに表示されます。チャートの色のセグメントにカーソルを合わせると、各項目におけるトランザクションエラーの回数が表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントにカーソルを合わせると、エラーの詳細が表示されます。

DNS Server Latency
このチャートには、各 DNS サーバーにおける DNS 平均遅延が表示されます。チャートにカーソルを合わせると、各サーバーの遅延時間（ミリ秒単位）が表示されます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、タイムラインをクリックして詳細を表示できます。

DNS Server Transactions
このチャートには、ワイヤレスコントローラから報告された各 DNS サーバーの平均 DNS サーバー トランザクション ステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、DNS サーバーのトランザクションを表示できます。 水平バーとして表示されるデータを選択して、上位の DNS サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

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

デバイス別のDNSサーバー	
アイテム	**説明**
[DNS Server table]	DNS サーバー名、IP アドレス、場所などを含む表形式で DNS サーバー情報を表示します。サーバー名をクリックして、[Device 360] の情報を表示するスライドインペインを開きます。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします。 3. [Apply] をクリックします。



第 10 章

SD-Accessの正常性のモニターとトラブルシューティング

- SD-Access ファブリック （257 ページ）
- SD-Access ファブリックの正常性のモニターとトラブルシューティング （265 ページ）
- ファブリックサイトの正常性の監視 （271 ページ）
- トランジットおよびピアネットワークの正常性の監視 （276 ページ）
- 仮想ネットワークの正常性の監視 （281 ページ）

SD-Access ファブリック

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

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

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、ファブリックサイトを作成できます。IPDT を有効にするには、**[設計（Design）]** > **[ネットワーク設定（Network Settings）]** > **[テレメトリ（Telemetry）]**に移動し、[有線エンドポイントデータコレクション（Wired Endpoint Data Collection）] エリアで、[このサイトでのCatalyst Center有線エンドポイントデータ収集の有効化（Enable Catalyst Center Wired Endpoint Data Collection At This Site）] オプションボタンをクリックします。

IPv6 アンダーレイのサポートについて、以下の要件が満たされていることを確認してください。

- サポートされているプラットフォーム：Cisco IOS XE 26.1.1 以降、Cisco ISE リリース 3.5 パッチ 3。
- サポートされている製品：Cisco Catalyst 9000 シリーズ スイッチ。

  Cisco Catalyst 9200、IE9300、およびIE3500 シリーズ スイッチは、ファブリック エッジ ロールではサポートされていませんが、拡張ノードおよびポリシー拡張ノードロールではサポートされています。Cisco Catalyst 9200 シリーズ スイッチは、サプリカントベースの拡張ロールでサポートされています。

  Cisco Catalyst C9350、C9610、9550、9600x、および 9500x シリーズ スイッチは、IPv6 アンダーレイファブリックのファブリックロールおよび IPv4 ファブリックサイトのデュアル スタック ボーダーロールではサポートされていません。
- ファブリックサイトは、IPv4 または IPv6 のいずれかのアンダーレイをサポートしますが、両方をサポートすることはできません。
- IPv6 アンダーレイは、LISP Pub/Sub SDA ファブリックでのみサポートされます。
- IPv6 オーバーレイマルチキャストは、IPv4 および IPv6 アンダーレイ ファブリック サイトの両方で HER/ユニキャストモードでサポートされています。

手順

ステップ 1 メインメニューから次を選択します。 **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

結果のウィンドウには、すでに作成されているすべてのファブリックサイトとその情報（正常性スコア、ファブリックゾーン、ファブリックデバイス、ファブリックロール、接続されたトランジットなど）が表形式で表示されます。

選択した列のみを表示するようにテーブルビューをカスタマイズできます。ウィンドウの右上隅にある歯車アイコンを使用して、[Table Settings] を編集し、[Apply] をクリックして変更を適用します。

ステップ 3 [Create Fabric Sites] をクリックします。

または、最初の 3 つの手順の代わりに、メニューアイコンをクリックして次を選択します。**[Workflow]** > **[Create Fabric Sites and Fabric Zones]** の順に選択します。

ステップ 4 [Create Fabric Sites] ウィンドウで、[Let’s Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Fabric Site Location] ウィンドウで、ファブリックサイトとして追加するエリア、建物、またはフロアを選択します。

ステップ 6 [Wired Endpoint Data Collection] ウィンドウで、[Wired Endpoint Data Collection] 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。

ステップ 7 ファブリックの [アンダーレイのIPアドレッシング（Underlay IP Addressing）] を選択します。

- デュアルスタックCatalyst Center展開の場合、アドレッシングタイプ（**IPv4** または **IPv6**）を選択できます。
- シングルスタックCatalyst Center展開の場合、アドレッシングタイプはデフォルトで **IPv4** または **IPv6** のいずれかが選択されます。

ステップ 8 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

テンプレートオプション	説明
クローズド認証	認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
オープン認証	ホストには、802.1X 認証を受ける必要なくネットワークアクセスが許可されます。
影響小	スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
なし（None）	なし。

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

設定	タスク
[First Authentication Method]	[802.1x] または [MAC Authentication Bypass (MAB)] を選択します。
[802.1x Timeout (in seconds)]	スライダを使用して、802.1x タイムアウトを秒単位で指定します。
Wake On LAN	[はい（Yes）] または [いいえ（No）] を選択します。
ホスト数	[Unlimited] または [Single] を選択します。
音声 VLAN	このチェックボックスを使用して、サイトのデフォルトの音声VLAN（VLAN 2046）を有効または無効にします。
BPDU ガード	このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。

設定	タスク
[Pre-Authentication Access Control List]	IPv4 および IPv6 用の事前認証アクセス制御リスト（ACL）を設定できます。 1. トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を設定します。 2. [Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択し、ルールの説明を入力します。 3. アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 9 （オプション）[Fabric Zones] 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	タスク
後でファブリックゾーンを指定する場合	[Setup Fabric Zones Later] をクリックします。
ファブリックゾーンを指定し、範囲指定されたサブネットを作成する場合	[Setup Fabric Zones Now] をクリックし、表示されているネットワーク階層からファブリックサイトを選択します。

ステップ 10 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（79 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 13 サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Fabric Site Creation Completed」というメッセージが表示されます。

次に、新しいファブリックサイトを作成するか [Tasks] ウィンドウでアクティビティを表示するかを選択できます。

デバイスをファブリックに追加

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

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。IPDTを有効にするには、**[設計（Design）]**> **[ネットワーク設定（Network Settings）]** > **[テレメトリ（Telemetry）]**に移動し、[有線エンドポイント データ収集（Wired Endpoint Data Collection）] エリアで、[このサイトでのCatalyst Center 有線エンドポイントデータ収集の有効化（Enable Catalyst Center Wired Endpoint Data Collection At This Site）] オプションボタンをクリックします。

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

Note

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

Before you begin

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

- **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウに、検出されたデバイスが表示されます。
- 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、トポロジビューにデバイスが灰色で表示されます。
- 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構成を更新する場合は、そのデバイスに対して**[Inventory]**> **[Resync]** を実行して、デバイス情報を再同期してください。

Note 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。

Procedure

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

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

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。スライドインペイン に、次の [Fabric] オプションが表示されます。

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

デバイスをファブリックインアボックスとして設定するには、[Control Plane Node]、[Border Node]、および [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 Node] と [Border Node] の両方を選択します。

ステップ 5 (Optional) デバイスのワイヤレス機能を有効にするには、[Capability] で [Embedded Wireless LAN Controller] トグルボタンをクリックして、次の手順を実行します。

トグルボタンがすでに有効になっている場合は、代わりに [Configure] をクリックしてワイヤレス設定を設定できます。

a) デバイスにワイヤレスパッケージをまだインストールしていない場合、機能を有効にするには組み込みの ワイヤレスコントローラ ソフトウェアイメージが必要であることを示す警告メッセージが Catalyst Center に表示されます。[Warning] ダイアログボックスで [OK] をクリックして、イメージを手動でインストールします。

b) [Download Image] で [Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP ソースを指定します。

c) [Import] をクリックします。

イメージのインポートの進捗状況が表示されます。ウィンドウを閉じてインポートの進行状況を表示し、後でインストールをスケジュールする場合は、[Close] をクリックします。

d) イメージのインポートが完了したら、[Download Image] ウィンドウの [Schedule Image Installation] で、次のいずれかのオプションを選択します。

- [Now]：イメージをすぐにインストールします。
- [Later]：将来の日付と時刻でイメージのインストールをスケジュールします。

e) [Task Name] フィールドで、必要に応じてタスク名を更新します。

f) [Later] を選択した場合は、次の手順を実行します。

- [Start Date/Time] で、イメージのインストールの開始日時を指定します。
- イメージのインストールにデフォルトのサイトのタイムゾーンを使用するには、[Site Settings] チェックボックスをオンにします。タイムゾーンを選択するには、[Site Settings] チェックボックスをオフにして、ドロップダウンリストからタイムゾーンを選択します。

g) [適用（Apply）] をクリックします。

イメージのインストールのステータスを表示するには、**[Activities]** > **[Tasks]**ウィンドウに移動し、関連する作業項目を開きます。ソフトウェアイメージが配信され、スイッチでアクティブ化されたら、**[Provision]** > **[Inventory]** > **[Resync]**オプションを使用してデバイスを再同期する必要があります。

h) [Manage Scope] で、組み込みワイヤレスコントローラの管理対象 AP の場所を割り当てます。

- [Primary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。
- [Secondary] タブで、必要なサイト名の横にあるチェックボックスをオンにします。

親サイトまたは個々のサイトを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

また、[Search Hierarchy] 検索フィールドまたはフィルタアイコンを使用してサイトを検索できます。

i) [Next] をクリックします。

j) [Advanced] ウィンドウで、必要な設定を行います。

- ローリング AP アップグレード機能を有効にするには、[Rolling AP Upgrade] チェックボックスをオンにします。

（オプション）このチェックボックスをオンにする場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot Percentage] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。

- 有効期限が切れる前に、関連する AP のローカルで有効な証明書（LSC）を更新するには、[AP LSC Certificate Renewal] チェックボックスをオンにします。

  このチェックボックスをオンにする場合は、次の設定を行います。

  - [Renewal Profile] ドロップダウンリストから、AP LSC 更新プロファイルを選択します。
  - （オプション）段階的な更新に AP LSC 更新プロファイルを選択する場合は、最小限のクライアント中断で再起動が可能となるように、[AP Reboot %] ドロップダウンリストから AP のパーセンテージを選択します。デフォルトは 25% です。



Note 設定すると、同じ AP 再起動パーセンテージ値が、ローリング AP アップグレードプロセスと段階的 AP LSC 更新プロセスの両方に適用されます。たとえば、AP の再起動パーセンテージを 25% に設定すると、ローリング AP アップグレードおよび段階的 AP LSC 更新の両方で、一度に 25% の AP のみが再起動されます。

k) [Next] をクリックします。
l) [Summary] で設定を確認します。
m) [Save] をクリックします。

デバイスのワイヤレス機能が有効になっており、ワイヤレスネットワーク設定に変更がある場合、変更をデバイスにプッシュするには、[Configure] をクリックして設定を保存する必要があります。

ステップ 6 [Add] をクリックして設定を保存します。

ステップ 7 [Fabric Infrastructure] タブで [Deploy] をクリックして、デバイスを設定します。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する, on page 78を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開, on page 79を参照してください。



Note デバイスは、Catalyst Center リリースと互換性のあるソフトウェアリリースを実行している場合にのみ、ファブリックに追加されます。ファブリックデバイスの互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

特定のファブリックロールについて、デバイスのソフトウェアイメージが Catalyst Center リリースと互換性がない場合、デバイスはファブリックに追加されず、エラーメッセージが表示されます。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

What to do next

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

SD-Access ファブリックの正常性のモニターとトラブルシューティング

この手順を使用して SD-Access ファブリックの概要を把握して、対処する必要がある潜在的な問題があるかどうかを判断します。

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。Catalyst Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

始める前に

ファブリックサイトを監視およびトラブルシューティングするには、最初にファブリックサイトを構成する必要があります。ファブリックサイトの追加（257ページ）およびデバイスをファブリックに追加 （261 ページ）を参照してください。

Assurance は、ユーザーのアクセス範囲を特定のクライアント 360 に制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。Assurance SD-Access ファブリックの機能は、アクセスグループで指定されたユーザーロールとサイトによって異なります。ユーザーロールと権限の詳細については、『*Cisco Catalyst Center Administrator Guide*』を参照してください。

マルチサイト ファブリック サイトの詳細情報については、*Cisco Catalyst Center User Guide*の「Provision Your Network」の章を参照してください。

（注） サブテンドノードと拡張ノードは、ファブリックの正常性の対象にはなりません。ファブリックのプロビジョニング時に、これらのノードには、エッジ、ボーダー、コントロールプレーンなどのファブリックロールが割り当てられないためです。

手順

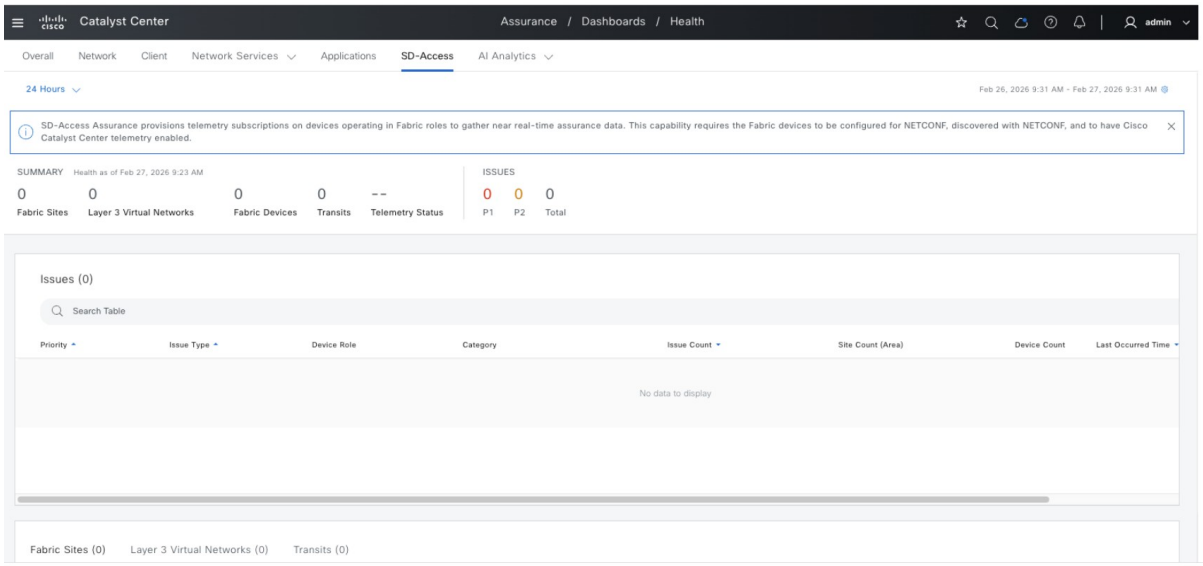
ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

図 *23 : SD-Access* 正常性ダッシュボード



ステップ 3 上部のメニューバーにある時間範囲設定（24 Hours）をクリックして、ダッシュボードに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューで、[3 hours]、[24 hours]、[7 days] のいずれかの時間範囲を選択します。
b) [Start Date] と時刻、[End Date] と時刻を指定します。
c) [Apply] をクリックします。

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

アイテム	説明
Summary	• [Fabric Sites]：ファブリックサイトの数。 • **[Layer 3 Virtual Networks]**：レイヤ 3 仮想ネットワークの数。 • **[Fabric Devices]**：ファブリックデバイスの数。 • [Transits and Peer Networks]：トランジットネットワークとピアネットワークの数。 • **[Telemetry Status]**：ファブリックサイトのテレメトリステータスを表示します。

アイテム	説明
Issues	• [P1]：優先度 1 の問題の数。 • [P2]：優先度 2 の問題の数。 • [Total]：P1、P2、および P3 の問題の合計数。

ステップ 5 次の機能には SD-Access の [Top 10 Issue Types] ダッシュレットを使用します。

[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、問題インスタンスをクリックし、必要に応じて次の操作を実行できます。 • 問題インスタンスを解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題のインスタンスを無視するには、次の手順を実行します。 1. [Status] ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 [View All Issues] をクリックすると、[Open Issues] ウィンドウが開きます。

ステップ 6 [Fabric Sites] ダッシュレットを使用して、ネットワーク内のファブリックサイトに関する詳細情報を表示します。このダッシュレットが提供する機能を次の表に示します。

[Fabric Sites] ダッシュレット	
アイテム	説明
[Health]	次のオプションを使用して、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** • [Poor]：正常性スコアが 1 ～ 3 のファブリックサイト。 • [Fair]：正常性スコアが 4 ～ 7 のファブリックサイト。 • [Good]：正常性スコアが 8 ～ 10 のファブリックサイト。 • [No Data]：データのないファブリックサイト。

[Fabric Sites] ダッシュレット	
アイテム	説明
[Fabric Site] テーブル	ファブリックサイトの詳細情報を表形式で表示します。デフォルトでは、[Fabric Site] テーブルには次の情報が表示されます。 • [Fabric Site]：ファブリックサイトの名前。 ファブリックサイト名をクリックして、ファブリックサイトの 360 度ビューを表示することもできます。ファブリックサイトの正常性の監視 （271 ページ）を参照してください。 • [# of Fabric Devices]：ファブリックサイト内のファブリックデバイスの数。 • [Fabric Site Health]： • [Overall]：ファブリックサイトの全体的な正常性。 • [Fabric Connectivity]：ファブリックサイトとの接続の状態。 • [Fabric Control Plane]：ファブリックサイトのコントロールプレーンの正常性。 • [Fabric Infrastructure]：ファブリックサイトを構成するデバイスの正常性。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。
	テーブルの表示をカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 3. [Apply] をクリックします。

ステップ 7 [Virtual Networks] ダッシュレットを使用して、ファブリックサイト内の仮想ネットワークに関する詳細情報を表示します。このダッシュレットは次の機能を提供します。

[Virtual Networks] ダッシュレット	
アイテム	説明
[Health]	仮想ネットワークの正常性に基づいて、次のオプションを使用してテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 の仮想ネットワーク。 • [Fair]：正常性スコアが 4 ～ 7 の仮想ネットワーク。 • [Good]：正常性スコアが 8 ～ 10 の仮想ネットワーク。 • [No Data]：データのない仮想ネットワーク。
[Virtual Networks] テーブル	仮想ネットワークの詳細情報を表形式で表示します。デフォルトでは、[Virtual Networks] テーブルには次の情報が表示されます。 • [VN Name]：仮想ネットワークの名前。 仮想ネットワーク名をクリックして、仮想ネットワークの 360 度ビューを表示することもできます。仮想ネットワークの正常性の監視 （281 ページ）を参照してください。 • [# of Active Sites]：仮想ネットワーク内のアクティブなサイトの数。 • [# of Clients]：仮想ネットワーク内のエンドポイントの数。 • [Virtual Network Health]： • [Overall]：仮想ネットワークの全体的な正常性。 • [Fabric Control Plane]：仮想ネットワークのコントロールプレーンの正常性。 • [VN Services]：仮想ネットワークサービスの正常性。
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。
⚙	テーブルの表示をカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 3. [Apply] をクリックします。

ステップ 8 [Transits and Peer Networks] ダッシュレットを使用して、ファブリックサイト内のトランジットネットワークおよびピアネットワークに関する詳細情報を表示します。このダッシュレットは次の機能を提供します。

アイテム	説明
[Health]	トランジットネットワークおよびピアネットワークの正常性に基づいて、次のオプションを使用してテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のトランジットネットワークおよびピアネットワーク。 • [Fair]：正常性スコアが 4 ～ 7 のトランジットネットワークおよびピアネットワーク。 • [Good]：正常性スコアが 8 ～ 10 のトランジットネットワークおよびピアネットワーク。 • [No Data]：データのないトランジットネットワークおよびピアネットワーク。
[Transits and Peer Networks] テーブル	トランジットネットワークおよびピアネットワークの詳細情報を表形式で表示します。デフォルトでは、トランジットネットワークおよびピアネットワークのテーブルには次の情報が表示されます。 • [トランジット/ピアネットワーク名（Transit/ Peer Network Name）]：トランジットネットワークの名前。 名前をクリックして、トランジットネットワークの 360 度ビューを表示することもできます。トランジットおよびピアネットワークの正常性の監視（276 ページ）を参照してください。 • [タイプ（Type）]：トランジットネットワーク内のアクティブなサイトの数。 • [クライアント数（# of Clients）]：トランジットネットワーク内のエンドポイントの数。 • [Associated Fabric Sites] • [Transit and Peer Networks Health]： • [Overall]：トランジットネットワークおよびピアネットワークの全体的な正常性。 • [Transit Control Plane]：トランジット コントロール プレーンの正常性。

アイテム	説明
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。 （注） テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。
	テーブルの表示をカスタマイズします。 **1.** [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 **2.** [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 **3.** [Apply] をクリックします。

ファブリックサイトの正常性の監視

この手順を使用して、特定のファブリックサイトの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

ステップ 3 [Fabric Site] テーブルで、ファブリックサイトの名前をクリックします。

ファブリックサイトの 360° ビューを提供する [Fabric Site] ウィンドウが表示されます。

図 *24 : Fabric Site 360*



ステップ 4 左上隅にある時間範囲設定（ 24 Hours ）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

a) ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 5 正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。水平バーにカーソルを合わせると、ファブリックサイトのテレメトリステータス（[Good]、[Fair]、[Poor] など）が表示されます。ツールチップの [Telemetry Status] をクリックするとスライドインペインが開き、ファブリックサイトのテレメトリステータスの概要が表示されます。

[Fabric Site Health]：正常性は、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスの正常性は含まれません。[Fabric Sub Category Health] は、基礎となる KPI スコアの最小値です。

（注） KPI は正常性スコアに含まれません。

[Fabric Site Connectivity]：コントロールプレーンの到達可能性、拡張ノードの接続性など、サイトの到達可能性ステータスに寄与する KPI サブカテゴリが一覧表示されます。

ファブリック コントロール プレーン

ファブリック インフラストラクチャ

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。この境界により、[Fabric Site 360] ウィンドウに表示されるファブリックサイトデータのコンテキストが設定されます。

[Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。

- [Latest]：ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。
- [Trend]：過去 24 時間のデータが表示されます。

ステップ 6 タイムラインの下にある [Fabric Site Health] エリアで、次の情報を確認します。

Fabric Site Health	
アイテム	**説明**
Latest	デフォルトで表示されます。2つのペインがあります。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Health Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] 状態のデバイスの数。 • [Charts]：この色分けされたスナップショットビューチャートには、過去 5 分間のファブリックサイトの接続とインフラストラクチャが表示されます。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。 チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。たとえば、ファブリック CP の到達可能性、マルチキャスト RP、AAA サーバーのステータスなどが示されます。 この KPI は、有線およびワイヤレスデバイスの Dot1 x および MAB 認証を行う、各 AAA サーバーのセッションマネージャデーモン（SMD）およびワイヤレス ネットワーク コントロール デーモン（WNCD）インスタンスのステータスをモニターします。 Telnet および SSH 認証を行う iOS インスタンスはモニターされません。この KPI は、エッジおよび拡張ノードのロールにのみ適用されます。 チャート内のハイパーリンクされたファブリックカテゴリをクリックしてサイドペインを開き、それぞれの KPI サブカテゴリを表示できます。 • [Fabric Site Connectivity]：コントロールプレーンの到達可能性、拡張ノードの接続性、ボーダーからコントロールプレーンへの BGP セッション、ボーダーからピアノードへの BGP セッション。 • [Fabric Control Plane]：LISP セッションステータス。 • [Fabric Infrastructure]：インフラ VN の AAA サーバーステータスと Pub/Sub セッションステータス、CTS 環境データのダウンロード。

Fabric Site Health	
アイテム	説明
Trend	[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ●：中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 です。 ●：正常性データなし。ヘルス スコアは 0 です。

ステップ 7 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

ISSUES
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、次のタスクを実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （299 ページ）を参照してください。

ステップ 8 次の表に示す機能には、[Fabric Nodes] ダッシュレットを使用します。

[Networks Devices] ダッシュレット	
アイテム	説明
Type	オプション（[All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric WLC]、[Fabric AP]、[Extended Node]）を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
ファブリックサイトの正常性	次のオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。
[Fabric Node] テーブル	選択したサイトのすべてのファブリックノードのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、ファブリックサイト接続とファブリックインフラストラクチャの KPI メトリック正常性スコアの最小サブスコアです。 [Name]、[Issue Type Count]、および [Fabric Role] 列には、ファブリック名、問題数、およびファブリックロール（エッジ、ボーダー、マップサーバーなど）が表示されます。 [Device Fabric Site Health] の [Overall] 列で、正常性スコアの上にマウスカーソルを合わせます。全体の [Device Fabric Site Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。 カーソルを [Fabric Site Connectivity]、[Fabric Control Plane]、および [Fabric Infrastructure] アイコンに合わせると、正常性スコアが表示されます。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。

[Networks Devices] ダッシュレット	
アイテム	説明
⚙	テーブルに表示するデータをカスタマイズします。 1. ⚙ をクリックします。 オプションのリストが表示されます。 2. テーブルに表示するデータのチェックボックスをオンにします。 3. [Apply] をクリックします。

トランジットおよびピアネットワークの正常性の監視

この手順を使用して、特定のトランジットネットワークの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

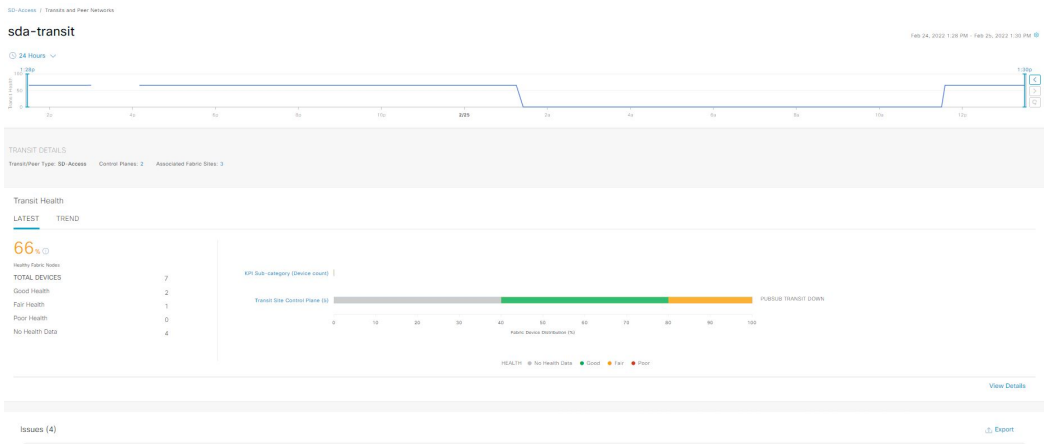
ステップ 2 [Overall Health] ダッシュボードで、[SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

ステップ 3 [Transit and Peer Network] テーブルで、トランジットの名前をクリックします。

ファブリックサイトの 360° ビューを提供する [Transit Site 360] ウィンドウが表示されます。

図 *25 :* トランジット *360°* ビュー



ステップ 4 左上隅にある時間範囲設定（24 Hours）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

a) ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 5 正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Transit Network Health]：正常性スコアは、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスの正常性は含まれません。[Fabric Category Health] は、基礎となる KPI スコアの最小値です。

[Transit Site Control Plane]：トランジットの LISP セッションや Pub/Sub セッションなどの KPI サブカテゴリが一覧表示されます。トランジット正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。テレメトリのステータスを表示するには、次の手順を実行します。

- 水平バーにカーソルを合わせると、トランジットネットワークの正常性の割合、テレメトリステータス（[Good]、[Fair]、[Poor] など）、トランジット サイト コントロール プレーン、トランジットサービスなどの情報がツールチップに表示されます。
- ツールチップの [Telemetry Status] をクリックするとスライドインペインが開き、テレメトリステータスの概要が表示されます。

カテゴリに表示されるデータの範囲を変更するには、次のいずれかのタブをクリックします。

- [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。

ステップ 6 タイムラインの下にある [Transit Health] エリアで、次の情報を確認します。

アイテム	説明
LATEST	デフォルトで表示されます。2つのペインがあります。左側のペインには、ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Health Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] 状態のデバイスの数。 • [Charts]：この色分けされたスナップショット ビュー チャートは、過去 5 分間のトランジット コントロール プレーンを示します。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。 チャート内のハイパーリンクされた [Transit Control Plane] をクリックしてサイドペインを開き、トランジットコントロールプレーンの次の KPI サブカテゴリを表示します。 • [BGP Session from Border to Transit Control Plane] • [LISP session from Border to Transit Control Plane] • [PubSub session from Border to Transit Control Plane] チャートの色のセグメントにカーソルを合わせると、ファブリックノードの名前、問題数、ファブリックロール、ファブリックサイト、デバイスのトランジットの正常性などのファブリックノードの詳細を表形式で表示できます。
[TREND]	[TREND] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ●：不良なネットワークデバイス。正常性スコアの範囲は 1 ～ 3 です。 ●: 中程度のネットワークデバイス。正常性スコアの範囲は 4 ～ 7 です。 ●：良好なネットワークデバイス。正常性スコアの範囲は 8 ～ 10 です。 ●：正常性データなし。正常性スコアは 0 です。

ステップ 7 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

ISSUES
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、次のタスクを実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （299 ページ）を参照してください。

ステップ 8 次の機能には、[Associated Fabric Sites] ダッシュレットを使用します。

アイテム	説明
[Health]	次のオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。
[Associated Fabric Sites] テーブル	ファブリックテーブルに次の詳細を表示します。[Fabric Site]、[Health]、使用可能な [Connected Transit/ Peer Networks] の数、[Layer 3 Virtual Network]、および [Fabric Devices]。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] ウィンドウには、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。

アイテム	説明
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. 設定アイコン（）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. [Table Settings] スライドインペインで、テーブルに表示するデータのトグルボタンを有効にします。 3. [Apply] をクリックします。

ステップ 9 次の機能には、[Fabric Nodes] ダッシュレットを使用します。

アイテム	説明
Type	オプション（[All]、[Transit Control Plane]、[Border]）を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
[Transit and Peer Network Health] テーブル	次のオプションを使用して、トランジットの全体的な正常性スコアに基づいてテーブルをフィルタ処理します： • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。

アイテム	説明
[Fabric Node] テーブル	選択したトランジットのすべてのファブリックノードのデバイス情報を表形式で表示します。 （注） 全体的な正常性スコアは、トランジット サイト コントロール プレーンの KPI メトリック正常性スコアの最小サブスコアです。 [Name]、[Issue Type Count]、[Fabric Role]、および [Fabric Site] 列には、ファブリック名、問題数、ファブリックロール、およびファブリックサイトが表示されます。 [Device Transit Health] の [Overall] 列で、正常性スコアの上にカーソルを合わせます。全体の [Device Transit Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。 [Transit Site Control Plane] アイコンにカーソルを合わせると、正常性スコアが表示されます。
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] ウィンドウには、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. 設定アイコン（）をクリックします。 2. [Table Settings] スライドインペインで、テーブルに表示するデータのトグルボタンを有効にします。 3. [Apply] をクリックします。

仮想ネットワークの正常性の監視

この手順を使用して、特定の仮想ネットワークの詳細を表示します。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

ステップ 3 下にスクロールし、[Virtual Network] をクリックします。

ステップ 4 [Virtual Network] テーブルで、仮想ネットワークの名前をクリックします。

仮想ネットワークの 360 度ビューを提供する [Virtual Network 360] ウィンドウが表示されます。

図 *26 : Virtual Network 360*



ステップ 5 左上隅にある時間範囲設定（24 Hours）をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。

b) [Start Date] と時刻、[End Date] と時刻を指定します。

c) [Apply] をクリックします。

ステップ 6 仮想ネットワークの正常性タイムラインスライダを使用して、より詳細な時間範囲の仮想ネットワークの正常性スコアや仮想ネットワークの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Virtual Network Health]：正常性スコアは、VN における正常なデバイスの割合です。[VN Category Health] は、対応するサブカテゴリの KPI スコアの最小値です。[VN Services] には、[BGP Session from Border to Peer Node]、[Multicast (external RP)]、[Default Route Registration]、および [VN Control Plane] が含まれます。

VN 正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

タイムラインの下にある [Telemetry Status] チェックボックスをオンにして、タイムラインに水平バーを表示させます。テレメトリのステータスを表示するには、次の手順を実行します。

- 水平バーにカーソルを合わせると、仮想ネットワークの正常性の割合、テレメトリステータス（[Good]、[Fair]、[Poor] など）、ファブリック コントロールプレーン、VN サービス、VN 終了などの情報がツールチップに表示されます。

- ツールチップの [Telemetry Status] をクリックするとスライドインペインが開き、仮想ネットワークのテレメトリステータスの概要が表示されます。

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、360 ウィンドウに表示されるデータのコンテキストが設定されます。

[Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。

- [Latest]：ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。
- [Trend]：過去 24 時間のデータが表示されます。

ステップ 7 タイムラインの下にある [Virtual Network Health] エリアで、次の情報を確認します。

Virtual network health	
アイテム	**説明**
Latest	デフォルトで表示されます。左側のペインには、仮想ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。 • [Healthy Fabric Nodes]：選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices]：ファブリックデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] 状態のデバイスの数。 • [Charts]：この色分けされたスナップショットビュー チャートには、[VN Control Plane]（[Pub-Sub Sessions Status]）や [VN Services]（[BGP Session from Border to Peer Node]、[Multicast-external RP] および [Default Route Registration]）などのサブカテゴリを持つ KPI が表示されます。 いずれかの色の上にカーソルを重ねると、その色に関連付けられたデバイスの正常性スコアと数が表示されます。 チャートに低い正常性スコア（赤またはオレンジ）が示されている場合、その低い正常性スコアに寄与した KPI がバーの隣に示されます。 ハイパーリンクされたカテゴリをクリックして、詳細を含むサイドペインを開きます。

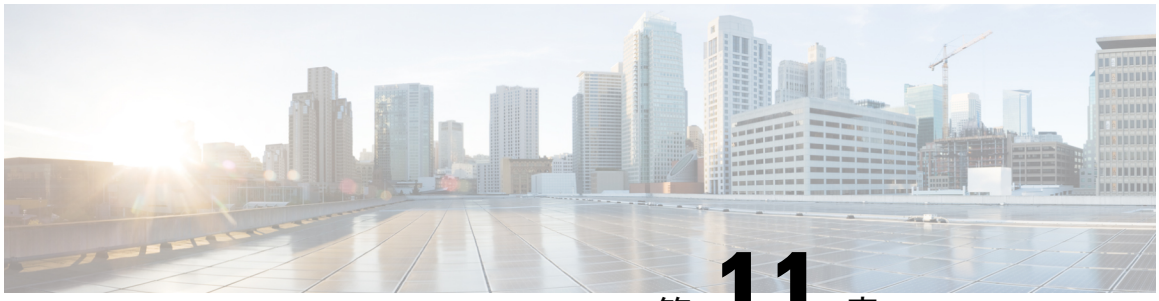
Virtual network health	
アイテム	説明
Trend	[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、ある時間範囲におけるデバイスのパフォーマンスを示しています。チャートにカーソルを重ねると、デバイスの合計数とその健全性が時系列で表示されます。 チャートの色は、ネットワークデバイスの正常性を表します。 ● : 不良なネットワークデバイス。ヘルス スコアの範囲は 1 ～ 3 です。 ● : 中程度のネットワークデバイス。ヘルス スコアの範囲は 4 ～ 7 です。 ● : 良好なネットワークデバイス。ヘルス スコアの範囲は 8 ～ 10 です。 ● : 正常性データなし。ヘルス スコアは 0 です。

ステップ 8 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

ISSUES
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、次のタスクを実行できます。 • この問題を解決するには、次の手順を実行します。 1. ドロップダウンリストから [Resolve] を選択します。 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。 • 問題を無視するには、次の手順を実行します。 1. ドロップダウンリストから [Ignore] を選択します。 2. スライダで問題を無視する時間数を設定します。 3. [Confirm] をクリックします。 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。 問題のタイプの詳細については、問題の表示と管理 （299 ページ）を参照してください。

ステップ 9 [Virtual Network Devices] ダッシュレットを使用して、この機能を利用します：

[Virtual Network Devices] ダッシュレット	
アイテム	説明
Type	タイプに基づいてテーブルをフィルタ処理します。
[Virtual Network Health]	次のオプションを使用して、仮想ネットワークの全体的な正常性スコアに基づいてテーブルをフィルタ処理します： • [All] • [Poor]：正常性スコアが 1 ～ 3 のデバイス。 • [Fair]：正常性スコアが 4 ～ 7 のデバイス。 • [Good]：正常性スコアが 8 ～ 10 のデバイス。 • [No Health]：正常性データのないデバイス。
[Virtual Network Devices] テーブル	選択した項目のデバイス情報が表形式で表示されます。 （注） 全体的な正常性スコアは、仮想ネットワーク接続とインフラストラクチャの KPI メトリック正常性スコアの最小サブスコアです。 各種の正常性スコアとアイコンにカーソルを合わせると、追加情報が表示されます。\
[Device 360]	[Name] 列でデバイス名をクリックすると、デバイスの 360 度ビューが表示されます。 [Device 360] には、デバイスの問題のトラブルシューティングに関する詳細情報が記載されています。
Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 **1.** をクリックします。 オプションのリストが表示されます。 **2.** テーブルに表示するデータのチェックボックスをオンにします。 **3.** [Apply] をクリックします。



第 11 章

サイト分析を使用したネットワークのモニターとトラブルシューティング

- サイト分析について （287 ページ）
- [Site Analytics] ダッシュボードのインサイト （289 ページ）
- サイト分析の表示, on page 292
- サイト分析設定の構成 （297 ページ）

サイト分析について

サイト分析は、ネットワークトラブルシューティングを可視化し、最も問題のあるサイト、建物、フロアまたは AP にドリルダウンすることを可能にします。KPI のしきい値を設定し、問題が発生する前の KPI ごとの傾向をモニターできます。

ネットワーク全体の問題について警告するために使用できる KPI しきい値を定義できます。KPI 値に基づいて、最もパフォーマンスの低いサイトを特定し、特定の建物とフロアにドリルダウンして問題を見つけることができます。オンボーディングの試行、オンボーディングの期間、ローミングの試行、ローミングの期間、カバレッジ、および接続速度に関する問題を分析できます。

[Site Analytics] ウィンドウは、パフォーマンスの問題を調査するときに、次の情報を得るのに役立ちます。

- **問題の内容**：KPI を使用して、問題の詳細を調べます。KPI カードには、KPI の名前、KPI の成功率、および最もパフォーマンスの低い参加者の名前とスコアが表示されます。KPI のしきい値に達している場合、KPI スコアは黒で表示されます。パーセンテージがしきい値未満の場合、スコアは赤で表示されます。

  次のカテゴリが利用可能です。

  - [Onboarding Attempts]：指定されたサイトの AP に正常にオンボーディングできるワイヤレスクライアントの割合を測定します。ワイヤレスクライアントがネットワークに正常に参加すると SLA が達成され、ワイヤレスクライアントがネットワークに正常に参加できないと SLA の達成に失敗します。たとえば、100 のクライアントがネットワークへのオンボーディングを試みたとします。50 のクライアントが正常にオンボー

ディングし、50がオンボーディングに失敗しました。この場合、[Onboarding Attempts] の KPI 値は 50% です。

- [オンボーディング期間（Onboarding Duration）]：設定されたしきい値時間内に AP にオンボーディングできる、正常にオンボーディングされたワイヤレスクライアントの割合を測定します（しきい値の設定については「サイト分析設定の構成 （297 ページ）」を参照）。ワイヤレスクライアントがオンボーディングに失敗した場合、メトリックにはカウントされません。ワイヤレスクライアントが正常にオンボーディングされたものの、設定された SLA 期間よりも時間がかかった場合、失敗としてカウントされます。たとえば、オンボーディングに成功した 50 のクライアントのうち、30 のクライアントは 10 秒未満、20 のクライアントは 10 秒以上かかったとします。この場合、[Onboarding Duration] の KPI 値は 60% です。

- [Roaming Attempts]：特定のサイト内に存在する 1 つの AP から別の AP に正常にローミングできるワイヤレスクライアントの割合を測定します。あるワイヤレスクライアントが正常にローミングして別の AP 経由でネットワークに参加すると SLA が達成され、そのワイヤレスクライアントがネットワークに正常に参加できないと失敗と見なされます。たとえば、100 のクライアントが一定時間内にローミングを試みたとします。50 のクライアントが正常にローミングし、50 のクライアントがローミングに失敗しました。この場合、[Roaming Attempts] の KPI 値は 50% です。

- [Roaming Duration]：設定されたしきい値時間内に、ある AP から別の AP に正常にローミングできるワイヤレスクライアントの割合を測定します。ワイヤレスクライアントが正常なローミングに失敗した場合、このメトリックにはカウントされません。ワイヤレスクライアントが正常にローミングしたものの、ローミング期間に設定されたしきい値よりも時間がかかった場合、失敗としてカウントされます。たとえば、正常にローミングした 50 のクライアントのうち、30 のクライアントは 10 秒未満、20 のクライアントは 10 秒以上かかったとします。この場合、[Roaming Duration] の KPI 値は 60% です。

- [Connection Speed]：設定されたしきい値レートより高い無線データレートのデータトラフィックがワイヤレスクライアントにある時間のパーセンテージを測定します。たとえば、正常にオンボーディングされた 50 のクライアントのコントローラによってサンプリングされたデータレートのうち、200 のサンプルは 11 Mbps のしきい値より高く、50 のサンプルは低かったとします。この場合、[Connection Speed] の KPI 値は 80% です。

- [Coverage]：設定されたしきい値より高い RSSI 値のデータトラフィックがワイヤレスクライアントにある時間のパーセンテージを測定します。たとえば、コントローラによってサンプリングされた 50 の正常にオンボーディングされたクライアントの RSSI 値のうち、200 のサンプルはしきい値の -72 dBm を超えましたが、50 のサンプルはそれよりも低かったとします。この場合、[Coverage] の KPI 値は 80% です。

- **時間**：時間範囲設定（24 Hours）をクリックして、KPI、タイムラインスライダ、およびヒートマップで使用する期間を指定します。

- **場所**：サイトレベルから建物、フロア、デバイスレベルへとドリルダウンします。

- ヒートマップ内の赤または緑の色で、パフォーマンスの低いサイトや建物、およびそれらに対応するKPI値を簡単に識別できます。緑はKPIのしきい値が満たされていることを示し、赤はKPIが満たされていないことを示します。
- 建物レベルにドリルダウンすると、低いKPIスコアの原因となったいくつかの主要指標を確認できます。
- 正常性ステータスとデバイスの詳細を示すフロアヒートマップでアクセスポイントを表示します。
- 特定のフロアにあるアクセスポイントのリストを、各アクセスポイントの特定のKPIスコアおよびクライアント数とともに表示します。
- アクセスポイントをクリックして、その [Device 360] ウィンドウを表示します。

サイト分析ダッシュボードは、アシュアランス ヘルス ダッシュボードの [AI Analytics] メニューオプションから利用できます。

[AI Analytics] メニューオプションでは、AI ネットワーク分析ツールにもアクセスできます。これらのツールについては、ネットワークのトレンドの観察およびインサイトの取得（437ページ） を参照してください。

[Site Analytics] ダッシュボードのインサイト

サイト分析は、ワイヤレスネットワークのKPIをモニターするのに役立ちます。KPIは、オンボーディングの試行、オンボーディングの期間、ローミングの試行、ローミングの期間、接続速度、およびカバレッジです。これらのKPIごとにパフォーマンスのしきい値を設定できます。その後、**[Assurance]** > **[Health]** > **[Overall]**正常性ダッシュボードまたは**[Assurance]** > **[Health]** > **[AI Analytics]** > **[Site Analytics]**ダッシュボードでKPIをモニターできます。

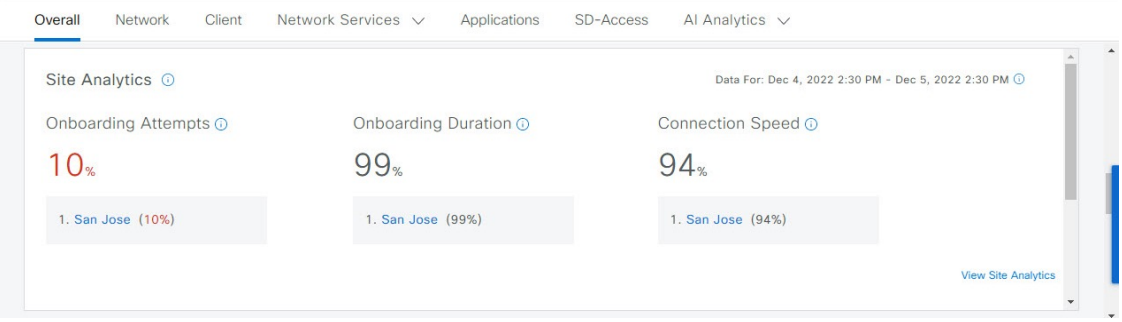
[Overall] 正常性ダッシュボードには、KPIのスコアを表示する [Site Analytics] ダッシュレットがあります。これらのKPIのいずれかのパフォーマンスが設定したしきい値を下回った場合、パフォーマンスが最も低いサイトが表示されます。[Site Analytics] ダッシュボードから、フロアおよびデバイスレベルにドリルダウンして、問題の発生場所、発生時期、根本原因を正確に特定できます。

次の例を検討して、問題の内容、発生時期、発生場所を判定しましょう。

オンボーディング試行KPIを85%に設定します。このKPIは、100回のオンボーディング試行のうち少なくとも85回が成功した場合、少なくともこのKPIカテゴリでサイトがパフォーマンス基準を満たしていることを意味します。

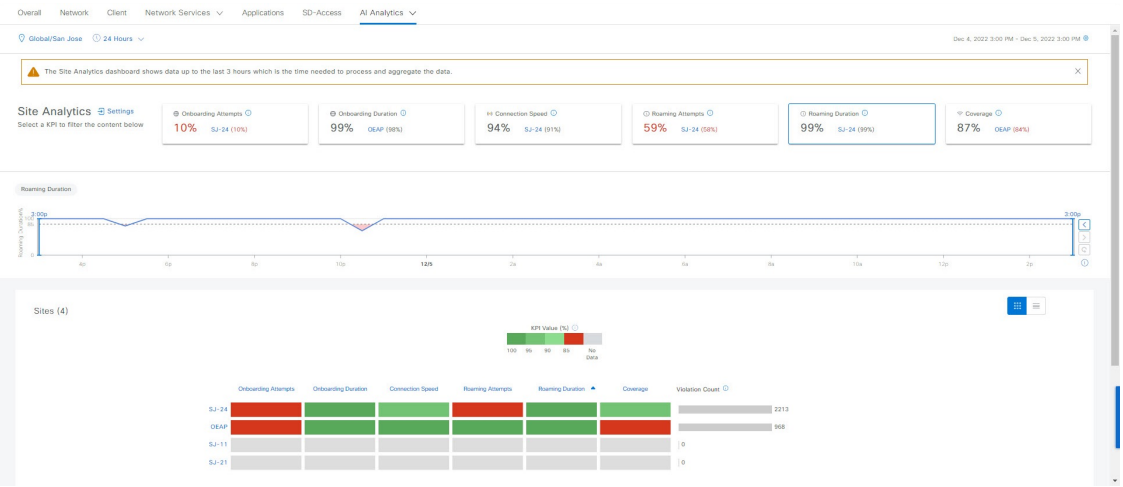
[Global] ドロップダウンリスト（Global）が [Global] に設定されている [Overall] 正常性ダッシュボードの [Site Analytics] ダッシュレットは、サンノゼのサイトが最もパフォーマンスの低いサイトであり、オンボーディングの試行が成功したのは10%のみであることを示しています。このパーセンテージは、100回のオンボーディング試行のうち10回が成功したことを意味します。KPIの計算方法の詳細を確認するには、KPI名の横にある [i] アイコンにカーソルを合わせます。

図 *27 : [Site Analytics]* ダッシュレットが表示されている *[Overall Health]* ダッシュボード



何が影響を受けており、何が失敗の原因であるかを調べるには、サイトの名前である [San Jose] をクリックします。[Site Analytics] ダッシュボードが表示されます。[Global] ドロップダウンリスト（Global）に、範囲として [Global/San Jose] が表示されていることに注目してください。サンノゼのサイトにある建物の分析結果が表示されます。表示には 各 KPI のパフォーマンスが最も低い建物が含まれます。

図 *28 :* タイムラインスライダとヒートマップグラフィックが表示されている、サイトのサイト分析

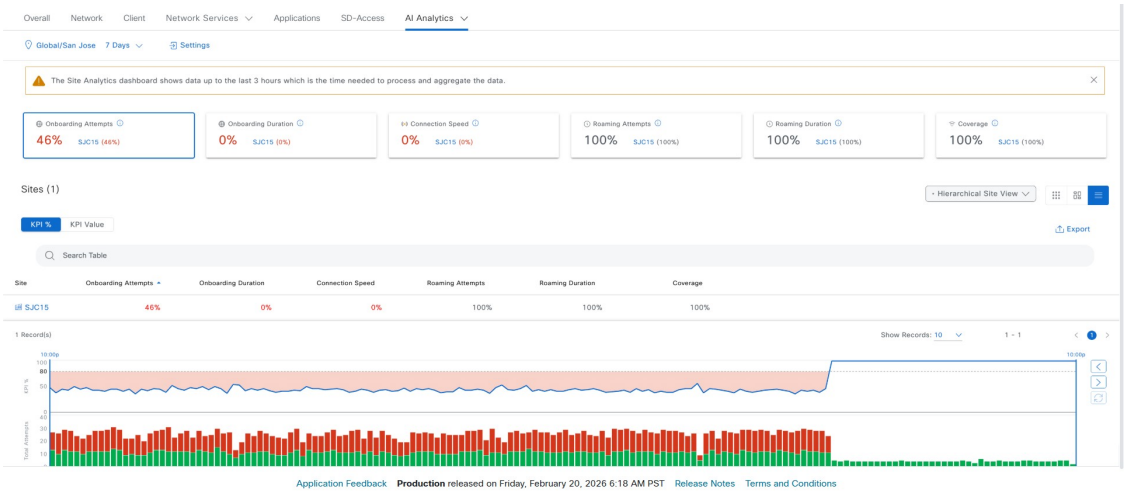


タイムラインスライダの基準値は 85% で、トレンドラインには 24 時間（時間範囲設定（24 Hours）で設定）の間に成功したオンボーディング試行のパーセンテージが表示されています。

表示からすると、サンノゼのサイトにオンボーディングの問題があります。では、具体的にどこで問題が発生しているのでしょうか。タイムラインスライダの下には、色分けされたデータを表示するヒートマップがあります。緑色のバーは、KPI 値のパーセンテージに基づく成功の度合いを示します。濃い緑色は成功率が高いことを示しており、薄い緑色は成功率が低いことを示しています。赤色のバーは達成できていない KPI を示しており、灰色のバーはデータがないことを示しています。[Violation Count] は、建物に関する KPI エラー数の未処理データを示します。

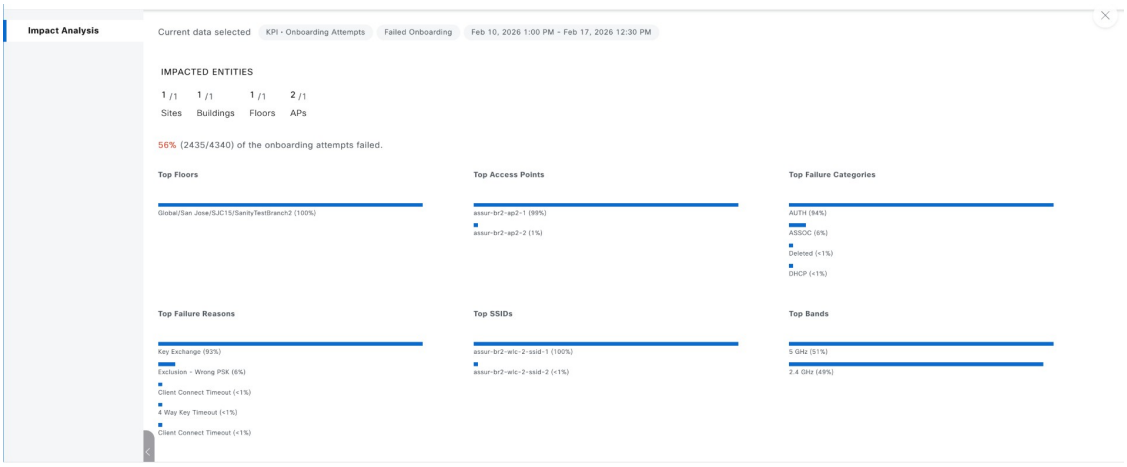
赤色のバーの上にカーソルを重ねると、サイトと特定のKPIに関する情報が表示されます。または、[List View] トグルボタン（ ）をクリックすると、すべての建物と KPI の詳細が表示されます。

図 *29* : タイムラインスライダとヒートマップテーブルが表示されている、サイトのサイト分析



表示されたデータによると、SJ-24 の建物でオンボーディング試行の失敗が最も多く発生しています。影響分析を表示するには、建物の名前（この場合は [SJ-24]）をクリックします。

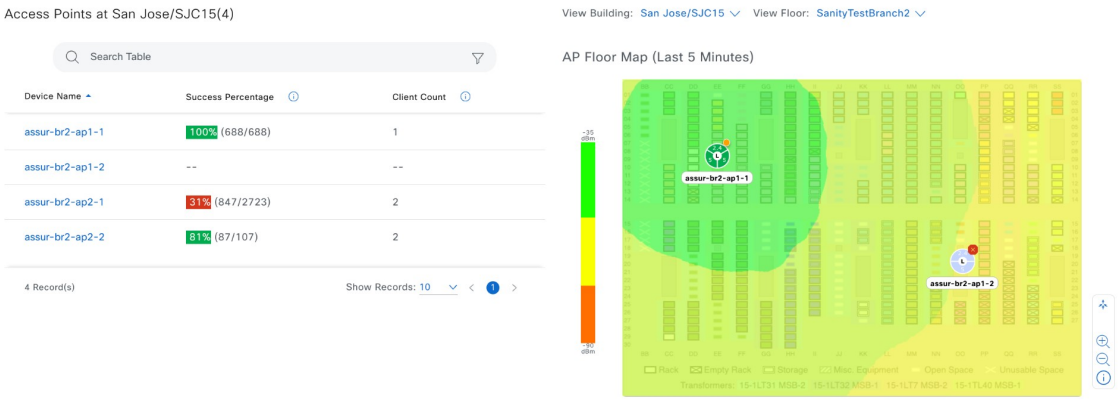
図 *30* : 影響分析が表示されている、建物のサイト分析



フロアの [Site Analytics] ダッシュボードが表示されます。このダッシュボードの [Impact Analysis] ダッシュレットには、上位のフロア、上位のアクセスポイント、上位の障害カテゴリ、上位の障害理由といったさまざまな情報が表示されます。

下にスクロールして AP フロアマップを表示します。

図 *31* : アクセスポイントテーブルとフロアヒートマップが表示されている、フロアのサイト分析



[View Floor] ドロップダウンリストには、選択されているフロアが表示されます。

このテーブルには、選択されているフロアのデバイス、オンボーディング試行の成功率、およびオンボーディングに成功したクライアントの数が表示されます。

フロアヒートマップで、APにカーソルを合わせると、そのAPに関する詳細が表示されます。ヒートマップの右側にツールバーがあります。ヒートマップのアイコンに慣れていない場合は、[i] アイコンをクリックしてマップの凡例を表示します。

テーブル内のデバイスをクリックすると、そのデバイスの [Device 360] ウィンドウが表示されます。たとえば、オンボーディングの成功率が 45% の [SJC24-11A-AP10] デバイスをクリックします。[Device 360] に、問題のトラブルシューティングに役立つ非常に詳細な情報が表示されます。詳細については、デバイスの正常性のモニターとトラブルシューティング （117ページ）を参照してください。

サイト分析の表示

サイト、建物、フロアのオンボーディング、ローミング、接続速度、ワイヤレスカバレッジに関する問題をモニターおよびトラブルシュートします。

Before you begin

- サイト分析データを収集するには、AI Network Analytics を有効にする必要があります。[Enable AI Network Analytics] リンクをクリックして、このシステム設定を構成できる [Cisco AI Analytics] ウィンドウに直接移動します。詳細については、Cisco AI Network Analytics の設定, on page 95を参照してください。

  AI Network Analytics が有効になっていない場合、Assurance ではサンプルデータを含むダッシュレットの例が表示されます。

- サイト分析設定の構成。詳細については、サイト分析設定の構成, on page 297を参照してください。

Procedure

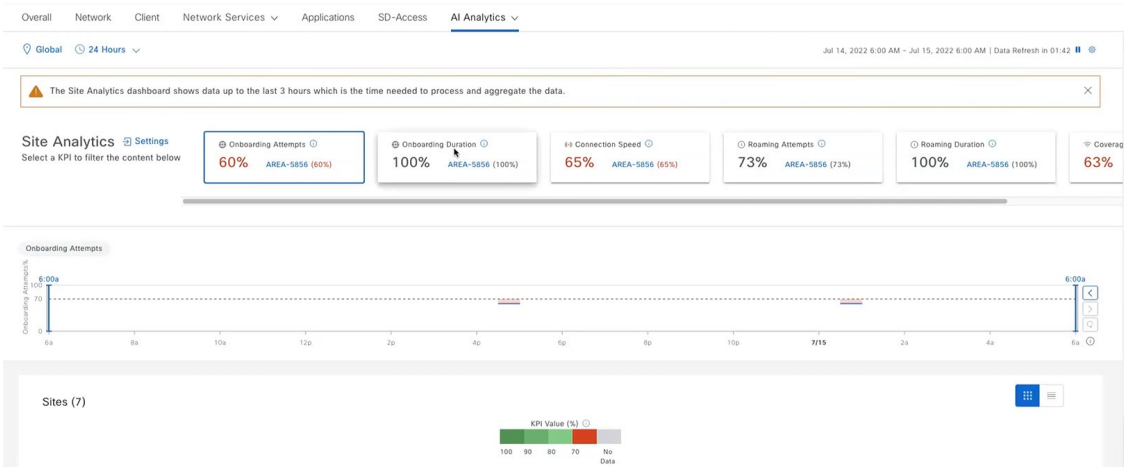
ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 **[AI Analytics]** > **[Site Analytics]** を選択します。

[Site Analytics health] ダッシュボードが表示されます。表示される情報は、[Global] ドロップダウンリスト（ Global ）で選択した場所によって異なります。[Global] を選択すると、ネットワーク内のすべてのサイトが表示されます。特定のサイトを選択すると、そのサイト内の建物すべてが表示されます。特定の建物を選択すると、その建物内のフロアすべてが表示されます。このガイドでは、サイト分析の説明を [Global] ロケーションから始めます。

***Figure 32: [Site Analytics Health]* ダッシュボード**



ステップ 3 次の機能には、トップのメニューバーを使用します。

アイテム	説明
Global [Location] ペイン	• Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。
時間範囲	過去 3 時間、24 時間、または 7 日間のデータを表示できます。

ステップ 4 （[Global] またはサイトレベルの）[Site Analytics] 領域で、次のタスクのいずれかを実行します。

- KPI カテゴリをクリックします。タイムラインスライダが更新され、選択した KPI が反映されます。

  各 KPI カテゴリの表示には、集計された KPI 値（パーセンテージ）と、各カテゴリで最もパフォーマンスが低いサイトまたは建物が含まれます。次のカテゴリが利用可能です。

- [Onboarding Attempts]：指定されたサイトの AP に正常にオンボーディングできるワイヤレスクライアントの割合を測定します。ワイヤレスクライアントがネットワークに正常に参加すると SLA が達成され、ワイヤレスクライアントがネットワークに正常に参加できないと SLA の達成に失敗します。たとえば、100 のクライアントがネットワークへのオンボーディングを試みたとします。50 のクライアントが正常にオンボーディングし、50 がオンボーディングに失敗しました。この場合、[Onboarding Attempts] の KPI 値は 50% です。
- [Onboarding Duration]：設定されたしきい値時間内に AP にオンボーディングできる、正常にオンボーディングされたワイヤレスクライアントの割合を測定します。ワイヤレスクライアントがオンボーディングに失敗した場合、メトリックにはカウントされません。ワイヤレスクライアントが正常にオンボーディングされたものの、設定された SLA 期間よりも時間がかかった場合、失敗としてカウントされます。たとえば、オンボーディングに成功した 50 のクライアントのうち、30 のクライアントは 10 秒未満、20 のクライアントは 10 秒以上かかったとします。この場合、[Onboarding Duration] の KPI 値は 60% です。
- [Roaming Attempts]：特定のサイト内に存在する 1 つの AP から別の AP に正常にローミングできるワイヤレスクライアントの割合を測定します。あるワイヤレスクライアントが正常にローミングして別の AP 経由でネットワークに参加すると SLA が達成され、そのワイヤレスクライアントがネットワークに正常に参加できないと失敗と見なされます。たとえば、100 のクライアントが一定時間内にローミングを試みたとします。50 のクライアントが正常にローミングし、50 のクライアントがローミングに失敗しました。この場合、[Roaming Attempts] の KPI 値は 50% です。
- [Roaming Duration]：設定されたしきい値時間内に、ある AP から別の AP に正常にローミングできるワイヤレスクライアントの割合を測定します。ワイヤレスクライアントが正常なローミングに失敗した場合、このメトリックにはカウントされません。ワイヤレスクライアントが正常にローミングしたものの、ローミング期間に設定されたしきい値よりも時間がかかった場合、失敗としてカウントされます。たとえば、正常にローミングした 50 のクライアントのうち、30 のクライアントは 10 秒未満、20 のクライアントは 10 秒以上かかったとします。この場合、[Roaming Duration] の KPI 値は 60% です。
- [Connection Speed]：設定されたしきい値レートより高い無線データレートのデータトラフィックがワイヤレスクライアントにある時間のパーセンテージを測定します。たとえば、正常にオンボーディングされた 50 のクライアントのコントローラによってサンプリングされたデータレートのうち、200 のサンプルは 11 Mbps のしきい値より高く、50 のサンプルは低かったとします。この場合、[Connection Speed] の KPI 値は 80% です。
- [Coverage]：設定されたしきい値より高い RSSI 値のデータトラフィックがワイヤレスクライアントにある時間のパーセンテージを測定します。たとえば、コントローラによってサンプリングされた 50 の正常にオンボーディングされたクライアントの RSSI 値のうち、200 のサンプルはしきい値の -72 dBm を超えましたが、50 のサンプルはそれよりも低かったとします。この場合、[Coverage] の KPI 値は 80% です。

- サイトや建物とそのパフォーマンスに関する情報を表示するには、KPI カテゴリでサイト名または建物名をクリックします。
- タイムラインスライダで、ある KPI カテゴリについての情報を表示するには、その KPI カテゴリをクリックします。

ステップ 5 積み上げ棒グラフでタイムラインスライダを使用して、選択した時間範囲における選択した KPI に関する情報を表示します。

タイムラインスライダを使用すると、次の情報が表示されます。

- タイムラインと積み上げ棒グラフの横にある点線は、構成されたしきい値を表します。
- タイムライン内でマウスカーソルを合わせると、特定の時間範囲における KPI パーセンテージが表示されます。
- グラフにカーソルを合わせると、特定の時間範囲の KPI 情報が表示されます。たとえば、[Onboarding Attempts] は次の色コードを使用して表されます。
  - 🟢：正常な試行の合計数
  - 🔴：失敗した試行の合計数
  - 🔵：オンボーディング試行の割合
- 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、タイムラインの下に表示される KPI データのコンテキストが設定されます。
- タイムラインの右にある矢印ボタンを使用して、最大 30 日分のデータを表示します。

ステップ 6 この情報を表示するには、[Site] 領域で、次のヒートマップビューを使用します。

項目	説明
 ヒートマップビュー	このトグルボタンをクリックすると、対応する KPI 値のデータがヒートマップビューに表示されます。ドロップダウンリストから [Hierarchical Site] または [Building] ビューを選択して、対応する建物またはサイトレベルのヒートマップデータを表示します。 ヒートマップデータは色分けされています。緑色のバーは、KPI 値のパーセンテージに基づく成功の度合いを示します。赤色のバーは達成できていない KPI を示しており、灰色のバーはデータがないことを示しています。 [Violation Count] は、特定のサイトや建物に関する KPI エラー数の未処理データを示します。 KPI（カラム）の横にある下矢印をクリックして、KPI を昇順または降順に並べ替えます。順序は違反数に基づいきます。

項目	説明
[Summary] ダッシュレット	サイト、建物、フロア、AP などの影響を受けるエンティティの数を表示できます。色分けされたチャートには、KPI に基づいてエンティティの分布とインサイトが表示されます。[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。

ステップ 7 この情報を表示するには、[Site] 領域で、次のバブルビューを使用します。

項目	説明
 バブルビュー	このトグルボタンをクリックすると、対応する KPI 値のデータがバブルビューに表示されます。ドロップダウンリストから [Hierarchical Site] または [Building] ビューを選択して、対応する建物レベルまたはサイトレベルのヒートマップデータを表示します。 [Count] ドロップダウンリストを使用して、[AP Count] または [Client Count] に基づいてバブルチャートに表示される KPI データをフィルタ処理します。 バブルチャートのデータは色分けされています。緑色の円は、KPI 値のパーセンテージに基づく成功の度合いを示します。赤色の円は、失敗した KPI を示します。灰色の円は、データがないことを示します。 円のサイズは、接続されているクライアントと AP 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。 バブルチャートにカーソルを合わせると、詳細が表示されます。 [Summary] ダッシュレットに、サイト、建物、フロア、AP などの影響を受けるエンティティの数を表示できます。色分けされたチャートには、KPI に基づいてエンティティの分布とインサイトが表示されます。[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。

ステップ 8 この情報を表示するには、[Site] 領域で、次のテーブルビューを使用します。

項目	説明
 テーブル ビュー	このトグルボタンをクリックすると、KPI カテゴリの特定のサイトまたは建物に関するデータが表形式で表示されます。ドロップダウンリストから [Hierarchical Site] または [Building] ビューを選択して、各 KPI に対応する建物レベルまたはサイトレベルのデータを表示します。 CSV ファイルにテーブルをエクスポートするには、[Export] をクリックします。
[Summary] ダッシュレット	サイト、建物、フロア、AP などの影響を受けるエンティティの数を表示できます。色分けされたチャートには、KPI に基づいてエンティティの分布とインサイトが表示されます。[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。

ステップ 9 [Site Analytics] 領域またはヒートマップで建物名をクリックすると、建物レベルのビューにドリルダウンします。

建物レベルのビューには、次の付加的な領域が含まれます。

- [Impact Analysis]：表示される情報は、選択した KPI カテゴリによって異なります。たとえば、[Onboarding Attempts] を選択した場合、[Impact Analysis] 領域の情報はオンボーディング試行の失敗に関連したものになります。この情報には、上位のアクセスポイント、上位の障害カテゴリ、上位の SSID、上位の帯域などが含まれます。
- [Access Points] テーブル：[View Floor] ドロップダウンリストのフロアに対応する AP、オンボーディング試行、およびクライアント数が表示されます。各 AP のクライアント数は、選択した時間範囲の間にネットワークに接続した個別のクライアントの数です。

  特定のデバイスの [Device 360] ビューを表示するには、デバイス名をクリックします。
- [AP Floor Map (Last 5 Minutes)]：[View Floor] ドロップダウンリストで選択したフロアに関して、ヒートマップには、既存の AP とそのステータスを示すフロアマップビューが表示されます。

  ヒートマップで、AP にカーソルを合わせると、その AP に関する詳細情報が表示されます。ヒートマップの右側には、ワイヤレスコントローラのステータスを表示したり、ズームインおよびズームアウトしたりできるツールバーがあります。ヒートマップのアイコンに慣れていない場合は、[i] アイコンをクリックしてマップの凡例を表示します。

サイト分析設定の構成

この手順では、主要なクライアント評価指標のしきい値を構成する方法を示します。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **サイト分析の設定**

[Site Analytics Settings] ウィンドウが表示されます。

ステップ 2 しきい値の [KPI Value %] を変更するには、次の手順を実行します。

a) [Edit] をクリックします。

b) スライドインペインで、サイト評価指標の目標のパーセンテージを入力します。このしきい値は、任意のサイトのKPIデータポイントの正常な割合を定義します。緑（GOOD）の目標は100%で、変更することはできません。赤（POOR）の目標は 0 から 95 までの数値でなければなりません。これらの目標値は、すべてのクライアント評価指標に影響します。

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

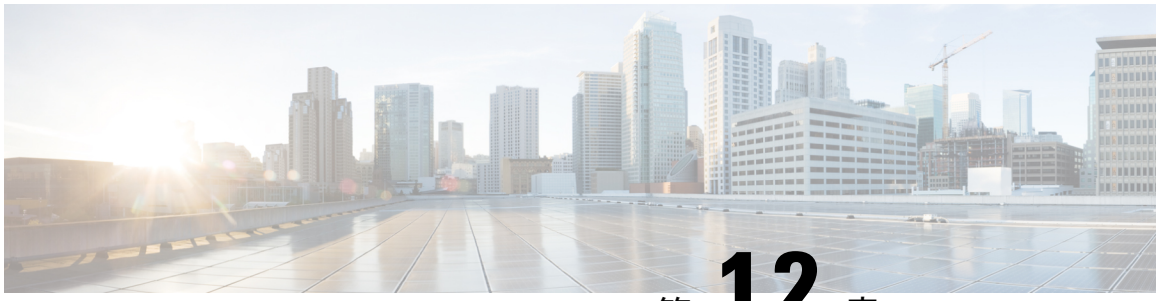
KPI のスライドインペインが表示されます。

ステップ 4 KPI のしきい値を設定します。

- 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。
- デフォルト設定に戻すには、[View Default Setting] をクリックします。

ステップ 5 [Apply] をクリックします。

確認用のダイアログボックスが表示されます。



第 12 章

問題の表示と管理

- 問題について （299 ページ）
- 機械推論エンジンについて （300 ページ）
- VLAN に関連するレイヤ 2 ループの問題について （300 ページ）
- 未解決の問題の表示, on page 301
- MRE を使用した有線クライアントの問題のトラブルシューティング （319 ページ）
- 解決済みの問題の表示 （322 ページ）
- 無視された問題の表示 （324 ページ）
- 問題の解決または無視 （326 ページ）
- 無線にアクティビティなしの問題のトリガー （328 ページ）
- 自動問題解決, on page 328
- グローバルな問題の設定の管理 （332 ページ）
- ユーザー定義問題の設定の管理 （334 ページ）
- カスタム問題の設定の管理 （336 ページ）
- 問題の通知の有効化 （338 ページ）
- Assurance、Cisco AI Network Analytics、および MRE の問題 （341 ページ）

問題について

Assurance 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。Assurance では、多数の問題についてシステムガイド付きのアプローチが提供されます。複数の重要業績評価指標（KPI）が関連付けられており、テストやセンサーからの結果に基づいて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。Assurance 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行われます。

Catalyst 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 では次のタイプのクラウドベースの AI 駆動型の問題を検出できます。

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

（注） 標準のアシュアランスの問題とは異なり、AI で生成された問題は GUI にすぐに表示されません。AI で生成された問題は、Catalyst Center アプライアンスによってポーリングされ、取り込まれる前に、クラウド側でバッチ処理されます。この複数ステップによるプロセスのため、AI で生成された問題が GUI に表示されるまでに最大 5 時間の遅延が予想されます。

機械推論エンジンについて

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

MRE を使用して、有線クライアントの問題、レイヤー 2 ループの問題、および PoE の問題をトラブルシュートできます。問題のリストについては、MRE の問題 （362 ページ）を参照してください。

手順については、MRE を使用した有線クライアントの問題のトラブルシューティング （319 ページ）、レイヤ 2 ループ問題の問題インスタンスの詳細 （310 ページ）、PoE の問題に関する問題インスタンスの詳細 （314 ページ）を参照してください。

VLAN に関連するレイヤ 2 ループの問題について

レイヤ 2 のループ問題は、1 つ以上の VLAN パスで転送ループが形成されたときに発生します。この場合、リンクとデバイスが最大キャパシティに達するまで、パケットは転送され、影響を受けるパスで無限に増幅されます。ブロードキャストストームが発生すると、レイヤ 2 ネットワーク全体は即時にシャットダウンします。MRE の次の機能を使用することで、レイヤ 2 のループ問題をトラブルシューティングできます。

- ループに関係すると考えられる VLAN とポートが表示されます。

- ループに関係しているデバイスが表示されます。

（注） レイヤ 2 ループのスケールには以下の制約事項があります。

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

重要 現在、MRE では、アンマネージドネットワークデバイス、仮想マシン、または Catalyst Center で認識されるトポロジには含まれないエンティティが原因で発生するレイヤ 2 のループについては、根本原因分析が実行されません。

未解決の問題の表示

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**：Assurance 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。

  Catalyst Center で Cisco AI Network Analytics アプリケーションをインストールおよび設定している場合は、次のタイプのクラウドベース AI 駆動型の問題を表示できます。

  - **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。

Note 接続の問題が表示されるようにするには、AP がサイトに適切に割り当てられていることを確認してください。

- **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーションアプリケーションのスループット、およびソーシャルアプリケーションのスループット。

Note アプリケーション エクスペリエンスに関する問題を表示するには、ワイヤレスコントローラで Application Visibility and Control（AVC）が有効になっていることを確認してください。スループットの問題では、AVC データに基づいて基準化と異常検出を行います。

- **レイヤ 2 ループの問題**と **PoE の問題**：Assurance によって検出された、MRE ワークフローを使用してトラブルシューティングできる問題。機械推論エンジンについて, on page 300を参照してください。

Before you begin

- 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 の設定, on page 95を参照してください。
- syslog メッセージを表示するため、syslog が設定されていることを確認します。テレメトリを使用した syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定, on page 93を参照してください。

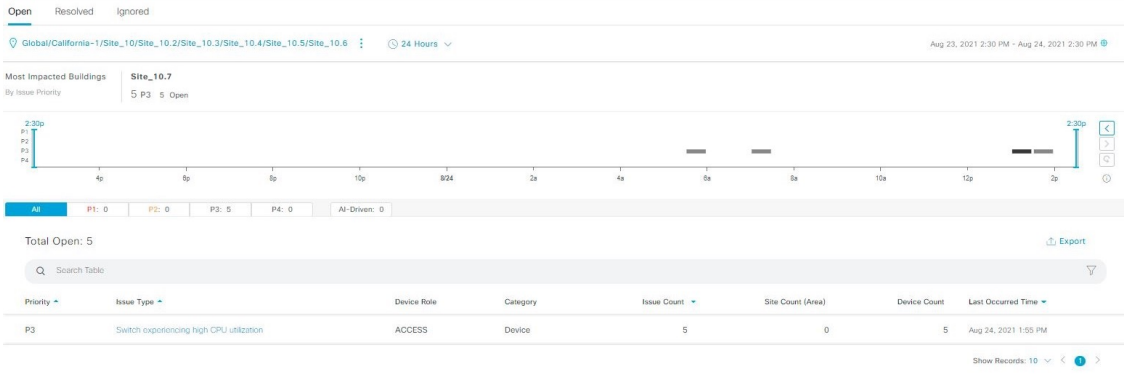
Procedure

ステップ 1 次のいずれか 1 つのタスクを実行します。

- Catalyst Center ホームページの **Assurance [Summary]** > **[Critical Issues]**エリアで、[View Details] を選択します。
- メインメニューから次を選択します。**[Assurance]** > **[Issues and Events]**の順に選択します。

[Open Issues] ダッシュボードが表示され、次の情報が示されます。

***Figure 33: [Open Issues]* ダッシュボード**



[Open Issues] ダッシュボード	
アイテム	**説明**
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[サイトテーブル（Site Table）] を選択してサイトテーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Open Issues] ダッシュボードに表示されます。
24 Hours [Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **a.** [24 Hours] ドロップダウン リストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **b.** [Start Date] と時刻、[End Date] と時刻を指定します。 **c.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。

[Open Issues] ダッシュボード	
アイテム	説明
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 **Note** 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。
問題の優先順位別の最も影響を受けるロケーション（Most Impacted Locations by Issue Priority）	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階層をクリックして、問題が発生した、影響を受けるエリア、建物、フロア、および屋外エリアを特定します。

ステップ 2 [すべて（All）]、[P1]、[P2]、[P3]、[P4]、または [AI主導（AI-Driven）] トグルをクリックすると、[問題のタイプ（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。

[AI主導（AI-Driven）] トグルは、クラウドエージェントがアクティブな場合にのみ機能します。クラウドエージェントが実行されていない場合、このトグルは無効になります。

[Open Issues] ウィンドウの [Issue Type] テーブル	
アイテム	説明
Total Open	アクションを必要とする未解決の問題の合計数が表示されます。 [Total Open] の値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。
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。 **Note** AI 駆動型の問題の場合、 問題のタイプの前に AI アイコンが表示されます。
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。

[Open Issues] ウィンドウの [Issue Type] テーブル	
アイテム	説明
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、[問題のインスタンス（Issue Instances）] に、その問題タイプに関するすべての問題が次の情報とともに一覧表示されます。

[Issue Instances]（最初のスライドインペイン）	
アイテム	説明
Open Issues	その問題タイプで未解決の問題の数。
Area	問題の影響を受けるビルディングとフロアの数。
[Device]	問題の影響を受けるデバイスの数。
[Actions] ドロップダウン リスト	個別に問題を解決または無視することも、一度に大量の問題を解決または無視することもできます。問題の解決または無視, on page 326を参照してください。
Issue	問題の説明。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。
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、[問題インスタンスの詳細（Issue Instance Details）] に、問題に関する具体的な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。これらの問題の詳細については、以下のセクションを参照してください。

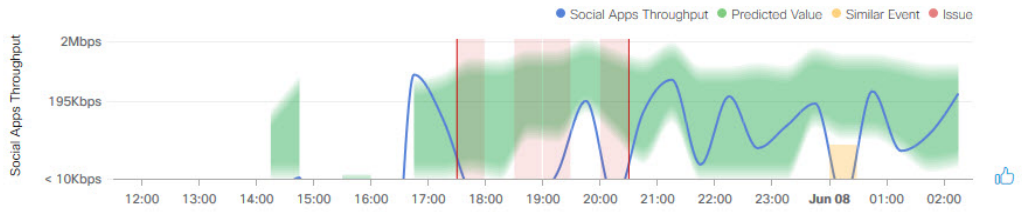
• AI 駆動型の問題の問題インスタンスの詳細, on page 306
• AP 切断の問題についての [Issue Instance Details], on page 309
• レイヤ 2 ループ問題の問題インスタンスの詳細, on page 310
• PoE の問題に関する問題インスタンスの詳細, on page 314

AI 駆動型の問題の問題インスタンスの詳細

（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題の表示 （301 ページ） 」のステップ 4 を参照してください。

AI 駆動型の問題が発生すると、[Issue Instance Details]（2 番目のスライドインペイン）に次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	**説明**
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。次のタスクを実行します。 • 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、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。
注アイコン（）	管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。
[Summary] エリア	問題の簡単な要約。ここには、影響を受ける無線、無線の場所、問題が発生した日時、問題の場所などの情報が表示されます。
[Impacted Summary for this Network]	問題によって影響を受けた場所と、影響を受けたクライアント数に関する情報が表示されます。
[Feedback] アイコン	アイコンをクリックして、このページの情報が役に立ったかどうかについてコメントを入力し、[Submit] をクリックしてください。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Problem	問題の簡単な説明と、実際の KPI 値が予測した正常な動作からどの程度乖離しているかを視覚的に示すグラフが表示されます。 デフォルトでは、次の図のように、チャートは問題発生の前後 6 時間にズームインされています。 **図 *34* : 問題のチャート**  AI 駆動型の問題のチャートでは、詳細がさまざまな色で表されます。 • **緑色の帯域**：機械学習に基づいて予測されたネットワークの正常な動作。 • **青色の実線**：実際の KPI 値。 • **垂直の赤色の線またはバー**：問題を示します。青色の線（実際の KPI 値）が緑色の帯域（予測される正常な動作）の外側になると、問題が発生します。 • **垂直の黄色のバー**：類似のイベントが発生したことを示します。 グラフの上にカーソルを移動すると、選択した時点での KPI 値、予測下限値、予測上限値などの同期情報が表示されます。
Impact	問題の影響を受ける接続済みクライアント、AP、デバイス、およびアプリケーションに関する情報が表示されます。 過剰なオンボーディング時間と失敗、過剰な DHCP、関連付け、または認証時間と失敗については、[Impacted Clients] と [Top 10 Impacted APs] のタブが表示されます。 総無線スループットおよびアプリケーションのスループット（クラウド、コラボレーション、メディア、ソーシャル）については、[Impacted Clients]、[Device Breakout]、[Applications by TX/RX] のタブが表示されます。 タブをクリックすると、チャートとチャートの下の表が更新されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	次の図のように、問題および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 *35 :* 根本原因の分析チャート  過剰なオンボーディング時間と失敗については、[Network Causes]、[Failed Distribution]、[Failed Percentage]、[Failed Count] のタブが表示されます。 過剰な DHCP、アソシエーション、または認証時間については、[Network Causes]、[Top Impacted APs]、[Top Impacted Times] のタブが表示されます。 過剰な DHCP、アソシエーション、または認証の失敗については、[Network Causes]、[Top Impacted APs、[Top Impacted Failures] のタブが表示されます。 総無線スループットおよびアプリケーションスループット（クラウド、コラボレーション、メディア、ソーシャル）については、[Network Causes] タブが表示されます。 タブをクリックすると、下のチャートが更新されます。 その他の KPI のチャートを表示するには、の [KPI] アイコンをクリックし、KPI を選択してから、[Apply] をクリックします。
Suggested Actions	この問題を解決するために実行できるアクションが表示されます。

AP 切断の問題についての [Issue Instance Details]

（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。「未解決の問題の表示 （301 ページ） 」のステップ 4 を参照してください。

AP 切断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。

AP 切断の [Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	**説明**
[Status] ドロップダウン リスト	• 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、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。
注アイコン（）	管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。
[Insights]	問題の簡単な要約として、影響を受けるスイッチ、問題の発生日時、スイッチの場所などの情報が表示されます。
[Impact Summary]	影響を受けるサイト、クライアント、および AP の数が表示されます。
[Problem Details]	次の詳細情報が提供されます。 • 問題に関連するデバイスの説明（既知の場合）。 • 関連する問題（ある場合）とその問題の詳細へのリンク。 • 影響を受ける AP、その場所と電力の情報、切断の理由など、問題に関する詳細。 • スイッチとそれに接続されている隣接デバイスを含む物理ネイバートポロジ。

AP 切断の [Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
[Impact Details]	影響を受ける AP に接続されたワイヤレスクライアントとその場所が一覧表示されます。
Suggested Actions	この問題を解決するために実行できるアクションが表示されます。

レイヤ 2 ループ問題の問題インスタンスの詳細

（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題の表示 （301 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、「機械推論エンジンについて （300 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は以下の制約事項があります。

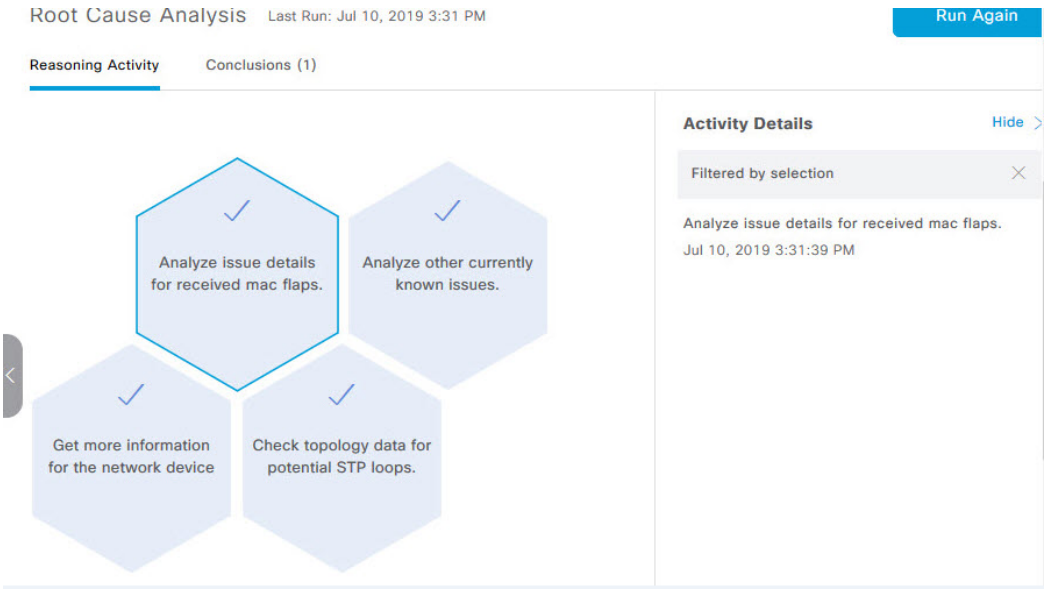
- VLAN 数は 10 です。
- VLAN ごとのデバイス数は 30 です。

機械推論をサポートするレイヤ 2 ループ問題については、Issue Instance Details][スライドインペインに次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
[Status] ドロップダウンリスト	問題のステータスを変更できます。次のタスクを実行します。 • 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、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。
注アイコン（）	管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
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次の項目が表示されます。 • [Relevant Events] ドロップダウンリスト：ループ中に発生したイベントが一覧表示されます。イベントをクリックすると、サイドペインに詳細情報が表示されます。 • [Potential Loop Details] ドロップダウンリスト：ループ情報（デバイス、ロール、ループ状態のポート、デュプレックスモード、ループに関与している VLAN など）が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 1. [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Run Machine Reasoning] ポップアップ ダイアログボックスが表示されます。 2. このポップアップ ダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 3. [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。このアクティビティは、根本原因分析の各ステップで使用されたコマンドを示します。 4.  アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力し、[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、次の図のように、六角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインにアクティビティの詳細が表示されます。 実行中の推論アクティビティをキャンセルするには、[Stop] をクリックします。 （注） チェックマークは、ステップが完了したことを示します。 **図 *36* : 推論アクティビティ** 

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	6. MRE を再実行する場合は、[Run Again] をクリックします。
[Topology] アイコン	アイコンをクリックすると、ループが発生したネットワークセグメントのトポロジが表示されます。

PoE の問題に関する問題インスタンスの詳細

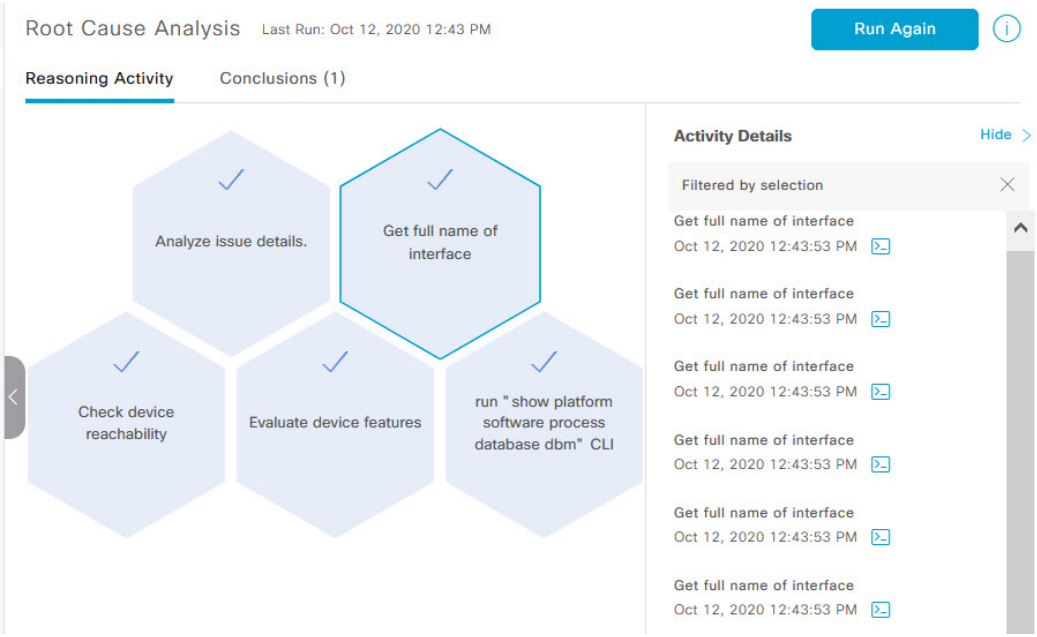
（注） [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題の表示 （301 ページ） 」のステップ 4 を参照してください。

機械推論をサポートする PoE の問題については、[Issue Instance Details] スライドインペインに次の情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
[Status] ドロップダウンリスト	問題のステータスを変更できます。次のタスクを実行します。 • 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから [Ignore] を選択します。 2. スライダを使用して、問題を無視する時間数を設定し、[Confirm] をクリックします。
注アイコン（）	管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。
Summary	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。
Problem Details	問題の簡単な説明と次の情報が表示されます。 • [Event Types] タブ：発生したイベントのタイプのタブが含まれます。イベントのタブをクリックすると、そのイベントタイプに関するエラーのリストが表示されます。 • [Errors]：各イベントタイプに関して発生したエラー。エラーは、クリックした [Event Types] タブに基づいて更新されます。 • [Detailed Information]：エラーをクリックすると、そのエラーに関する追加情報が表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
Root Cause Analysis	

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 **1.** [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。 **2.** このポップアップ ダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 **3.** [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。このアクティビティは、根本原因分析の各ステップで使用されたコマンドを示します。 **4.**  アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力してください。 **5.** [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図のように、六角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインに [Activity Details] が表示されます。 実行中の推論アクティビティをキャンセルするには、[Stop] をクリックします。 （注） チェックマークは、ステップが完了したことを示します。 図 *37 :* 推論アクティビティ

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
	 6. MRE を再実行する場合は、[Run Again] をクリックします。

アプリケーション正常性低下の問題に関する問題インスタンスの詳細

アプリケーションの正常性低下の問題は、次のようなネットワーク イベント インジケータです。

- アプリケーションの正常性スコアが設定されたしきい値を下回っていることを識別します。
- クライアントへの影響の評価とパフォーマンス原因のトラブルシュートに役立つ詳細情報を表示します。
- ThousandEyes からのデータを統合して、根本原因の分析と修復を強化します。

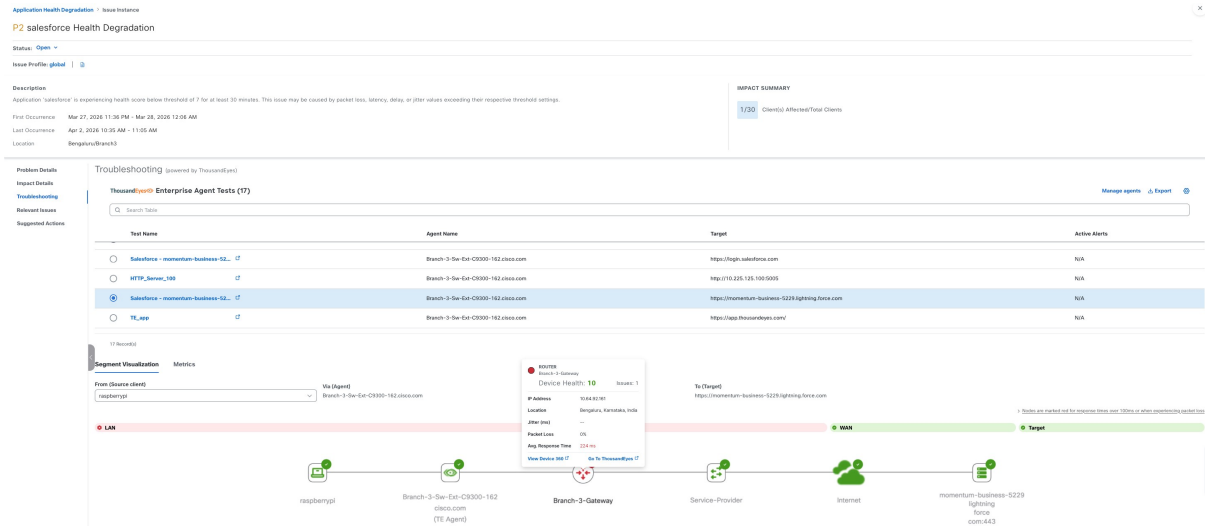
[Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題の表示 （301 ページ） 」のステップ 4 を参照してください。

アプリケーションの正常性低下の問題については、[問題インスタンスの詳細（Issue Instance Details）] スライドインペインに次の情報が表示されます。

- [ステータス（Status）]：問題の現在の状態が表示されます。
- [問題のプロファイル（Issue Profile）]：問題をトリガーしたグローバル設定プロファイルを特定します。

- [説明（Description）]：問題が発生した理由の概要を示します。これには、正常性低下の期間や、しきい値を超えたパケット損失、遅延、ジッターなどの特定のメトリックが含まれます。
- [発生（Occurrences）]：最初の発生および最後の発生のタイムスタンプを表示します。
- [場所（Location）]：正常性低下が発生しているサイトまたはブランチを指定します。
- [影響の概要（Impact Summary）]：そのサイトでアプリケーションを使用しているクライアントの総数に対する、影響を受けたクライアントの数を表示します。

図 *38 : [Issue Instance Details]*（*2* 番目のスライドインペイン）



[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	**説明**
[Status] ドロップダウンリスト	問題のステータスを変更できます。次のタスクを実行します。 • 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、次の手順を実行します。 1. [Status] ドロップダウンリストから [Ignore] を選択します。 2. スライダを使用して、問題を無視する時間数を設定し、[Confirm] をクリックします。
Problem Details	現在のアプリケーションの正常性スコアとパフォーマンス履歴グラフを表示します。このタブでは、低い正常性スコアの原因となっているメトリックを特定します。
[Impact Details]	影響を受ける上位のロケーション、アクセスポイント（AP）、およびスイッチを表示する棒グラフを使用して、問題の範囲を分析します。このタブには、影響を受けるクライアントのリストも表示されます。

[Issue Instance Details]（2 番目のスライドインペイン）	
アイテム	説明
トラブルシューティング	このタブを使用して、アプリケーションの正常性データを ThousandEyes のテスト結果と関連付けます。 • [ThousandEyes Enterprise Agentテスト（ThousandEyes Enterprise Agent Tests）]：アプリケーションに関連付けられたテストデータを表示、管理、またはエクスポートします。 • [セグメントの可視化（Segment Visualization）]：ホップバイホップのパストレースを使用して、問題がどこにあるかを特定します。応答時間が長いノードまたはパケット損失が多いノードが強調表示されるため、問題の原因を LAN、WAN、またはターゲットサーバーに切り分けることができます。
[Suggested Actions]	推奨される手順に従って問題を調査し、解決します。
関連する問題（Relevant Issues）	同じロケーション内の他のアクティブな問題を表示して、アプリケーションの正常性低下がより広範なネットワークイベントの一部であるかどうかを判断します。

MREを使用した有線クライアントの問題のトラブルシューティング

Assurance によって検出された有線クライアントの問題を表示し、MRE ワークフローを使用してトラブルシュートするには、次の手順を使用します。MRE をサポートする有線クライアントの問題のリストについては、MRE の問題 （362 ページ）を参照してください。

始める前に

MRE ナレッジベースが最新のナレッジパックで更新されていることを確認します。機械推論ナレッジベースの更新 （98 ページ）を参照してください。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

ステップ 3 [Wired Clients] サマリーエリアで、[View Details] をクリックしてスライドインペインを開きます。

ステップ 4 スライドインペインの [Wired Clients] チャートで、[Authentication] または [DHCP] をクリックします。

[Authentication] をクリックすると、チャートの下に [Top Authentication Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。認証に失敗したクライアントのリストを示すテーブルも表示されます。

[DHCP] をクリックすると、チャートの下に [Top DHCP Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。テーブルも表示されます。

ステップ 5 次のいずれか 1 つのタスクを実行します。

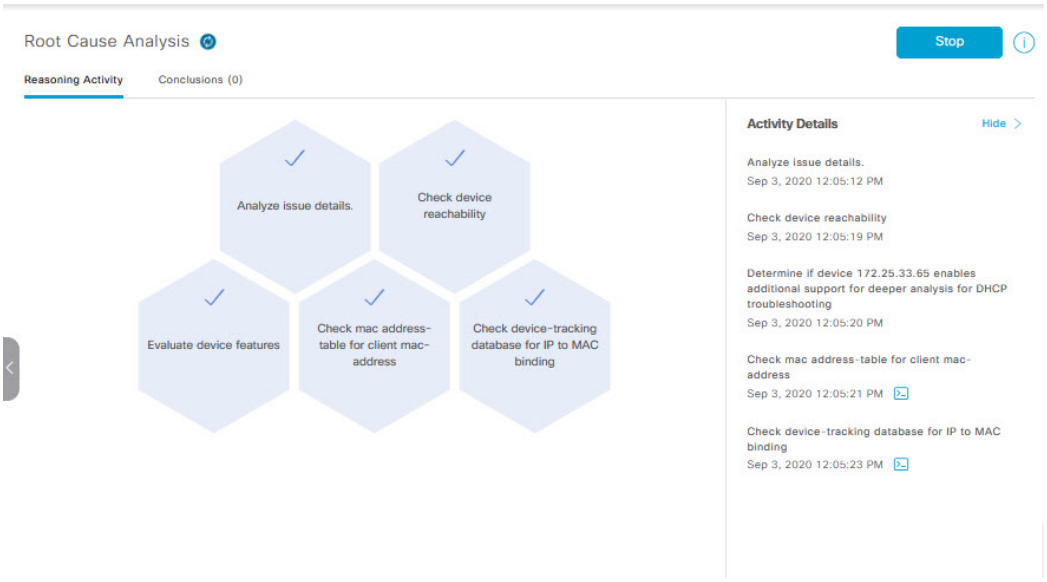
- SUPER-ADMIN-ROLE 権限を持つユーザーの場合は、検索ツールにクライアントの MAC アドレスを入力します。
- テーブルの [Identifier] 列で、ハイパーリンクされた識別子をクリックします。

[Client 360] ウィンドウが表示されます。

ステップ 6 [Client 360] ウィンドウの [Issues] ダッシュレットで、認証または DHCP の問題をクリックします。

[Issue Details] ウィンドウが表示され、次の情報が示されます。

問題の詳細	
アイテム	**説明**
[Status] ドロップダウンリスト	問題の現在のステータスが表示されます。このステータスは変更できます。次のタスクを実行します。 • 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。 • 問題が報告されるのを停止するには、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。
注アイコン（）	管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。
Summary	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。

問題の詳細	
アイテム	説明
Root Cause Analysis	機械推論エンジン（MRE）により、複雑な根本原因を分析して、是正措置を提案できます。 **1.** [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。 **2.** このダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 **3.** [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。 **4.** 👍 👎 アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力し、[Submit] をクリックしてください。 **5.** [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図のように、六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 *39 :* 推論アクティビティ**  **6.** MRE を再実行する場合は、[Run Again] をクリックします。

解決済みの問題の表示

次のカテゴリに分類される解決済みの問題をすべて表示するには、次の手順を実行します。

- しきい値ベースの問題：Assurance 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 の設定 （95 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Issues and Events]**の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 [Status] ドロップダウンリストから、[Resolve] を選択します。

[Resolved Issues] ウィンドウが表示されます。

ステップ 3 [Resolved Issues] ウィンドウには、次の情報が表示されます。

[Resolved Issues] ウィンドウ	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[サイトテーブル（Site Table）] を選択してサイトテーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Resolved Issues] ダッシュボードに表示されます。

[Resolved Issues] ウィンドウ	
アイテム	説明
[24 Hours] ドロップダウンリスト	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Resolved Issue] ウィンドウの [Issue Type] 表	
アイテム	説明
Total Resolved	解決済みの問題の合計数を示します。 [Total Resolved] 値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。
Priority	問題タイプの優先度レベル（事前割り当てされたもの）。
Issue Type	問題のタイプ。 （注） AI 駆動型の問題の場合、 問題のタイプの前に AI アイコンが表示されます。
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題タイプに関するすべての解決済み問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプ、問題を更新したエンティティ名などの情報が表示されます。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

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 （328 ページ）を参照してください。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細（問題を解決したエンティティ名とタイムスタンプ）が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

無視された問題の表示

無視されたとしてマークされているすべての問題を表示するには、次の手順を実行します。無視された問題は次のカテゴリに分類されます。

- しきい値ベースの問題：Assurance 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 の設定 （95 ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Issues and Events]**の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 [Status] ドロップダウンリストから、[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 3 [Ignored Issues]ウィンドウには次の情報が表示されます。

[Ignored Issues] ウィンドウ	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックし、[サイトテーブル（Site Table）] を選択してサイトテーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのデータのみが [Ignored Issues] ダッシュボードに表示されます。
[24 Hours] ドロップダウンリスト	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Ignored Issues] ウィンドウの [Issue Type] テーブル	
アイテム	説明
Total Ignored	無視された問題の合計数が表示されます。 [Total Ignored] の値は、選択したタブに応じて変わります。[All]（デフォルト）、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。
Priority	問題タイプの優先度レベル（事前割り当てされたもの）。
Issue Type	問題のタイプ。 （注） AI 駆動型の問題の場合、 問題のタイプの前に AI アイコンが表示されます。

[Ignored Issues] ウィンドウの [Issue Type] テーブル	
アイテム	説明
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題のタイプのすべての無視された問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプなどの情報が表示されます。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add] をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

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。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Issues and Events]**の順に選択します。

[Open Issues] ダッシュボードが表示されます。

ステップ 2 複数の問題の解決または無視を一括して行うには、次の手順を実行します。

a) [Open Issues] ダッシュボードの [Issue Type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] が開き、その問題タイプに関するすべての未解決問題が一覧表示されます。このスライドインペインでは、問題の解決や無視を一括して行えます。 管理者ユー

ザーは、メモを追加、編集、削除できます。メモアイコン（  ）をクリックし、[Add]をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

b) 次のいずれか 1 つのタスクを実行します。

- 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。

[Warning] ダイアログボックスで、[Yes] をクリックして操作を続行します。

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。 管理者ユーザーは、メモを追加、編集、削除できます。メモアイコン（）をクリックし、[Add]をクリックします。管理者以外のユーザーは、メモ情報のみを表示できます。

b) 問題を解決するには、[Status] ドロップダウンリストで [Resolve] を選択します。
c) 問題が報告されるのを停止するには、次の手順を実行します。

1. [Status] ドロップダウンリストから [Ignore] を選択します。
2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。

無線にアクティビティなしの問題のトリガー

「無線にアクティビティなし」の問題は、次のすべての条件がデフォルトのトリガー時間である 60 分間にわたって満たされるとトリガーされます。

（注） デフォルトのトリガー時間を変更するには、**Assurance** > **[Manage]** > **[Issue Settings]**に移動します。グローバルな問題の設定の管理 （332 ページ）を参照してください。

- AP 無線動作状態は [up] である。
- AP モードはローカルまたは FlexConnect である。
- この無線でクライアント数が 0 である。
- RX データまたは管理フレーム数が増えていない。
- AP 無線チャンネルの使用率が 0 である。
- AP は**分離された** AP ではない。

自動問題解決

次の問題については、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。

問題の名称
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。
スイッチファンの障害。

問題の名称
スイッチの電源の障害。
インターフェイスが停止した。
スタックメンバーの削除
スタックポートリンクに障害が発生した場合
ワイヤレスコントローラ からの AP の切断。
無線でのアクティビティなし。

次の問題は、最後に発生してからの時間に基づいて自動的に解決されます。

問題の名称	自動解決までの時間
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	24 時間
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	24 時間
ネットワークデバイスの HA スイッチオーバー	24 時間
WLC が予期せず再起動	24 時間
AP のリブートクラッシュ	24 時間
デバイス リブート	24 時間
AP 異常	24 時間
AP フラップ	24 時間
フロアでの RF（5 GHz）の低下	24 時間
RF（6 GHz）の低下	24 時間
フロアでの RF（2.4 GHz）の低下	24 時間
AP の高 CPU 使用率	24 時間
AP の高メモリ使用率	24 時間
WLC での AP ライセンス枯渇	24 時間
スイッチの高メモリ使用率	24 時間
デバイスでメモリ使用率が高くなっています。	24 時間

問題の名称	自動解決までの時間
スイッチの高 CPU 使用率	24 時間
ルータの高 CPU 使用率	24 時間
スイッチインターフェイスの入出力使用率が高い	24 時間
スイッチインターフェイスの入出力エラー率が高い	24 時間
スイッチインターフェイスの入出力破棄率が高い	24 時間
スイッチ WAN インターフェイスの入出力破棄率が高い	24 時間
スイッチ WAN インターフェイスの入出力使用率が高い	24 時間
ルータインターフェイスの入出力使用率が高い	24 時間
ルータ WAN インターフェイスの入出力使用率が高い	24 時間
ルータインターフェイスの入出力破棄率が高い	24 時間
ルータ WAN インターフェイスの入出力破棄率が高い	24 時間
ルータ WAN インターフェイスの入出力使用率が高い	24 時間
ボーダーノードからトランジット コントロール プレーン ノードへのファブリック BGP セッションがダウン	6 時間
ファブリック BGP セッションステータスがピアデバイスでダウン（VN 単位）	6 時間
ボーダーノードからコントロールプレーンノードへの BGP セッションがダウン	6 時間
ファブリックボーダーノードのインターネットが使用できない（VN 単位）	6 時間
ファブリックボーダーノードのリモートインターネットが使用できない（VN 単位）	6 時間
ファブリック AAA サーバステータス	6 時間
ファブリック LISP セッションステータスがコントロールプレーンノードへ	6 時間

問題の名称	自動解決までの時間
ファブリック LISP PubSub セッションステータスがダウン（VN 単位）	6 時間
Cisco TrustSec 環境データがファブリックノードで完全ではない	6 時間
ファブリック LISP エクストラネットポリシーステータスがダウン	6 時間
サードパーティデバイスインターフェイスの入出力使用率が高い	24 時間
サードパーティデバイスインターフェイスの入出力エラー率が高い	24 時間
サードパーティデバイスインターフェイスの入出力破棄率が高い	24 時間
サードパーティデバイス WAN インターフェイスの入出力使用率が高い	24 時間
サードパーティデバイス WAN インターフェイスの入出力破棄率が高い	24 時間
高 TCAM 使用率の問題	24 時間
ファブリックデバイスの接続 - ボーダーアンダーレイ	6 時間
ファブリックデバイスの接続 - ボーダーオーバーレイ	6 時間
ファブリックデバイスの接続 - マルチキャスト RP	6 時間
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	6 時間
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	6 時間
ファブリックデバイスの接続 - AAA サーバー	6 時間
ファブリックデバイスの接続 - DHCP オーバーレイ	6 時間
ファブリックデバイスの接続 - DHCP アンダーレイ	6 時間
ファブリックデバイスの接続 - DNS オーバーレイ	6 時間
ファブリックデバイスの接続 - DNS アンダーレイ	6 時間
ファブリック WLC と MapServer の接続性	6 時間

問題の名称	自動解決までの時間
コントロールプレーンノードでのファブリック LISP セッションステータス	6 時間
ファブリック LISP PubSub セッションステータスがダウン	6 時間
ファブリックボーダーノードのインターネットが使用できない	6 時間
ファブリックボーダーノードのリモートインターネットが使用できない	6 時間
ファブリック BGP セッションステータスがピアデバイスでダウン	6 時間

問題が自動的に解決したか、手動で解決されたかを表示できます。**[Issue Settings] の [Global Profile]** ウィンドウ内にある [Issue Resolution] 列に、システムが解決した問題には [Auto] が、手動で解決する問題には [Manual] が表示されます。

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] 列に [System] と表示されます。解決済みの問題の表示, on page 322を参照してください。

グローバルな問題の設定の管理

次の手順に従って、問題の設定を管理します。特定の問題の有効化または無効化、優先順位の変更、問題がトリガーされる際のしきい値の設定が可能です。さらに、到達可能性イベントについて、サイトレベルの相関を設定して、複数のデバイスの障害を単一のインシデントにグループ化できます。これにより、サイト全体の障害時の通知ノイズを削減できます。

Assuranceは、問題へのユーザーのアクセス範囲を制限するサイトベースのロールベース アクセス コントロール（SRBAC）をサポートしています。サイト、デバイス、およびそれらの問題の設定にアクセスできることを確認する必要があります。ユーザーロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Issue Settings]**。

[Global Profile] タブが選択された状態で [Issue Settings] ウィンドウが表示されます。

ステップ 2 [デバイスタイプ（DEVICE TYPE）] フィルタと [カテゴリ（CATEGORY）] フィルタを設定して、問題の設定テーブル内の問題のタイプを表示します。問題の設定テーブルには、優先順位、問題名、問題の解決、有効、グローバル、現在の設定、最終変更日、サブスクリプションが含まれます。

（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。

[問題の解決（Issue Resolution）] 列では、システムによって解決された問題には [自動（Auto）]、解決する必要がある問題には [手動（Manual）] が表示されます。

ステップ 3 問題テーブルで、[問題の名前（Issue Name）] 列の問題をクリックすると、次の設定を含む スライドインペイン が開きます。

（注） いくつかの問題については、設定に加えられた変更は複数のデバイス タイプで共有されます。スライドインペイン で、情報アイコン（ⓘ）にカーソルを合わせると、影響を受けるデバイス タイプが表示されます。

a) 問題がトリガー可能かどうかを有効または無効にするには、[Enabled] トグルをクリックします。

b) 問題の優先順位を設定するには、[Priority] ドロップダウンリストをクリックし、優先順位を選択します。次のオプションがあります。

- [P1]：ネットワーク運用に幅広い影響を与える可能性がある、早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
- [P3]：局所的または最小限の影響を与える軽微な問題。
- [P4]：ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。

c) （一部の問題のみ）[Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。

（注） 到達不能なネットワークデバイスの問題については、次の手順を実行します。

- デバイスしきい値：サイトレベルの問題をトリガーするために到達不能になる必要があるデバイスの最小数を入力します。
- サイトレベル：相関の階層レベル（エリア、建物、またはフロア）を選択します。選択したレベルでしきい値が満たされた場合、単一の関連する問題が生成されます。
- 時間範囲：この問題では、固定された15分の時間枠を使用して複数の障害を検出します。この範囲は設定できません。
- 検出ロジック：到達可能性は1分ごとにチェックされます。pingが3回連続して失敗した後、デバイスは到達不能とマークされます。

「無線にアクティビティなし」のトリガー条件については、無線にアクティビティなしの問題のトリガー （328 ページ）を参照してください。

トリガー条件の例：

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
アクセスポイントのメモリ使用率が 90% を超えた
```

```
建物レベルで到達不能なネットワークデバイスが、15 分以内に 3 台以上検出
```

d) （任意） 設定に変更がある場合は、[View Default Settings] の上にカーソルを置くと、デフォルトの問題が表示されます。問題の設定をすべてデフォルト値に復元するには、[Use Default] をクリックします。

e) [Apply] をクリックします。

ステップ 4 （特定の問題について）[Manage Subscriptions] をクリックすると、サポートされている問題がトリガーされたときの外部通知に登録できます。問題の通知の有効化 （338 ページ）を参照してください。

ユーザー定義問題の設定の管理

ユーザー定義問題の設定を管理するには、次の手順を使用します。ユーザー定義問題を作成する、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。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Issue Settings]**。

[Global Profile] タブが選択された状態で [Issue Settings] ウィンドウが表示されます。

ステップ 2 [User Defined] タブをクリックして、ユーザー定義問題のリストを表示します。

ステップ 3 [Issue Name] 列の問題をクリックして、[Create an Issue] スライドインペイン を開きます。

ステップ 4 syslog の詳細に基づいてユーザー定義問題を設定するには、[Create an Issue] スライドインペイン で次の手順を実行します。

a) [Issue name] フィールドに、問題名を入力します。

b) [Description] フィールドに、問題の説明を入力します。

c) [Syslog Details] の [Severity] ドロップダウンリストから、0 ～ 6 の重大度を選択します。

Assurance は、重大度が 0、1、2（緊急、アラート、クリティカル）のすべての syslog と、重大度 3、4、5、6（エラー、警告、通知、および情報）の一部の syslog をサポートしています。ユーザー定義の問題を作成する場合は、サポートされている syslog を表示して選択できます。

d) [Facility] フィールドに、施設名を入力します。

e) [Mnemonic] フィールドにニーモニック名を入力し、[Next] をクリックします。

f) [Message Pattern] フィールドに、syslog メッセージを入力します。メッセージパターンの下にある syslog メッセージをプレビューできます。

g) [Occurrences] フィールドに、発生回数の値を入力します。

h) [Duration] ドロップダウンリストで、問題の継続時間を選択します。

i) 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。

j) 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、優先順位のレベルを選択します。

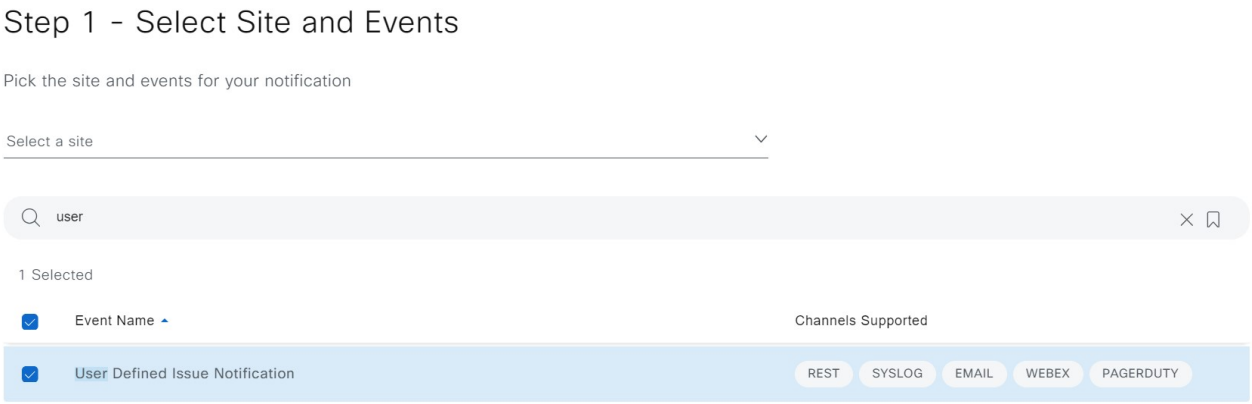
- [P1]：ネットワーク運用に幅広い影響を与える可能性があり、早急な対応を必要とする重大な問題。
- [P2]：複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
- [P3]：局所的または最小限の影響を与える軽微な問題。
- [P4]：ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。

k) 問題の通知を有効または無効にするには、[Notification] トグルをクリックします。

l) [Save] をクリックします。

ステップ 5 問題がトリガーされた場合の問題の外部通知に登録するには、[Manage Subscriptions] をクリックします。問題の通知の有効化 （338 ページ）を参照してください。次に示すように、**ユーザー定義の問題通知**イベントに対するサブスクリプションを作成します。

図 *40 :* ユーザー定義の問題通知イベント



カスタム問題の設定の管理

特定のサイトまたはサイトのグループ用にカスタムの問題設定を作成できます。これらの設定は Assurance のネットワークプロファイルと呼ばれ、Assurance と Catalyst Center の両方から管理できます。

Assurance のネットワークプロファイルを作成することで、監視する問題の設定を制御したり、問題の優先度を変更したりできます。

注：

- ネットワークデバイスの正常性スコアへの同期は、グローバルな問題設定に対してのみ使用できます。カスタムの問題設定では使用できません。詳細については、デバイスの正常性のモニターとトラブルシューティング （117 ページ）を参照してください。
- 一部のグローバルな問題はカスタマイズできません。これらの問題は、変更するカスタム問題のリストには表示されません。
- 変更された問題をリストの一番上に表示するには、[Last Modified] でソートします。
- カスタム設定を削除するには、最初にすべてのサイトの割り当てを解除する必要があります。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Issue Settings]**。

[Global Profile] タブが選択された状態で [Issue Settings] ウィンドウが表示されます。

ステップ 2 [Custom Profile] タブをクリックします。

ステップ 3 [+Add a Profile] をクリックします。

ステップ 4 [Profile Name] フィールドに有効なプロファイルの名前を入力し、[Next] をクリックします。

Catalyst Center によってプロファイルが追加され、プロファイルテーブルにプロファイル名、サイト、およびアクションが表示されます。

ステップ 5 サイトにプロファイルを割り当てるには、[Sites] 列名の [Assign Sites] をクリックして、[Add Sites to Profile] スライドインペインを開きます。このプロファイルを関連付けるサイトの横にあるチェックボックスをオンにし、[Save] をクリックします。

[Edit Profile] ウィンドウが表示されます。

（注） 親ノードまたは個々のサイトを選択できます。親ノードを選択すると、その親ノードに属する子もすべて選択されます。チェックボックスをオフにして、サイトの選択を解除できます。

[アクション（Action）] 列の [コピー（Copy）] をクリックして、既存のプロファイルを複製します。

ステップ 6 [デバイスタイプ（DEVICE TYPE）] および [カテゴリ（CATEGORY）] フィルタを設定し、問題の設定テーブルで問題のタイプを表示します。問題の設定テーブルには、優先順位、問題名、問題の解決、有効、グローバル、現在の設定、最終変更日、サブスクリプションが含まれます。

（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。

[問題の解決（Issue Resolution）] 列では、システムによって解決された問題には [自動（Auto）]、解決する必要がある問題には [手動（Manual）] が表示されます。

ステップ 7 [User Defined] タブをクリックして、ユーザー定義問題のリストを表示します。

ステップ 8 [Issue Name] 列の問題をクリックすると、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は、影響を受けるデバイスタイプを示す注意が Catalyst Center によって表示されます。

ステップ 9 この問題の Catalyst Center によるモニタリングを有効または無効にするには、[Enabled] トグルボタンをクリックします。

ステップ 10 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。

ステップ 11 （一部の問題のみ）[Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。



（注） 到達不能なネットワークデバイスのサイトレベルの相関は、サイトプロファイルごとにカスタマイズできます。たとえば、大きな建物にはデバイスしきい値を高く設定し、特定のフロアには低く設定できます。

トリガー条件の例：

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%
```

ステップ 12 （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、デフォルトの設定が表示されます。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。

ステップ 13 [Apply] をクリックします。

ステップ 14 （特定の問題について）[Manage Subscriptions] をクリックすると、サポートされている問題がトリガーされたときの外部通知に登録できます。

ステップ 15 ユーザー定義の問題を編集するには、問題の syslog メッセージで [Edit] をクリックし、[Save] をクリックします。

ステップ 16 [Done] をクリックします。

新しく追加されたプロファイルは、[Issue Settings] ウィンドウの [Custom Profile] タブに表示されます。

問題の通知の有効化

Assurance 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、 Assurance は、REST または電子メール通知を生成できます。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Issue Settings]**。

[Issue Settings] ウィンドウが表示されます。

ステップ 2 [Manage Subscription] をクリックします。[Events Notifications] ウィンドウが表示されます。

[Platform] > **[Developer Toolkit]** > **[Event Notifications]** ウィンドウが表示されます。各通知はタイルで表され、通知の詳細を表示するためのリンクが含まれています。

ステップ 3 左側のペインの [CHANNELS] エリアで、それぞれの通知タイルを表示するチャネルの横にあるオプションボタンをクリックします。

サポートされているチャネルは、[REST]、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、[EMAIL] です。アシュアランスイベントは SNMP をサポートしていません。

（注）
- それぞれのチャネルでイベントの通知を作成し、通知をトリガーする必要があります。詳細については、*Cisco Catalyst Center User Guide* の「**イベント通知の作成**」を参照してください。
- 1 つのイベント通知で複数のチャネルがサポートされます。
- すべてのユーザー定義の問題は、[User Defined Issue Notification] イベント名にマッピングされます。したがって、ユーザー定義の問題の場合は、その通知イベントに登録する必要があります。

ステップ 4 通知の詳細を表示する通知タイルリンクをクリックします。

[Notification Details] スライドインペインには、選択したチャネルに基づいて次の通知の詳細が表示されます。

- [名前（Name）]：イベントの名前。
- [説明（Description）]：イベントの説明。
- [Sites]
- [Event]
- [REST]：REST 通知の詳細を表示する場合にのみ表示されます。[REST] エリアには、次の情報が表示されます。
  - [URL]：イベントが送信される REST API エンドポイントの URL アドレス。
  - [メソッド（Method）]：PUT メソッドまたは POST メソッド。
  - [信頼できる証明書（Trust certificate）]：REST API エンドポイント通知に信頼できる証明書が必要かどうかを指定します。
  - [ヘッダー（Headers）]：[ヘッダー名（Header Name）] と [ヘッダー値（Header Value）]。
- **[PAGERDUTY]**：PAGERDUTY 通知の詳細を表示する場合にのみ表示されます。[PAGERDUTY] エリアには、次の情報が表示されます。
  - [PagerDuty Events API URL]
  - [PagerDuty Integration Key]
  - [PagerDuty Events API Version]

- [SNMP]：[SNMP] 通知の詳細を表示する場合にのみ表示されます。
- [SYSLOG]：[SYSLOG] 通知の詳細を表示する場合にのみ表示されます。
- [WEBEX]：[WEBEX] 通知の詳細を表示する場合にのみ表示されます。
- [EMAIL]：[EMAIL] 通知の詳細を表示する場合にのみ表示されます。[EMAIL] エリアには、E メール受信者の [From] と [To] と E メールの [Subject] が表示されます。

ステップ 5 [Notification Details] スライドインペインで、右上隅にあるトグルボタンをクリックして、それぞれの通知を有効または無効にします。

ステップ 6 特定の通知を編集するには、[Actions] ドロップダウンリストをクリックし、[Edit] を選択します。

ステップ 7 [EDIT NOTIFICATION] ウィンドウで、選択したチャネルに基づいて以下の設定を行います。

1. [Name] フィールドに一意の名前を入力します。
2. [Description] フィールドに、それぞれのイベントの説明を入力します。
3. [Site and Events] を展開し、[Select a site] ドロップダウンリストからサイトを選択します。
4. イベントの横にあるプラスアイコンをクリックするか、[Add All] をクリックしてすべてのイベントをそれぞれの通知に追加します。
5. 通知からイベントを削除するには、削除するイベントの横にあるプラスアイコンをクリックするか、[Remove All] をクリックして、それぞれの通知からすべてのイベントを削除します。
6. [Configuration] を展開して、選択した通知チャネルの構成を編集します。

   [Configuration] エリアで詳細を指定するには、『*Cisco Catalyst Center User Guide*』の「**Create an Event Notification**」を参照してください。

（注） [Configuration] エリアに表示されるフィールドは、選択した通知チャネルのタイプによって異なります。

ステップ 8 右上隅にあるトグルボタンをクリックして、タイルビューとリストビューを切り替えます。

ステップ 9 [Event Catalog] タブをクリックして、作成されたイベントのリストを表示します。

（注） [Search] フィールドにキーワードを入力することで表示されるイベントを調整できます。

ステップ 10 テーブル内の個々のイベントのデータを確認します。

以下の [Event Details] タブのデータが表示されます。

- [説明（Description）]：イベントとそれを発生させるトリガーの簡単な説明。
- [イベントID（Event ID）]：イベントの識別番号。

- [バージョン（Version）]：イベントのバージョン番号。
- [名前空間（Namespace）]： イベントの名前空間。
- [Severity]：1 ー 5。

（注） シビラティ（重大度） 1 は最も重要または重大な優先度であり、このタイプのイベントに割り当てる必要があります。

- [Domain]：イベントが属する REST API ドメイン。
- [サブドメイン（Subdomain）]：イベントが属する REST API ドメインの配下のサブグループ。
- [Category]：エラー、警告、情報、アラート、タスクの進捗状況、タスクの完了。
- [コメント（Note）]：イベントの理解に役立つ追加情報。
- [イベントリンク（Event Link）]：REST URL を使用したイベントブロードキャスト。
- [タグ（Tags）]：イベントの影響を受ける Catalyst Center のコンポーネントを示すタグ。
- [チャネル（Channels）]：イベント通知でサポートされているチャネル（REST API、電子メール、Webex など）。
- [モデルスキーマ（Model Schema）]：イベントに関するモデルスキーマが提示されます。
  - [詳細（Details）]：イベントのモデルスキーマの詳細の例。
  - [REST Schema]：イベントの REST スキーマのフォーマット。

ステップ 11 [Notifications] タブをクリックして、それぞれのイベントに関連付けられたアクティブな通知を表示します。

Assurance、Cisco AI Network Analytics、および MRE の問題

ルータの問題

Assurance 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**	**概要**
接続性	BGP トンネル接続	自律システム（AS）番号が間違っているため、ピアとのボーダーゲートウェイ プロトコル（BGP）接続に失敗しました。
接続性	ネットワークデバイスを接続しているインターフェイスでダウン発生	ネットワークデバイスに接続しているインターフェイスがダウンしています。 この問題は、他のデバイスに接続されているインターフェイス（デバイス間接続リンク）に適用されます。この問題は、クライアント接続のインターフェイスおよびリンクには適用されません。
接続性	レイヤ 2 のループ症状	ネットワークデバイスでホストMACアドレスのフラッピングが見られます。
接続性	ネットワークデバイスインターフェイスの接続 - BGP フラップ	ネイバーとのボーダー ゲートウェイ プロトコル（BGP）接続がフラッピングしています。
接続性	ネットワークデバイスのインターフェイスの接続 - BGP ダウン	ネイバーとの BGP 接続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 - EIGRP 隣接関係の障害	ネイバーとの Enhanced Interior Gateway Routing Protocol（EIGRP）隣接関係に障害が発生しました。
接続性	ネットワークデバイスインターフェイスの接続 - インターフェイスダウン	デバイス上のインターフェイスがダウンしています。
接続性	ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害	デバイスで Intermediate System Intermediate System（ISIS）の隣接関係に障害が発生しました。
接続性	ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害	ネイバーとの Open Shortest Path First（OSPF）隣接関係に障害が発生しました。
接続	WAN インターフェイスダウン	WAN インターフェイスがダウンしています。
接続されている状態	SGT のアクセスポリシーのインストールに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセスポリシーのインストールに失敗しました。
接続されている状態	ルータインターフェイスの入出力エラー率が高い	ルータインターフェイスで、高い入出力エラー率が検出されました。しきい値はカスタマイズできます。

ルータの問題		
カテゴリ	問題の名称	概要
接続されている状態	ルータインターフェイスの入出力破棄率が高い	ルータインターフェイスで、高い入出力廃棄率が検出されました。しきい値はカスタマイズできます。
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	ルータインターフェイスで、高い入出力エラー率が検出されました。しきい値はカスタマイズできます。
接続されている状態	ルータ WAN インターフェイスの入出力破棄率が高い	ルータの WAN インターフェイスで、高い入出力廃棄率が検出されました。しきい値はカスタマイズできます。
接続されている状態	ルータ WAN インターフェイスの入力/出力使用率が高い	WAN インターフェイスの入出力使用率が高くなっています。 ルータの WAN インターフェイスで、高い入出力エラー率が検出されました。しきい値はカスタマイズできます。
接続されている状態	デバイスでSGTアクセスポリシーのダウンロードに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセス コントロール エントリ（ACE）のダウンロードに失敗しました。
接続されている状態	デバイスでSGTアクセスポリシーのインストールに失敗	セキュリティグループタグ（SGT）のアクセスポリシーのインストールに失敗しました。ロールベースのアクセスコントロールリスト（RBACL）でポリシールールエラーが見つかりました。
接続されている状態	ポリシーサーバーからSGTアクセスポリシーをダウンロードできない	セキュリティグループタグ（SGT）のアクセスポリシーのソースリストをダウンロードできませんでした。
接続されている状態	デバイスでSGTアクセスポリシーのアンインストールに失敗	セキュリティグループタグ（SGT）のセキュリティ グループ アクセス コントロール リスト（SGACL）アクセスポリシーのアンインストールに失敗しました。
デバイス	Catalyst Center とネットワークデバイスの時間がずれています	Catalyst 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	ルータの CPU 使用率が高くなっています。しきい値はカスタマイズできます。
デバイス	ルータの高メモリ使用率	ルータのメモリ使用率が高くなっています。しきい値はカスタマイズできます。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスで高可用性（HA）スイッチオーバーが発生しました。

ルータの問題		
カテゴリ	**問題の名称**	**概要**
可用性	ルータ到達不能	ルータは、Catalyst Center から ICMP または SNMP を介して到達できません。

コア層、ディストリビューション層、アクセス層に関する問題

Assurance によって検出されるコア層、ディストリビューション層、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、アクセス層に関する問題		
カテゴリ	**問題の名称**	**概要**
接続性	BGP トンネル接続	自律システム（AS）番号が間違っているため、ピアとの BGP 接続に失敗しました。
接続性	ネットワークデバイスを接続しているインターフェイスでダウン発生	ネットワークデバイスに接続しているインターフェイスがダウンしています。 この問題は、他のデバイスに接続されているインターフェイス（デバイス間接続リンク）に適用されます。この問題は、クライアント接続のインターフェイスおよびリンクには適用されません。
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のインターフェイスの接続 - BGP ダウン	ネイバーとの BGP 接続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 - BGP フラップ	ネイバーとの BGP 接続がフラッピングしています。
接続性	ネットワーク デバイス インターフェイスの接続 - EIGRP 隣接関係の障害	ネイバーとの EIGRP（Enhanced Interior Gateway Routing Protocol）隣接関係に障害が発生しました。
接続性	ネットワークデバイスインターフェイスの接続 - インターフェイスダウン	デバイス上のインターフェイスがダウンしています。
接続性	ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害	デバイスで Intermediate System Intermediate System（IS-IS）の隣接関係に障害が発生しました。

コア層、ディストリビューション層、アクセス層に関する問題		
カテゴリ	**問題の名称**	**概要**
接続性	ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害	ネイバーとの Open Shortest Path First（OSPF）隣接関係に障害が発生しました。
接続	WAN インターフェイスダウン	WAN インターフェイスがダウンしています。
接続性	ネットワークデバイスでデュアルアクティブ検出リンクに障害発生	ネットワークデバイス *Switch Name* でデュアルアクティブ検出リンクに障害が発生しました。
接続性	ネットワークデバイスで StackWise Virtual リンクに障害発生	ネットワークデバイスの *Switch Name* で StackWise Virtual リンクに障害が発生しました。
接続	ネットワークデバイスで StackWise リンクに障害発生	ネットワークデバイス *Switch Name* で StackWise リンクに障害が発生しました。
接続	トランシーバインターフェイスでの低送信電力	送信電力値がトランシーバ インターフェイスでアラームしきい値の下限を下回っています。
接続	トランシーバインターフェイスでの高送信電力	送信電力値がトランシーバ インターフェイスでアラームしきい値の上限を超えています。
接続	トランシーバインターフェイスでの低受信電力	受信電力 $value$dBm がトランシーバインターフェイスのアラームしきい値の下限を下回っています。
接続	トランシーバインターフェイスでの高受信電力	受信電力がトランシーバ インターフェイスのアラームしきい値の上限を超えています。
接続	トランシーバインターフェイスでの高温	温度がトランシーバ インターフェイスでアラームしきい値の上限を超えています。
接続	トランシーバインターフェイスでの低電圧	電圧がトランシーバ インターフェイスのアラームしきい値の下限を下回っています。
接続	トランシーバインターフェイスでの高電圧	電圧がトランシーバ インターフェイスのアラームしきい値の上限を超えています。
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 ノードが、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。

コア層、ディストリビューション層、アクセス層に関する問題		
カテゴリ	問題の名称	概要
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が、物理ネットワーク内のファブリック コントロール プレーン デバイスへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DHCP オーバーレイ	ファブリックノードが仮想ネットワーク内の DHCP サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DHCP アンダーレイ	ファブリックノードが物理ネットワーク内の DHCP サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DNS オーバーレイ	ファブリックノードが仮想ネットワーク内の DNS サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - DNS アンダーレイ	ファブリックノードが物理ネットワーク内の DNS サーバーへの接続を失いました。
接続されている状態	ファブリックデバイスの接続 - 外部 URL	ユーザーがプロビジョニングした外部 URL にファブリックボーダーが到達できません。
接続されている状態	ファブリックデバイスの接続 - ISE サーバー	ファブリックエッジが物理ネットワーク内の ISE サーバーへの接続を失いました。
接続されている状態	ファブリック WLC と MapServer の接続性	ファブリック ワイヤレスコントローラ でファブリック コントロール プレーン ノードへの接続が失われました。
接続されている状態	ファブリックとポートチャネルの接続性	ポートチャネルに接続しているファブリックノードがダウンしています。
接続されている状態	ファブリック AAA サーバステータス	ファブリックノードの AAA サーバステータスがダウンしています。
接続されている状態	ファブリックデバイスの接続 - マルチキャスト RP	ファブリックボーダーノードは、マルチキャスト ランデブー ポイント（RP）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 コントロールプレーンとの BGP セッションの状態	BGP セッションは、ファブリック サイトのコントロールプレーンとの境界でダウンしています。
接続されている状態	Fabric Control Plane - LISP セッションの状態	コントロールプレーンノードへの LISP セッションがダウンしています。
接続されている状態	Fabric Devices Connectivity - インターネットの接続	コントロールプレーンノードのデフォルトルートが失われたため、インターネットは使用できません。
接続されている状態	ファブリック エクストラネット ポリシー ステータス	ファブリック エクストラネット ポリシーのステータスがダウンしています。

コア層、ディストリビューション層、アクセス層に関する問題		
カテゴリ	問題の名称	概要
接続されている状態	Fabric Control Plane - LISP Pub/Sub セッションステータス	コントロールプレーンノードへの LISP Pub/Sub セッションがダウンしています。
接続されている状態	ファブリックデバイスの接続 - AAA サーバー	ファブリックエッジノードが物理ネットワーク内の AAA サーバーへの接続を失いました。
接続されている状態	Fabric Devices Connectivity - リモートインターネット接続	コントロールプレーン ノードのリモートインターネットへの接続が失われました。
接続されている状態	ピア デバイスへの BGP セッション ステータス	BGP セッションは、サイトの IP トランジットピアとの境界でダウンしています。
接続されている状態	トランジットコントロールプレーンへの BGP セッションステータス	BGP セッションは、SD-Access トランジットに接続された境界でダウンしています。
接続されている状態	ファブリックデバイスの接続 - アンカーされたボーダー	ファブリックボーダーノードが、物理ネットワーク内のファブリックのアンカーされたボーダーノード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で、高い入出力エラー率が検出されました。しきい値はカスタマイズできます。
接続されている状態	スイッチインターフェイスの入出力破棄率が高い	スイッチインターフェイスで高い入出力廃棄率が検出されました。しきい値はカスタマイズできます。
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	スイッチインターフェイスで、高い入出力エラー率が検出されました。しきい値はカスタマイズできます。
接続されている状態	デバイスで SGT アクセスポリシーのダウンロードに失敗	SGT の SGACL ACE のダウンロードに失敗しました。
接続されている状態	デバイスで SGT アクセスポリシーのインストールに失敗	SGT のアクセスポリシーのインストールに失敗しました。RBACL でポリシー規則エラーが検出されました。
接続されている状態	ポリシーサーバーから SGT アクセスポリシーをダウンロードできない	SGT のアクセスポリシーのソースリストをダウンロードできませんでした。
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。

コア層、ディストリビューション層、アクセス層に関する問題		
カテゴリ	**問題の名称**	**概要**
デバイス	デバイス時間のずれ Catalyst Center	Catalyst Center とデバイスネットワーク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。 デフォルトでは、この問題はインターフェイスが 30 分以内に 3 回以上フラップするとトリガーされます。デフォルトのフラップトリガーを変更できます。
デバイス	syslog イベントに基づく問題 - 高温	高温に関連する syslog イベントの単一オカレンスによって作成された問題。
デバイス	syslog イベントに基づく問題 - POE	電源に関連する syslog イベントの単一オカレンスによって作成された問題。
デバイス	PoE ポートがエラー状態	PoE ポートがエラーにより無効になっていることが syslog イベントで報告されました。
デバイス	PoE 受電デバイスに障害フラグあり	PoE ポートに接続された PoE 対応デバイスに障害フラグが設定されていることが syslog イベントで報告されました。
デバイス	PoE 受電デバイスへの電力供給拒否	PoE ポートに接続された PoE 対応デバイスへの電力供給が拒否されたことが syslog イベントで報告されました。
デバイス	スタックメンバーの削除	スタックメンバーが削除されました。
デバイス	スタックメンバーが互換性のないイメージを実行	スタックメンバーが互換性のないイメージを実行しています。
デバイス	スイッチの高 CPU 使用率	スイッチの CPU 使用率が高くなっています。しきい値はカスタマイズできます。
デバイス	スイッチの高メモリ使用率	スイッチのメモリ使用率が高くなっています。しきい値はカスタマイズできます。
デバイス	スイッチファンの障害	スイッチのファンに障害が発生しました。
デバイス	スイッチの電源障害	スイッチの電源に障害が発生しました。
デバイス	高 TCAM 使用率の問題	レイヤ 2、レイヤ 3、QoS、および SGACL での TCAM 枯渇の問題。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスで HA スイッチオーバーが発生しました。
可用性	スイッチ到達不能	スイッチは、ICMP または SNMP を介して Catalyst Center に到達できません。

コア層、ディストリビューション層、アクセス層に関する問題		
カテゴリ	問題の名称	概要
使用率	マップキャッシュの上限に達した	マップキャッシュエントリがマップサーバーの上限を超えました。
システム	アシュアランステレメトリのステータスが不良です	データ損失により、ネットワークデバイス、または有線もしくはワイヤレスのクライアントが影響を受けます。

サードパーティ製デバイスの問題

Assurance によって検出されるサードパーティ製デバイスの問題を次の表に示します。

サードパーティ製デバイスの問題		
カテゴリ	問題の名称	概要
可用性	サードパーティ製デバイスに到達できません	Catalyst Center から ICMP または SNMP 経由でサードパーティ製デバイスに到達できません。
接続	サードパーティ製デバイスインターフェイスの入出力エラー率が高い	サードパーティ製デバイスインターフェイスで高い入出力エラー率が検出されます。しきい値はカスタマイズできます。
接続されている状態	サードパーティ製デバイスインターフェイスの入出力破棄率が高い	サードパーティ製デバイスインターフェイスで高い入出力破棄率が検出されます。しきい値がカスタマイズされています。
接続	サードパーティ製デバイスインターフェイスの入出力使用率が高い	サードパーティ製デバイスインターフェイスで高い入出力使用率が検出されます。しきい値はカスタマイズできます。
接続されている状態	サードパーティ製デバイスのWANインターフェイスの入出力破棄率が高い	サードパーティ製デバイスのWANインターフェイスで高い入出力破棄率が検出されます。しきい値はカスタマイズできます。
接続されている状態	サードパーティ製デバイスのWANインターフェイスの入出力使用率が高い	サードパーティ製デバイスのWANインターフェイスで高い入出力使用率が検出されます。しきい値はカスタマイズできます。

コントローラの問題

Assurance 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**	**概要**
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に接続しているインターフェイスがダウンしています。 この問題は、他のデバイスに接続されているインターフェイス（デバイス間接続リンク）に適用されます。この問題は、クライアント接続のインターフェイスおよびリンクには適用されません。
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 ワイヤレスコントローラ でファブリック コントロール プレーン ノードへの接続が失われました。
デバイス	デバイス時間のずれ Catalyst Center	Catalyst Center とネットワークデバイス間に過剰なタイムラグがあります。 この問題は、Catalyst Center とデバイスの時間差が 10 分を超える場合にトリガーされます。
可用性	ネットワークデバイスの HA スイッチオーバー	ネットワークデバイスでHAスイッチオーバーが発生しました。
可用性	WLC モニター	ネットワークコントローラが ワイヤレスコントローラ からデータを受信していません。
可用性	WLC 電源の障害	このワイヤレスコントローラで電源が故障しました。
可用性	WLC のリブートクラッシュ	ワイヤレスコントローラの再起動クラッシュが発生しました。
可用性	WLC 到達不能	ワイヤレスコントローラは、Catalyst Center から ICMP または SNMP を介して到達できません。
使用率	WLC での AP ライセンス枯渇	ワイヤレスコントローラ には現在、空いている AP ライセンスはありません。
使用率	WLC 高メモリ使用率	ワイヤレスコントローラ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

Assurance 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**	**概要**
可用性	AP のカバレッジホール	ワイヤレス LAN コントローラが AP 周辺のカバレッジホールを検出しました。

アクセスポイントの問題		
カテゴリ	**問題の名称**	**概要**
可用性	WLC からの AP の切断	AP がワイヤレス LAN コントローラから切断されます。ワイヤレス LAN コントローラへの AP の CAPWAP リンクがダウンしています。 この問題は、APがワイヤレスコントローラから切断されたときに AP によって発生します。この問題は [AP 360] ウィンドウに表示されますが、[Issues] ダッシュボードには表示されません。この問題の通知を登録できます。 「**スイッチで WLC から切断された AP**」の問題に登録することを推奨します。「**WLC から切断された AP**」の問題ではありません。
可用性	スイッチで WLC から切断された AP	スイッチで、AP がワイヤレス LAN コントローラから切断されています。 この問題はアクセススイッチに集約されます。スイッチで切断されたAPの数に関係なく、アクセススイッチごとに1つの問題が生成されます。 たとえば、2 つのスイッチで 10 個の AP が切断された場合、Assurance は 2 つの問題を生成します。 切断された AP は、問題の詳細に表示されます。この問題は [Issues] ダッシュボードに表示されます。この問題の通知を登録できます。
可用性	AP のフラッピング	AP でフラッピングが発生しています。APがワイヤレスLANコントローラから切断され、ワイヤレスLANコントローラに再び接続しました。 この問題は AP が 15 分以内に 2 回以上フラップするとトリガーされます。
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	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	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	無線の高使用率（2.4 GHz）	AP の 2.4 GHz 無線の使用率が高くなっています。
使用率	無線の高使用率（5 GHz）	AP の 5 GHz 無線の使用率が高くなっています。
使用率	無線の高使用率（6 GHz）	AP の 6 GHz 無線の使用率が高くなっています。

アクセスポイントの問題		
カテゴリ	**問題の名称**	**概要**
使用率	無線でのアクティビティなし（2.4 GHz）	AP の 2.4 GHz 無線でアクティビティがありません。
使用率	無線でのアクティビティなし（5 GHz）	AP の 5 GHz 無線でアクティビティがありません。
使用率	無線でのアクティビティなし（6GHz）	AP の 6 GHz 無線でアクティビティがありません。
AP 異常	AP 異常	AP で異常が発生しました。
可用性	フロアでの RF（2.4 GHz）の低下	この問題は、APのワイヤレスエクスペリエンスが低い場合に発生します。RF の低下の問題は、少なくとも 1 つの AP の干渉またはノイズが、30分以内にしきい値を超えた場合に発生します。
可用性	フロアでの RF（5 GHz）の低下	この問題は、APのワイヤレスエクスペリエンスが低い場合に発生します。RF の低下の問題は、少なくとも 1 つの AP の干渉またはノイズが、30分以内にしきい値を超えた場合に発生します。
可用性	フロアでの RF（6 GHz）の低下	この問題は、APのワイヤレスエクスペリエンスが低い場合に発生します。RF の低下の問題は、少なくとも 1 つの AP の干渉またはノイズが、30分以内にしきい値を超えた場合に発生します。
可用性	無線ダウン（2.4GHz）	AP で 2.4 GHz 無線がダウンしています。
可用性	無線ダウン（5GHz）	AP で 5 GHz 無線がダウンしています。
可用性	無線ダウン（6GHz）	AP で 6 GHz 無線がダウンしています。

有線クライアントの問題

Assurance によって検出される有線クライアントの問題の一覧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**	**概要**
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IP アドレスを取得できませんでした。
オンボーディング	有線クライアント認証エラー - Dot1.x エラー	Dot1.x の問題が原因で、有線クライアントの認証に失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。

有線クライアントの問題		
カテゴリ	**問題の名称**	**概要**
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	MAC認証バイパスの問題が原因で、有線クライアントの認証に失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。

ワイヤレスクライアントの問題

Assurance 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**	**概要**
オンボーディング	802.11r クライアントの低速ローミング	高速ローミングが可能なワイヤレスクライアントが、ローミング中に高速認証ではなくフル認証を実行しています。
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IP アドレスを取得できませんでした。
オンボーディング	ワイヤレスクライアントの除外 - クライアントがローミング前に除外される	ワイヤレスクライアントの除外 - クライアントがローミングの前に除外されました。
オンボーディング	ワイヤレスクライアントの接続失敗 - 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 タイムアウト	ワイヤレスクライアントの接続に 10 秒を超える時間がかかりました。DHCP サーバーまたはクライアントのタイムアウトにより、IP 学習フェーズで遅延が発生しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - 不正な PSK	複数のワイヤレスクライアントが接続に失敗し、ワイヤレスコントローラによって除外されました。クライアントの PSK が、設定された WLAN PSK と一致しなかったため、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 - ワイヤレスコントローラ内部エラー。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**概要**
オンボーディング	ワイヤレスクライアントのローミング失敗 - AAA サーバーによるクライアントの拒否	ワイヤレスクライアントのローミング失敗 - AAA サーバーによりクライアントが拒否されました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - AAA サーバーのタイムアウト	ワイヤレスクライアントのローミング失敗 - AAA サーバーでタイムアウトが発生しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - クライアント PMK 未検出	ワイヤレスクライアントのローミング失敗 - クライアント PMK が見つかりません。
オンボーディング	ワイヤレスクライアントのローミング失敗 - クライアントのタイムアウト	ワイヤレスクライアントのローミング失敗 - クライアントのタイムアウトにより認証に失敗しました。
オンボーディング	ワイヤレスクライアントのローミング失敗 - セキュリティパラメータの不一致	ワイヤレスクライアントのローミング失敗 - セキュリティパラメータが一致していません。
オンボーディング	ワイヤレスクライアントのローミング失敗 - WLC 設定エラー	ワイヤレスクライアントのローミング失敗 - ワイヤレスコントローラ 設定エラー。
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 - ワイヤレスコントローラ 内部エラー。
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 LAN コントローラの設定不一致により、複数のワイヤレスクライアントが AP 間のローミングで失敗しました。
オンボーディング	ワイヤレスクライアントの接続に時間がかかった - 認証タイムアウトによる過剰な時間	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかったのは、認証のタイムアウトが原因です。この問題が発生するクライアントは、AAA サーバーまたはワイヤレスコントローラでグループ化されています。
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 サーバーの障害による過剰な時間	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかるのは、DHCP サーバーの障害が原因です。この問題が発生するクライアントは、DHCP サーバーまたはワイヤレスコントローラです。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**概要**
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った - ログイン情報エラーによる過剰な接続時間	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかったのは、ログイン情報エラーによる認証の遅延が原因でした。この問題が発生するクライアントは、AAA サーバーまたはワイヤレスコントローラでグループ化されています。
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った - WLC の障害による過剰な時間	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかったのは、認証中のワイヤレス LAN コントローラの障害が原因でした。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されています。
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った - AAA サーバーまたはネットワークの遅延による過剰な認証時間	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかったのは、認証の遅延が原因でした。認証の遅延は、AAA サーバーまたはネットワークの遅延によるものでした。
オンボーディング	ワイヤレスクライアントの除外 - IP 盗難の問題	複数のワイヤレスクライアントが、ワイヤレスネットワークへの接続から除外されました。クライアントで IP 盗難の問題が検出されました。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されています。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーによるクライアントの拒否	AAA サーバーの拒否の失敗が理由で、複数のワイヤレスクライアントが認証に失敗しました。AAA サーバーがクライアントの認証要求を拒否しました。この問題が発生するクライアントは、AAA サーバーまたはワイヤレスコントローラでグループ化されています。
オンボーディング	ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウト	AAA サーバーのタイムアウトの失敗により、複数のワイヤレスクライアントが認証に失敗しました。この障害は、ワイヤレスコントローラがAAA からクライアントの認証メッセージに対する応答を受信せず、再試行後にタイムアウトした場合に発生します。この問題が発生するクライアントは、AAA サーバーまたはワイヤレスコントローラでグループ化されています。
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	認証の問題により、複数のワイヤレスクライアントが接続に失敗しました。クライアントの PMK が見つかりませんでした。
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 サーバーのタイムアウト	複数のワイヤレスクライアントが接続に失敗しました。DHCP サーバーのタイムアウトにより、IP 学習フェーズで障害が発生しました。複数のワイヤレスクライアントが接続に失敗しました。この問題が発生するクライアントは、DHCP サーバーまたはワイヤレスコントローラでグループ化されています。

ワイヤレスクライアントの問題		
カテゴリ	**問題の名称**	**概要**
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	複数のワイヤレスクライアントが接続に失敗しました。クライアントがタイムアウトしたため、認証に失敗しました。クライアントが認証メッセージに時間内に応答できませんでした。この問題が発生するクライアントは、サイトまたはAPグループでグループ化されます。
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	複数のワイヤレスクライアントが接続に失敗しました。クライアントがタイムアウトしたため、IP アドレスを取得できませんでした。クライアントが DHCP メッセージに時間内に応答できませんでした。この問題が発生するクライアントは、サイトまたは AP グループでグループ化されます。
オンボーディング	ワイヤレスクライアントの接続失敗 - DHCPサーバーまたはクライアントのタイムアウトによるIPアドレスを取得失敗	複数のワイヤレスクライアントが接続に失敗しました。DHCP サーバーのタイムアウト、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。DHCP サーバーまたはクライアントが DHCP メッセージに時間内に応答できませんでした。この問題が発生するクライアントは、サイトまたは AP グループでグループ化されます。
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	セキュリティパラメータの不一致が原因で発生した認証の問題により、複数のワイヤレスクライアントが接続に失敗しました。
オンボーディング	ワイヤレスクライアントの接続失敗 - WLC 設定エラー	認証の問題により、複数のワイヤレスクライアントが接続に失敗しました。ワイヤレスLANコントローラの設定エラーがあります。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されています。
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	複数のワイヤレスクライアントがローミングに失敗しました。クライアントは、ワイヤレスLANコントローラのクライアント除外ポリシーにより除外されました。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されています。
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	複数のワイヤレスクライアントがローミングに失敗しました。クライアントは、ローミング前にワイヤレスLANコントローラで除外されました。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されています。
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LANコントローラの設定不一致により、複数のワイヤレスクライアントが AP 間のローミングで失敗しました。

ワイヤレスクライアントの問題		
カテゴリ	問題の名称	概要
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	複数のワイヤレスクライアントの接続に時間がかかりました。オンボーディングに過剰に時間がかかったのは、認証中のワイヤレス LAN コントローラの障害が原因でした。この問題が発生するクライアントは、ワイヤレスコントローラでグループ化されます。
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

AAA 障害の根本原因分析問題を有効化

Catalyst Center は、Cisco ISE syslog と統合して、次の問題をトラブルシューティングします。

- ワイヤレスクライアントの接続失敗：AAA サーバーによりクライアントが拒否されました
- ワイヤレスクライアントの接続失敗：AAA サーバーのタイムアウト

トラブルシューティング ワークフローは、[Client 360] ウィンドウの単一のクライアントの問題から、または [Issues] ダッシュボードのワイヤレスクライアントの問題からアクセスする MRE ワークフローです。

Catalyst Center は、クライアント認証の失敗に対して Cisco ISE によって生成された syslog を表示します。これにより、Cisco ISE にログインしてそこでクライアントを検索することなく、クライアント認証の失敗の根本原因を特定できます。

AAA 障害の根本原因分析の問題を Assurance で有効化するには、次の手順を実行します。

手順

ステップ 1 Catalyst Center で、**[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** の順に選択し、Cisco ISE を Catalyst Center に追加して設定します。この手順により、Cisco ISE ポリシーサービスノード（PSN）が syslog 許可リストに追加されます。

ステップ 2 Cisco ISE で、**[Administration]** > **[System]** > **[Logging]** > **[Remote Logging Targets]** の順に選択し、Catalyst Center を syslog の接続先として追加します。

ステップ 3 Cisco ISE で、**[Administration]** > **[System]** > **[Logging]** > **[Logging Categories]** の順に選択し、前の手順で追加したターゲットを [Failed Attempts]、[Authentication Flow Diagnostics]、および [RADIUS Diagnostics] ロギングカテゴリに追加します。

Cisco ISE syslog を Catalyst Center に送信できるようになりました。Catalyst Center はクライアントのオンボーディングの問題について、Cisco ISE syslog を処理して保存します。

アプリケーションは、次を発行する。

Assurance 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。

アプリケーションは、次を発行する。		
カテゴリ	**問題の名称**	**概要**
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

Assurance によって検出されるセンサーの問題を次の表に示します。

同じフロアにある 2 つ以上のセンサーが 30 分間のテストに失敗した場合、センサーは失敗の根本原因に基づいて問題を報告することがあります。これらのセンサーの問題はすべてグローバルな問題です。つまり、すべてのフロアのセンサーの問題がエスカレーションされて、[Issues] ダッシュボードに表示されます。

センサーの問題		
カテゴリ	**問題の名称**	**概要**
センサーテスト	センサー - 速度テスト HTTP エラー	クエリサーバーへのアクセス中、複数のセンサーが速度テスト HTTP エラーを報告しています。
センサーテスト	センサー - DHCPの障害	複数のセンサーが IPv4 アドレスを取得できませんでした。
センサーテスト	センサー - DNS 解決の失敗	複数のセンサーが DNS サーバーによるドメイン名の解決に失敗しました。
センサーテスト	センサー - オンボーディング時の関連付けの失敗	複数のセンサーがオンボーディング時の関連付けに失敗しました。
センサーテスト	センサー - オンボーディング時の認証の失敗	複数のセンサーがオンボーディング時の認証に失敗しました

センサーの問題		
カテゴリ	問題の名称	概要
センサーテスト	センサー - FTP テスト失敗	複数のセンサーが FTP サーバーに接続できないことを報告しています。
センサーテスト	センサー - FTP 転送の失敗	複数のセンサーが FTP サーバーとのファイル転送に失敗したことを報告しています。
センサーテスト	センサー - FTP 到達不能	複数のセンサーが FTP サーバーに到達できないことを報告しています。
センサーテスト	センサー - IPerf の無効な設定エラー	無効な iPerf 設定を受信したため、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPerf サーバーがビジー状態	iPerf のビジー状態エラーが原因で、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPerf テストネットワークエラー	iPerf のネットワークエラーが原因で、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPerf 未定義のエラー	未定義エラーが原因で、複数のセンサーが iPerf テストを実行できませんでした。
センサーテスト	センサー - IPSLA IP アドレスなし	複数のセンサーが Catalyst Center から IPSLA テスト IP アドレスを受信していないことを報告しています。
センサーテスト	センサー - IPSLA 応答なし	複数のセンサーが IPSLA テストで IPSLA 応答側からの応答がないことを報告しています。
センサーテスト	センサー - IPSLA ソケットエラー	複数のセンサーが IPSLA テストソケットエラーを報告しています。
センサーテスト	センサー - IPSLA テスト失敗	複数のセンサーが IPSLA テスト失敗を報告しています。
センサーテスト	センサー - IPSLA 非対応プローブタイプ	複数のセンサーが IPSLA テスト非対応プローブタイプを報告しています。
センサーテスト	センサー - メールサーバーのテスト失敗	複数のセンサーがメールサーバーに接続できなかったことを報告しています。
センサーテスト	センサー - メールサーバーに到達不能	複数のセンサーがメールサーバーに到達できないことを報告しています。
センサーテスト	センサー - NDT サーバーなし	複数のセンサーが速度テスト NDT サーバーが存在しないことを報告しています。
センサーテスト	センサー - オンボーディングの障害	センサーがワイヤレスネットワークに接続できませんでした。

センサーの問題		
カテゴリ	問題の名称	概要
センサーテスト	センサー - Outlook サーバーのテスト失敗	複数のセンサーが Outlook Web アクセスに接続できなかったことを報告しています。
センサーテスト	センサー - Outlook サーバーに到達不能	複数のセンサーが Outlook Web アクセスホストに到達できないことを報告しています。
センサーテスト	センサー - クエリサーバーのタイムアウト	複数のセンサーが速度テスト対象クエリサーバーのタイムアウトを報告しています。
センサーテスト	センサー - RADIUS 認証の失敗	複数のセンサーが RADIUS サーバーでの認証に失敗したことを報告しています。
センサーテスト	センサー - 速度テスト失敗	複数のセンサーが速度テスト失敗を報告しています。
センサーテスト	センサー - 速度テストの一般的なエラー	複数のセンサーが速度テストの一般的な障害を報告しています。
センサーテスト	センサー - 速度テストのアップリンクタイムアウト	複数のセンサーが速度テストでのアップリンクテストのタイムアウトを報告しています。
センサーテスト	センサー - 速度テスト URL エラー	クエリサーバーへのアクセス中、複数のセンサーが速度テスト URL エラーを報告しています。
センサーテスト	センサー - 到達不能なホスト	複数のセンサーがホストへの ping の失敗を報告しています。ホストに到達できません。
センサーテスト	センサー - 到達不能な RADIUS	複数のセンサーが RADIUS サーバーに到達できないことを報告しています。
センサーテスト	センサー - Web 認証の失敗	複数のセンサーが、クライアントが Web 認証テストに失敗していることを報告しています。
センサーテスト	センサー - Web サーバーのテスト失敗	複数のセンサーが Web サーバーからページをロードできなかったことを報告しています。
センサーテスト	センサー - Web サーバーに到達不能	複数のセンサーが Web サーバーに到達できないことを報告しています。
センサーテスト	センサー - Web ソケットエラー	複数のセンサーがテスト中に速度テスト websocket エラーを報告しています。
センサーテスト	センサー - 速度テストのアップリンクプロキシエラー	複数のセンサーが速度テストのアップリンクテストでプロキシエラーを報告しています。

AI 駆動型の問題

Cisco AI Network Analytics によって検出される AI 駆動型の問題を次の表に示します。

AI 駆動型の問題		
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	ネットワークで、通常と比較して過剰なオンボーディングエラーが発生しています。クライアントは、*SSID* に接続するのに通常より時間がかかっています。
オンボーディング	AI 過剰なワイヤレスクライアントの接続時間 - 基準を上回る合計時間	ワイヤレスクライアントが、*location* にある *SSID* への接続に時間がかかりました。
AAA	AI 過剰な関連付け時間 - 基準から大きく乖離	過剰な関連付け時間 - *SSID* での時間が少なくとも *value*% 増加しています。
AAA	AI 過剰な関連付け障害回数 - 基準から大きく乖離	過剰な関連付け障害回数 - *SSID* での障害回数が少なくとも *value*% 増加しています。
AAA	AI 過剰な認証時間 - 基準から大きく乖離	過剰な認証時間 - *SSID* での時間が少なくとも *value*% 増加しています。
AAA	AI 過剰な認証障害回数 - 基準から大きく乖離	過剰な認証障害回数 - *SSID* での障害回数が少なくとも *value*% 増加しています。
DHCP	AI IPアドレスの取得にかかる過剰な時間 - 基準から大きく乖離	IP アドレスを取得するための過剰な時間 - *server_IP*からの取得時間が少なくとも *value*% 増加しています。
DHCP	AI 過剰なIPアドレス取得失敗回数 - 基準から大きく乖離	過剰なIPアドレス取得失敗回数 - *server_IP* での障害回数が少なくとも *value*% 増加しています。
ネットワークの接続性に関する問題		
接続性	AI ネットワークデバイスでホストMACアドレスのフラッピングが発生	ネットワークでレイヤ 2 のループ症状が発生しています。
ローミングの問題		
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。

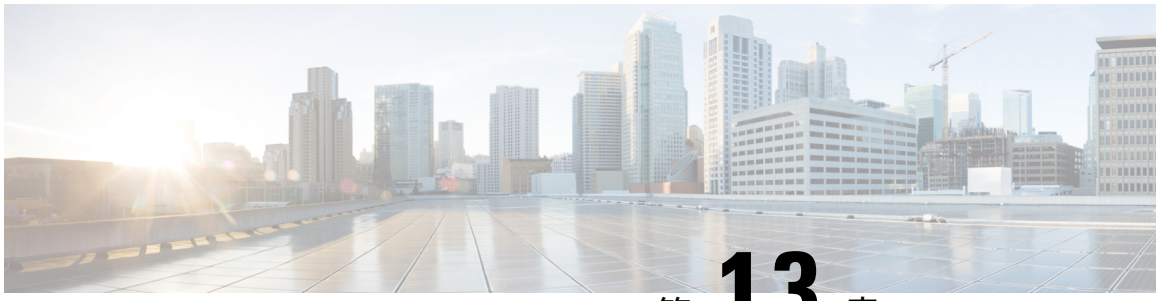
AI 駆動型の問題		
オンボーディング	AI ローミング時間の超過障害 - 基準から大きく乖離	通常と比較して、ネットワークでのローミング時間がかなり長くなっています。
アプリケーション エクスペリエンスの問題		
スループット	AI すべてのアプリケーションの合計無線スループットの低下	ネットワーク内の AP で、すべてのアプリケーションの合計無線スループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。
スループット	AI クラウドアプリケーションの無線スループットの低下	ネットワーク内の AP で、クラウド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。
スループット	AI Colab アプリケーションの無線スループットの低下	ネットワーク内の AP で Colab アプリケーションのスループットが低下しています。これらの無線は *frequency* 帯域内にあります。これらの無線は *location* にあります。

MRE の問題

MRE ワークフローを使用してトラブルシューティング可能な、Assurance で検出される問題を次の表に示します。

MRE の問題		
カテゴリ	**問題の名称**	**概要**
有線クライアントの問題		
オンボーディング	クライアントの DHCP 到達可能性の問題	クライアントが DHCP サーバーから IPv4 アドレスを取得できませんでした。
オンボーディング	有線クライアント認証エラー - Dot1.x エラー	Dot1.x の問題が原因で、有線クライアントの認証に失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。

MRE の問題		
カテゴリ	**問題の名称**	**概要**
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	MAC 認証バイパスの問題が原因で、有線クライアントの認証に失敗しました。 （注） この問題は、単独の有線クライアントにのみ適用されます。
PoE の問題		
デバイス	PoE 受電デバイスに障害フラグあり	PoE ポートに接続された PoE 対応デバイスに障害があると Syslog イベントにフラグが付きました。



第 13 章

イベントの表示と管理

- イベントダッシュボードの概要 （365 ページ）
- デバイスイベントの表示 （366 ページ）
- エンドポイントイベントの表示 （369 ページ）
- イベント分析ダッシュボードの表示, on page 375

イベントダッシュボードの概要

[Events] ダッシュボードは、デバイス（ルータ、スイッチ、ワイヤレスコントローラ、AP、サードパーティ製デバイス）およびエンドポイント（有線および無線）に対するイベントのコンテキストビューを提供します。イベントに関連する他のデバイスに接続されているデバイスによってトリガーされたイベントを検索する代わりに、Assurance がこれらの詳細を提供します。

デフォルトでは、**イベント**ダッシュボードにはタイムラインチャートとリストビューが表示されます。

タイムラインチャートは、一定期間に発生したデバイスタイプ別のイベント数を色で表現します。

リストビューには、イベントのテーブルが表示されます。最大 10,000 のイベントが表示できますが、それ以上のイベントがログに記録されている場合があります。最大 5000 件のイベントを CSV ファイルにエクスポートできます。5,000 を超えるイベントがある場合、それらのイベントをエクスポートすることはできません。「5,000 を超えるイベントがある場合、デバイスファミリフィルタの複数選択はサポートされません」という警告メッセージが GUI に表示されます。

リストビューからイベントをクリックして、接続されたデバイスによってトリガーされたイベントなどの詳細を表示できます。イベントの時間の範囲は、15 分刻みで最大 1 時間（+/- 15 分、+/- 30 分、+/- 45 分、+/- 1 時間）設定できます。

複数のイベントを選択すると、イベントの詳細を含む複数のカードを表示できます。複数のイベントカードが表示されている場合、カードを最小化、最大化、および閉じることができます。たとえば、あるイベントについて接続デバイスイベントテーブルを表示するには、そのイベントカードを最大化します。複数のカードビューに戻るには、 カードを最小化します。

デバイスイベントの表示

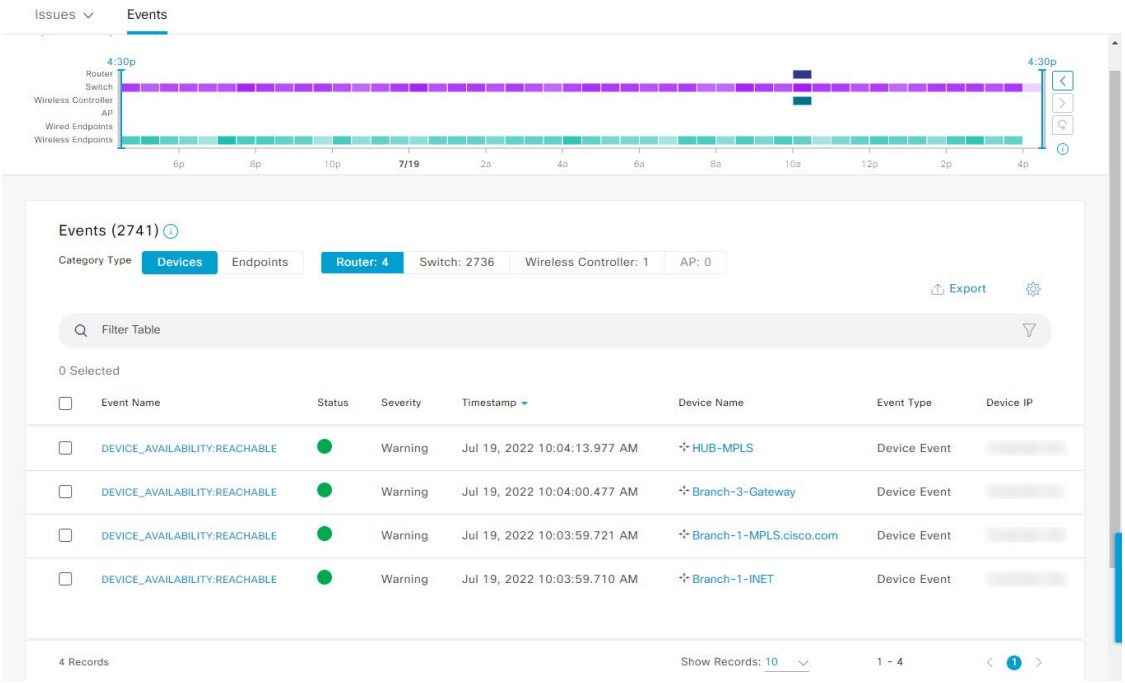
次の手順を使用すると、ルータ、スイッチ、ワイヤレスコントローラ、および AP によって生成されたイベントが表示されます。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

デフォルトで [Category Type] として [Device] が選択された状態で [Events] ダッシュボードが開きます。

図 *41 : [Device Events]* ダッシュボード



[Device Events] ダッシュボード	
アイテム	説明
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックして [Site Details] を選択すると、各サイトのイベントカウントが表示されます。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのイベントのみが表示されます。
24 Hours [Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [プリセット（Presets）] を選択した場合は、[現在（CURRENT）] 列（[今日（Today）]、[週（Week）]、または [月（Month）]）または [最後（LAST）] 列（24 時間、7 日、14 日、30 日、または 60 日）から選択できます。 **3.** [Start Date] と時刻、[End Date] と時刻を指定します。 **4.** [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。 色は、デバイスの種類を表します。 ：ルータ ：スイッチ ：ワイヤレスコントローラ ：AP ：サードパーティ製デバイス 色の明度は重要性（そのデバイスで発生したイベント数の多寡）を示します。たとえば、薄い青色は、濃い青色よりもルーターのイベントが少ないことを示します。
Total Events	特定の時間範囲におけるすべてのデバイスタイプのイベントの総数。

ステップ 2 [Events] の [Category Type]で、[Router]、[Switch]、[Wireless Controller]、[AP]、[Third Party Device] のいずれかのタブをクリックすると、そのデバイスタイプのイベントの一覧がテーブルに表示されます。

[Events] テーブル	
アイテム	**説明**
[Filter Table] オプション	上部にある [Filter Table] バーを使用すると、テーブル内で検索を行うことができます。 • [Match All]：指定された**すべての**条件を満たすイベントのみが表示されます。 • [Match Any]：指定された条件のいずれかに一致するイベントが表示されます。 • [Column Name] ドロップダウンで、フィルタ処理する特定の属性（シビラティ（重大度）、タイムスタンプ、デバイス名、イベントタイプ、デバイス IP など）を選択します。 • [Operator] ではフィルタのロジックを定義します。 • [Equals]：完全一致 • [Not Equals]：指定された値を除外します • [Contains]：指定された文字列を含む任意の値と一致します • [Value input]：検索する特定のテキストまたは ID を入力します赤いアスタリスク（*）が付いているフィールドは必須です。 • 条件の行をさらに追加するには、フィルタ行の右側にある [+] アイコンをクリックします。そうすると、複雑な多階層のトラブルシューティング（特定の [Switch] での特定の [Event Type] のフィルタ処理）が可能になります。
Event Name	イベントの名前。 イベント名をクリックすると、イベントの詳細が表示されたスライドインペインが開きます。 （注） Syslog イベントの場合は、スライドインペイン 内の [Create an Issue]リンクをクリックして [Confirm] をクリックすると表示される [User Defined Issue] ページで、問題を直接作成します。 Intel デバイスと関連付けられているイベントには、タグでラベル付けされています。
Status	デバイスのステータスです。 色はイベントの重大度を表します。 ●：エラー。 ●：警告。 ●：情報。 ●：使用できるデータがありません。

[Events] テーブル	
アイテム	説明
Severity	イベントの重大度：Critical 以上（Emergency および Alert）と、Critical レベルよりも低い重大度（Error、Warning、Notice、Info）。
Timestamp	イベントが発生した日付と時刻。
Device Name	イベントの影響を受けたデバイス名。 デバイス名をクリックして、[Device 360] ウィンドウを開きます。
Event Type	イベントのカテゴリ: Syslog、トラップ、イベント、または AP イベント。
Device IP	デバイスの IP アドレス。

ステップ 3 複数のイベントを表示するには、表示する各イベントの横にあるチェックボックスをオンにして、[Show Selected Events] をクリックします。

[Multiple Events] スライドインペインが開き、各イベントが個別のカードに表示されます。

カード内では次の操作を行うことができます。

- カードを最小化、最大化、および閉じます。
- 下矢印をクリックして詳細を表示します。
- ハイパーリンクをクリックして、それぞれの [Device 360] ウィンドウを起動します。

カードを最大化すると、接続されているデバイスのすべてのイベントが表示されます。

ステップ 4 [Multiple Events] スライドインペインで、リストビューアイコン をクリックすると、リスト内のすべてのサブイベントを集めたものが順番に表示されます。

カードビューに戻るには、カードビューアイコン をクリックします。

エンドポイントイベントの表示

この手順を使用して、有線およびワイヤレスエンドポイントによって生成されたイベントを表示します。

手順

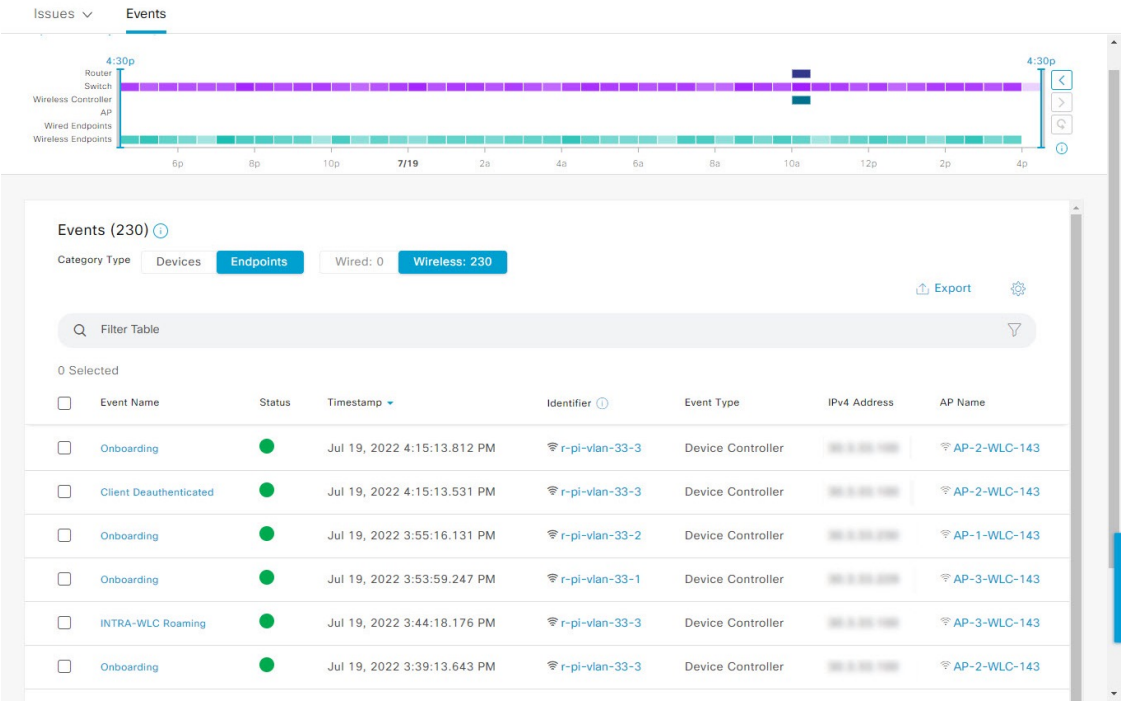
ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

ステップ 2 [Events] タブをクリックします。

[Events] ダッシュボードが開きます。

ステップ 3 [Category Type] で、[Endpoints] タブをクリックします。

図 *42 : [Endpoint Events]* ダッシュボード



[Device Events] ダッシュボード	
アイテム	**説明**
Global	• 上部のメニューバーで Global をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある をクリックして [Site Details] を選択すると、各サイトのイベントカウントが表示されます。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の をクリックすると、そのロケーションのイベントのみが表示されます。

[Device Events] ダッシュボード	
アイテム	説明
 [Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。次の手順を実行します。 **1.** [24 Hours] ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
Timeline Slider	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、エンドポイントの種類を表します。 ：有線 ：ワイヤレス 色の明度は重要性（そのデバイスで発生したイベント数の多寡）を示します。たとえば、薄い紫色は、濃い紫色よりもエンドポイントのイベントが少ないことを示します。
Total Events	特定の時間範囲におけるすべてのエンドポイントタイプのイベントの総数。

ステップ 4 [Wired] または [Wireless] タブをクリックして、テーブル内のそのエンドポイントタイプのイベントのリストを表示します。

[Events] テーブル	
アイテム	説明
[Filter Table] オプション	上部にある [Filter Table] バーを使用すると、テーブル内で検索を行うことができます。 • [Match All]：指定された**すべての**条件を満たすイベントのみが表示されます。 • [Match Any]：指定された条件のいずれかに一致するイベントが表示されます。 • [Column Name] ドロップダウンで、フィルタ処理の対象とする特定の属性を選択します。 • [Operator] ではフィルタのロジックを定義します。 • [Equals]：完全一致 • [Not Equals]：指定された値を除外します • [Contains]：指定された文字列を含む任意の値と一致します • [Value input]：検索する特定のテキストまたは ID を入力します赤いアスタリスク（*）が付いているフィールドは必須です。 • 条件の行をさらに追加するには、フィルタ行の右側にある [+] アイコンをクリックします。そうすると、複雑な多階層のトラブルシューティング（特定のエンドポイントでの特定のイベントタイプのフィルタ処理）が可能になります。
Event Name	イベントの名前。 イベント名をクリックすると、その詳細が表示されたスライドインペインが開きます。
Status（有線エンドポイントのみ）	色はイベントの重大度を表します。 ●：エラー。 ●：警告。 ●：情報。 ●：使用できるデータがありません。
Severity（有線エンドポイントのみ）	イベントのシビラティ（重大度）です。重大度は、Critical 以上（Emergency、Alert）、およびこれより低い重大度（Error、Warning、Notice、Info）の場合があります。
Timestamp	イベントが発生した日付と時刻。
[Identifier]	エンドポイントの識別子。これは、その順序での可用性に応じて、ユーザーID、ホスト名、IP アドレス、MAC アドレスのいずれかになります。 識別子をクリックすると、その詳細が表示されたスライドインペインが開きます。
イベント タイプ	イベントのカテゴリ: Syslog、トラップ、イベント、または AP イベント。

[Events] テーブル	
アイテム	説明
IPv4 アドレス（IPv4 Address）	エンドポイントに接続されているデバイスの IPv4 アドレス。
AP Name（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されている AP の名前。 AP 名をクリックして、[Device 360] ウィンドウを開きます。
Switch（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチの名前。 スイッチ名をクリックして、[Device 360] ウィンドウを開きます。
[MAC Address]	エンドポイントに接続されているデバイスの MAC アドレス。
Port（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチポート。
VLAN ID（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチポートの VLAN ID。
Switch IP Address（有線エンドポイントのみ）	有線エンドポイントに接続されているスイッチの IP アドレス。
AP MAC（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されている AP の MAC アドレス。
SSID（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している SSID。
UserID（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントのユーザー ID。
Wireless Controller Name（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントに接続されているワイヤレスコントローラの名前。
Band（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している無線帯域。
DHCP Server（ワイヤレスエンドポイントのみ）	ワイヤレスエンドポイントが使用している DHCP サーバー。

ステップ 5 イベント名をクリックすると、そのイベントに関する詳細情報が スライドインペイン に表示されます。

スライドインペインには、基本情報（識別子やシビラティ（重大度）など）、ハイパーリンク付きのデータ、および接続済みデバイスイベントの詳細が表示されます。

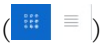
（注） ワイヤレスエンドポイントで AAA 管理に Cisco ISE が使用されている場合、Catalyst Center は Cisco ISE から Cisco ISE 認証イベントの詳細を取得し、それを [ISE Authentication] イベントに表示します。イベント スライドインペイン では、[Show ISE Events] をクリックすると、AAA サーバーによって完了された Cisco ISE 認証手順が表示されます。

[Connected Device Events] ダッシュレットでは、[Show Events]をクリックすると、最大 10,000 件の接続済みデバイスイベントがテーブルに表示されます。このダッシュレットでは、イベントデータをフィルタ処理またはエクスポートすることができます。

- ダッシュレットの右上隅にある [+_15 mins] ドロップダウンリストでタイムフレームを選択すると、そのタイムフレーム内で発生したすべてのイベントが表示されます。
- [Switch] や [AP] などのデバイスタブをクリックすると、そのデバイスに接続されているイベントが表示されます。
- テーブルの右上隅にある [Export] をクリックすると、テーブルから最大 5,000 件のイベントが CSV ファイルとしてエクスポートされます。
- 右上隅にある歯車アイコンをクリックすると、テーブルビューの設定をカスタマイズできます。
- テーブル検索バーを使用すると、テーブルで特定のデータをフィルタ処理できます。

ステップ 6 複数のイベントを表示するには、表示する各イベントの横にあるチェックボックスをオンにして、[Show Selected Events] をクリックします。

[Multiple Events] スライドインペインでは、デフォルトのカードビューで各イベントが個別のカードに表示されます。

[Multiple Events] スライドインペインでは、ビュースイッチャー（  ）を使用してビューを変更できます。

カードの中から、次のことができます。

- カードを最小化、最大化、および閉じる
- 下矢印をクリックして詳細を表示する
- ハイパーリンクされたデータをクリックします。

カードを最大化すると、接続されているデバイスのイベントがすべて表示されます。

イベント分析ダッシュボードの表示

[イベント分析（Events Analytics）] ダッシュボードでは、syslog メッセージおよびさまざまなタイプのネットワークイベントが可視化されるため、さまざまなデータソース間でトレンドを特定し、イベントを関連付けることができます。

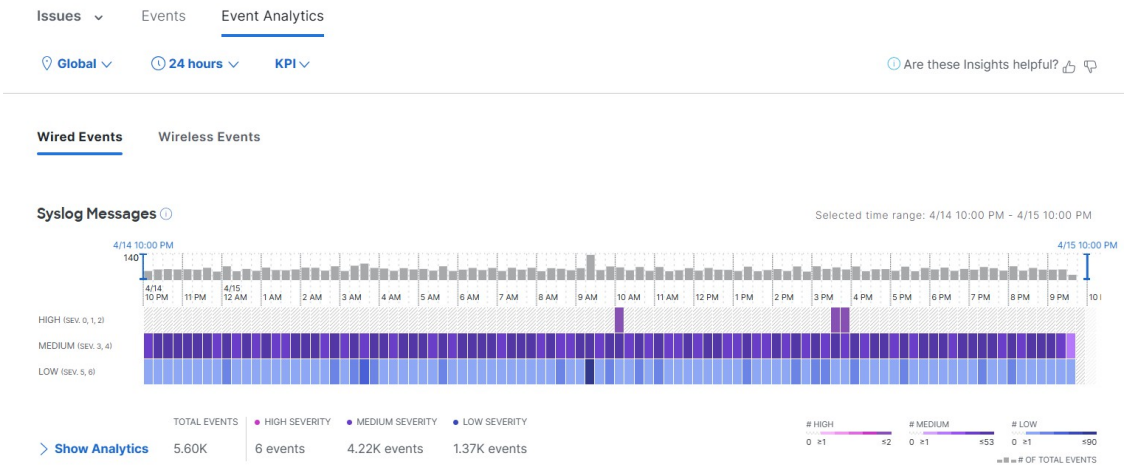
この手順を使用して、syslog メッセージの数と有線およびワイヤレス ネットワーク イベントの到達可能性の遷移を表示するヒートマップとして表される分析とインサイトを表示します。

Procedure

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboards]** > **[Issues and Events]** の順に選択します。

ステップ 2 [イベント分析（Event Analytics）] タブをクリックします。[Event Analytics] ダッシュボードが開き、有線イベントが表示されます。

Figure 43: イベント分析ダッシュボード



イベント分析ダッシュボード	
アイテム	説明
Global	上部のメニューバーでこのアイコンをクリックして、[ロケーションを選択（Select a location）] スライドインペインからサイト階層内のサイト、建物、またはフロアを選択します。

イベント分析ダッシュボード	
アイテム	説明
24 Hours [Time Range] の設定	選択した時間範囲に基づく情報をウィンドウに表示できます。デフォルトは [24 Hours] です。タイムラインの範囲を設定するには、次の手順を実行します。 **a.** [24 Hours] ドロップダウンリストで、時間範囲（[3 hours]、[24 Hours]、または [7 days]）を選択します。 **b.** [プリセット（Presets）] を選択した場合は、[現在（CURRENT）] 列（[今日（Today）]、[週（Week）]、または [月（Month）]）または [最後（LAST）] 列（24 時間、7 日、14 日、30 日、または 60 日）から選択できます。 **c.** [Start Date] と時刻、[End Date] と時刻を指定します。 **d.** [Apply] をクリックします。
KPI	このドロップダウンをクリックして、有線デバイスまたはワイヤレスデバイスについて、Syslog メッセージ、到達可能性の遷移、クライアント オンボーディング、無線イベントなど、特定のイベントカテゴリの可視性を切り替えます。

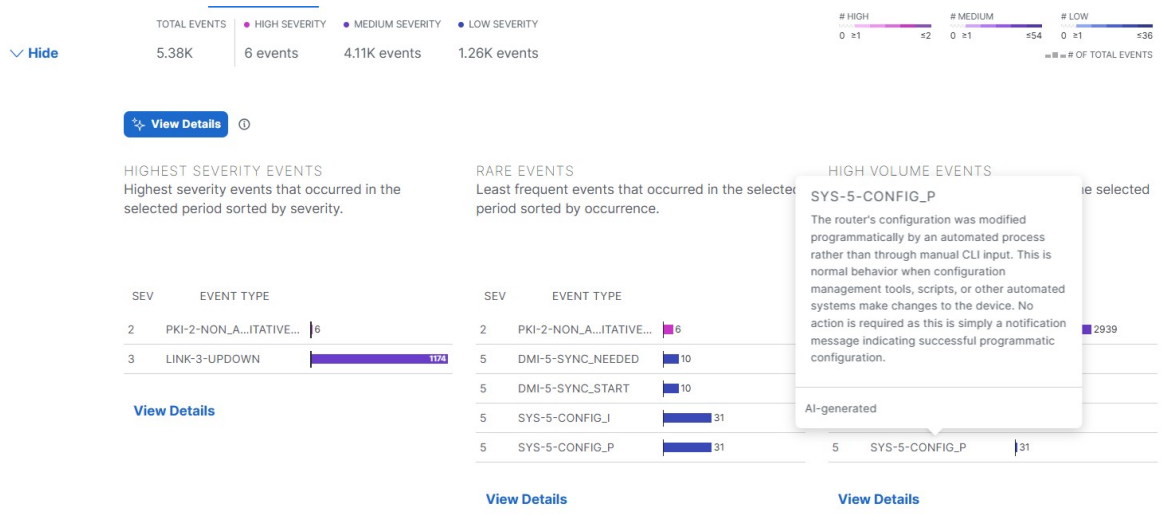
ステップ 3 [有線イベント（Wired Events）] をクリックして、有線デバイスからの syslog メッセージと到達可能性の遷移の数を表示するヒートマップを表示します。ヒートマップには、最大 24 時間における 15 分単位のメッセージ重大度データの内訳が含まれます。7 日の場合、粒度は 4 時間です。14 日と 30 日の場合、粒度は 12 時間です。60 日の場合、粒度は 24 時間です。

Syslog メッセージ：

- ヒートマップの上部にあるタイムスライダを使用して、syslog メッセージヒートマップの特定の期間を設定します。イベントの合計数と、メッセージ重大度（高、中、低）の数が表示されます。
- インサイトと分析データの syslog メッセージを表示するには、[Show Analytics] をクリックします。さまざまな可視化を備えた一連のカードには、さまざまな分析基準に基づいた順序で、syslog メッセージまたはデバイスの数が表示されます。Syslog メッセージは次の分析に対応しています。
  - 重大度が最も高いイベント：選択した期間に発生した重大度が最も高いイベントです（重大度別）。
  - 頻度の低いイベント：選択した期間に発生した最も頻度の低いイベントです（発生回数別）。
  - 大量のイベント：選択した期間に発生した最も頻度の高いイベントです（発生回数別）。
  - メッセージ量の増加：選択した期間内で増加量が最も高いイベントです（変動量別）。
  - メッセージ量の減少：選択した期間内で減少量が最も高いイベントです（変動量別）。
  - 新規イベント：選択した期間の終わりの時点で発生が開始されていたイベントです（発生回数別）。
  - 最もアクティブなデバイス：選択した期間に最も多くのイベントを生成したデバイスです（生成量別）。

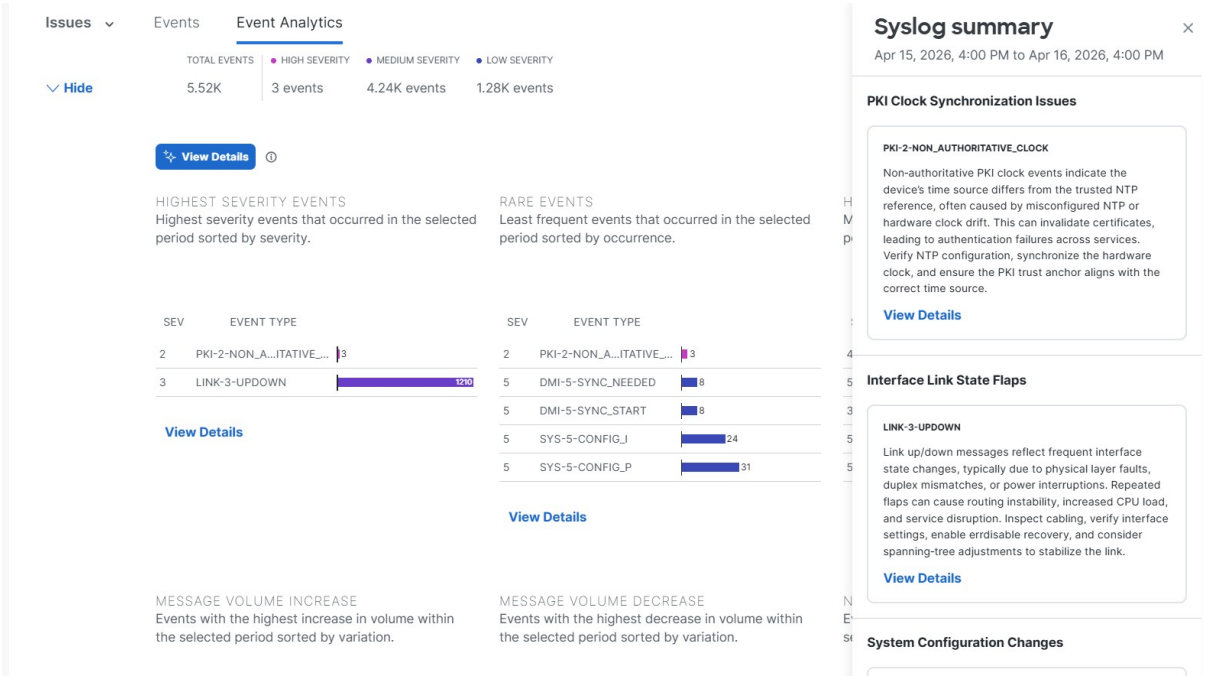
特定のsyslogの目的をすばやく理解するには、ニーモニックの上にカーソルを合わせます。ツールチップには、イベントについての簡単な説明が表示され、イベントをさらに調査するか無視するかについてのガイダンスが示されます。

***Figure 44: Syslog* メッセージの分析**



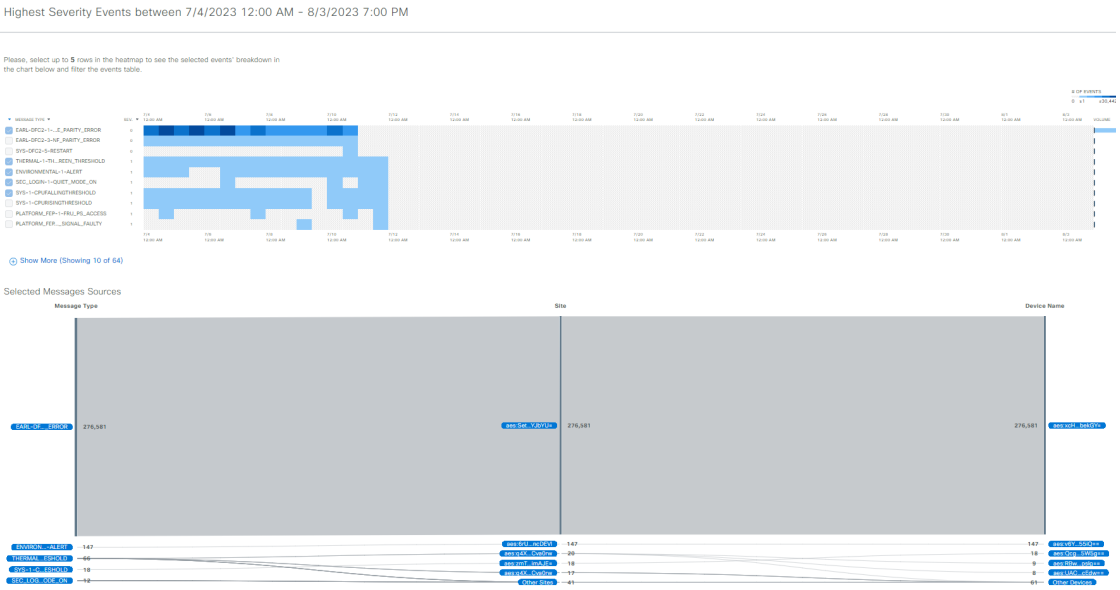
- View Details をクリックすると、生の syslog データを実用的な洞察に変換する AI syslog の自動要約と説明が表示されます。

***Figure 45: AI syslog* の自動要約と説明**



- [View Details] をクリックして、各イベントタイプのイベント数に関する時系列の詳細なヒートマップを表示します。ヒートマップで最大 5 つの syslog メッセージタイプを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。

***Figure 46: Sankey* グラフを使用した *Syslog* イベントのヒートマップ**



- Sankey チャートでメッセージタイプ、サイト、またはデバイスを選択して、チャートの下にあるイベントテーブルをフィルタ処理できます。イベントテーブルには、最大 10,000 のイベントを表示できます。ユーザー定義の問題を作成するには、イベントテーブルの [messages] をクリックし、[Confirm] をクリックします。

到達可能性の遷移：

- ヒートマップの上部にあるタイムスライダを使用して特定の期間を設定し、イベント、到達不能イベント、到達可能イベント、および ping 到達可能イベントの合計数を表示します。
- 別のカードに表示される有線デバイスからの各到達可能性の遷移（上位ステータス遷移、イベント別上位デバイス）のインサイトと分析データを表示するには、[Show Analytics] をクリックします。
- [View Details] をクリックして、各イベントタイプのイベント数に関する時系列の詳細なヒートマップを表示します。ヒートマップで最大 5 つのイベントを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトとデバイス生成イベントについて学習できます。
- Sankey グラフで from イベント、to イベント、サイト、またはデバイスを選択して、イベントテーブルをフィルタ処理し、各イベントの到達可能性の遷移を表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

ステップ 4 [Wired Events] をクリックして、ワイヤレスデバイスからの syslog メッセージと到達可能性の遷移の数を表示するヒートマップを表示します。ヒートマップには、15 分単位のメッセージ重大度データの内訳が含まれます。

Syslog メッセージ：

- ヒートマップの上部にあるタイムスライダを使用して、syslog メッセージヒートマップの特定の期間を設定します。イベントの合計数と、メッセージ重大度（高、中、低）の数が表示されます。
- 別のカードに表示される各 syslog メッセージのインサイトと分析データを表示するには、[Show Analytics] をクリックします。使用可能な syslog メッセージの分析カードが、重大度とイベントタイプとともに表示されます。syslog メッセージのニーモニックにカーソルを合わせると、イベントの簡単な説明が記載されたツールチップが表示されます。

  View Details をクリックすると、生の syslog データを実用的な洞察に変換する AI syslog の自動要約と説明が表示されます。
- [View Details] をクリックして、各イベントタイプのイベント数に関する時系列の詳細なヒートマップを表示します。ヒートマップで最大 5 つの syslog メッセージタイプを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトおよびデバイス生成イベントについて学習できます。
- Sankey グラフでメッセージタイプ、サイト、またはデバイスを選択し、イベントテーブルをフィルタ処理して syslog メッセージを表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

到達可能性の遷移：

- ヒートマップの上部にあるタイムスライダを使用して特定の期間を設定し、イベント、到達不能イベント、到達可能イベント、および ping 到達可能イベントの合計数を表示します。
- 別のカードに表示されるワイヤレスデバイスからの各到達可能性の遷移（上位ステータス遷移、イベント別上位デバイス）のインサイトと分析データを表示するには、[Show Analytics] をクリックします。
- [View Details] をクリックして、各イベントタイプのイベント数に関する時系列の詳細なヒートマップを表示します。ヒートマップで最大 5 つのイベントを選択して Sankey チャートをフィルタ処理し、選択したイベントタイプの分布を表示して、特定のサイトとデバイス生成イベントについて学習できます。
- Sankey グラフで from イベント、to イベント、サイト、またはデバイスを選択して、イベントテーブルをフィルタ処理し、各イベントの到達可能性の遷移を表示できます。イベントテーブルには、最大 10,000 のイベントを表示できます。

ステップ 5 Sankey グラフの下にあるイベントテーブルで、個々のログの AI Insight をクリックすると、生の syslog データが実用的な洞察に変換されます。次のような AI 生成の応答を確認すると、詳細な分析に役立ちます。

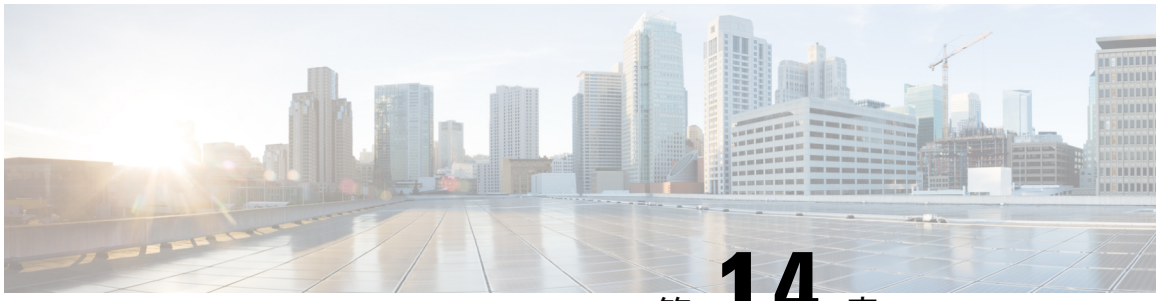
- サマリー：AI は、最も影響の大きいメッセージと傾向を示す、syslog アクティビティの簡潔なサマリーを生成します。

- 影響：ネットワークに対するイベントの潜在的な影響。アシュアランスは、ネットワークデバイスから syslog メッセージを継続的に収集します（syslog データは 3 か月保持されます）。
- 原因：イベントが発生した理由の分析。
- 修復：アシュアランスは、OpenAI モデルに組み込まれたシスコの広範なネットワークの専門知識に基づき、問題を効率的に解決するための提案を提供します。



Note AI syslog の自動要約とツールチップを無効にするには、**[システム（System）] > [設定（Settings）] > [外部サービス（External Services）] > [Cisco AI Analytics]** の順に選択します。[AI Network Analyticsの有効化（Enable AI Network Analytics）] トグルボタンをオフにして、[更新（Update）] をクリックします。この操作によって、Catalyst Center 展開での AI 分析用の収集が無効になります。

AI インサイトを無効にするには、**[システム（System）] > [設定（Settings）] > [外部サービス（External Services）] > [Cisco AI Analytics]** の順に選択します。[匿名化されないSyslogメッセージテキストのエクスポートの有効化（Enable Non-anonymized Syslog Message Text Export）] トグルボタンをオフにして、[更新（Update）] をクリックします。



第 14 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 （381 ページ）
- センサーのプロビジョニング （382 ページ）
- センサーを使用したネットワーク正常性のモニターとトラブルシューティング （388 ページ）
- センサーとバックホール設定の管理 （396 ページ）
- SCEP プロファイルの管理 （401 ページ）
- センサー主導テスト （402 ページ）

センサーとセンサー主導のテストについて

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

Assurance では専用センサー（センサー機能を実行するための専用ハードウェア）がサポートされています。

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、Assurance サーバーの到達可能性の詳細を取得すると、Assurance サーバーと直接通信します。

センサーのプロビジョニング

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

手順

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 `CiscoProvisioningSSID` を有効にする必要があります。

（注） ソフトウェアリリース 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサーデバイスプロファイル **`CiscoProvisioningSSID`** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。バックホール設定の管理 （398 ページ）を参照してください。

シスコ 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（382 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プロビジョニング SSID の有効化 （383 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。

『バックホール設定の管理 （398 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。

を参照してくださいAP またはセンサーデバイスのプロビジョニング （384 ページ）。

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 Catalyst Center User Guide* 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

手順

ステップ 1 シスコ 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 Catalyst 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プロビジョニング SSID の有効化

手順

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

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

[Cloud Services] ページが表示されます。

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

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

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

ステップ 5 [Apply] をクリックします。

プロビジョニングを有効化すると、[CiscoSensorProvisioning] という非表示の WLAN が作成されます。

ウィンドウの右下隅に、次のエラーメッセージが表示されます。

```
Error in Configuring
CLI Line 2 Please associate the wlan and policy profile CiscoSensorProvisioning to the desired AP.
```

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

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

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

[Policy Profile] ページが表示されます。

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

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

a) 左側のナビゲーションペインで、**[設定（Configuration）]** > **[タグ（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。

AP またはセンサーデバイスのプロビジョニング

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

Before you begin

- 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、または不明状態になっているネットワークデバイスを使用している場合は、『Network Plug and Play Troubleshooting Guide』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。

- インテントベース ネットワーク内の AP については、ネットワーク階層内でサイトを定義します。ネットワーク階層 （37 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。



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

- 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 Catalyst 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 Catalyst 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 Catalyst Center の仮想 IP アドレスです。

手順

ステップ 1 [プラグアンドプレイ（Plug and Play）] に移動して、必要なデバイスを選択します。

a) メインメニューから次を選択します。**[Provision]** > **[Plug and Play]**。
b) テーブル内のデバイスを表示します。

検索バーを使用して、特定のデバイスを検索できます。

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

ステップ 2 （任意） [Assign Site] ウィンドウで、次の手順を実行します。

a) 必要に応じてデバイスのホスト名を変更します。
b) 次のいずれかのタスクを実行して、サイトを割り当てます。

- 各デバイスに異なるサイトを割り当てるには、[Assign] をクリックし、[Select a Site] ドロップダウンリストからサイトを選択します。
- 最初のデバイスと同じサイトを他のすべてのデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Site to All] を選択します。
- あるデバイスのサイトを別のデバイスに割り当てるには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。
- デバイスに割り当てられたサイトをクリアするには、[Clear Site] をクリックします。

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

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

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

詳細については、『*Cisco Catalyst Center* 管理者ガイド』の「PnP 導入準備用の AP ロケーションの設定」を参照してください。

c) [Next] をクリックします。

ステップ 3 [Assign Configuration] ウィンドウで、次の手順を実行します。

a) [Configuration] 列で、設定するデバイスの [Assign] をクリックします。

b) デバイス構成を変更する必要がない場合は、[Cancel] をクリックして、次の手順に進みます。それ以外の場合は、次のいずれかの設定を変更または設定します。

- [Device Name]：必要に応じてデバイスのホスト名を変更します。
- [Template]：このドロップダウンリストで、デバイスに適用するオンボーディング設定テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

（注） デバイスをサイトに割り当てていない場合は、デバイスのテンプレートを選択する必要があります。選択するテンプレートには、デバイスにグローバル デバイスログイン情報を設定するために必要な CLI コマンドを含める必要があります。それ以外の場合、デバイスは管理対象外の状態で一覧に追加されます。

- AP の場合、[APゾーン（AP Zone）] ドロップダウンリストから AP ゾーンを選択します。[RFプロファイル（RF Profile）] は自動的に入力され、SSID 数は選択した AP ゾーンに基づいて表示されます。デフォルトの AP ゾーンを選択する場合は、RF プロファイルを選択します。
- AP の場合、[無線周波数プロファイル（Radio Frequency Profile）] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1 つのプロファイルをデフォルトとして指定した場合に設定できます。

- センサーの場合、[センサー設定（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（バックホール）を選択します。

（注） 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサー デバイス プロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。

- 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

c) [Clear Configuration] ドロップダウンリストから、次のオプションのいずれかを選択します。

- [Clear Device Certificates]：このオプションを選択し、証明書をクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Images]：このオプションを選択し、イメージをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear Templates]：このオプションを選択し、テンプレートをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。
- [Clear License Levels]：このオプションを選択し、ライセンスレベルをクリアする各デバイスの横にあるチェックボックスをオンにして、[Clear] をクリックします。

d) あるデバイスのイメージまたはテンプレートを他のデバイスに適用するには、[Actions] 列で、省略記号アイコン ••• の上にカーソルを置き、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択します。

e) プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

f) すべてのデバイスを設定したら、[Next] をクリックします。

ステップ 4 [Provision Templates] ウィンドウで、[Devices] エリアからテンプレートを選択し、[Domain] フィールドにドメイン名を入力して、[Next] をクリックします。

（注） デバイスがサイトに割り当てられている場合は、[次へ（Next）] をクリックします。

ステップ 5 [Summary] ウィンドウで、デバイスに関する詳細や構成プレビューを確認できます。

ステップ 6 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 [デバイス設定（Device Configuration）] 列をチェックします。

プレビューにエラーが表示された場合は、表の上にあるエラーメッセージの [アクション（Actions）] リンクをクリックして、実行する必要のあるアクションを確認します。アクションをクリックすると、変更が必要なウィンドウで新しいタブを開くことができます。デバイスを要求する前に問題を解決してプロビジョ

ニングエラーを回避する必要があります。[割り当ての設定（Assign Configuration）] 手順に戻って設定を変更したり、[設計（Design）] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。問題を解決したら、このタブに戻り、[Retrying get Day-0 configuration Preview for failed device(s)] をクリックし、[OK] をクリックします。デバイスを管理するワイヤレスコントローラがインベントリに追加され、デバイスが割り当てられているサイトに割り当てられたことを確認します。

ステップ 7 [Device Configuration] 列で、[Preview Configuration] をクリックして設定を確認します。

ステップ 8 [要求（Claim）] をクリックします。

ステップ 9 確認ダイアログボックスで [Yes] をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

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

次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、『*Cisco Catalyst Center*ユーザーガイド』の「プロビジョニングプロセスの完了」を参照してください。

センサーを使用したネットワーク正常性のモニターとトラブルシューティング

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

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

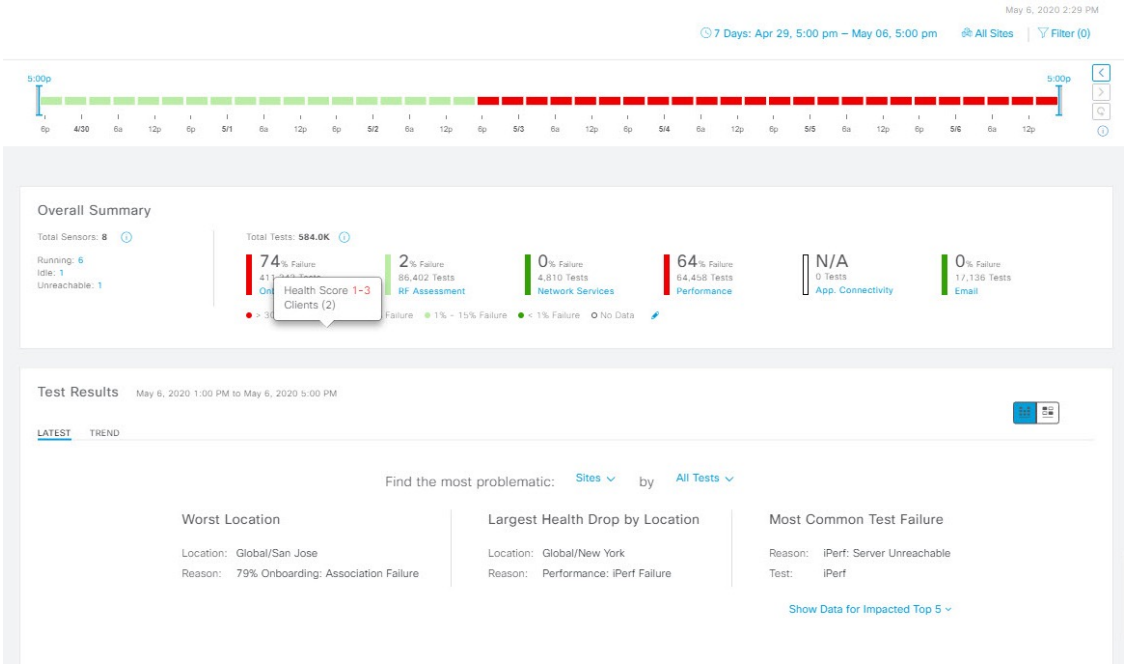
始める前に

センサー主導テストが追加され、スケジュール済みであることを確認してください。テンプレートを使用したセンサー主導テストの作成と実行 （402 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboards]** > **[Wireless Sensors]** の順に選択します。

図 *47 : [Wireless Sensors]* ダッシュボード



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

タイムラインエリア	
アイテム	**説明**
時間範囲の設定	ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 **1.** ドロップダウンメニューで範囲の長さ（[3 Hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。

タイムラインエリア	
アイテム	**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、ネットワーク内の選択した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] アイコン	ダッシュボードに表示するデータを、SSID および無線周波数帯域に基づいて選択できます。 フィルタを追加するには、次の手順を実行します。 1. [Filter] をクリックします。 2. ドロップダウンメニューから [SSID] タブをクリックし、該当する SSID のチェックボックスをオンにします。 3. ドロップダウンメニューから、[Band][タブをクリックし、 [2.4 GHz] または [5 GHz] のオプションボタンを選択します。 4. [Apply] をクリックします。 選択したすべてのフィルタを削除するには、次の手順を実行します。 1. [Filter] アイコンをクリックします。 2. [Clear Filters] をクリックします。

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

時間範囲は、タイムラインの上にある の設定で決まります。

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

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

ブロックは、テストが失敗した割合の重大度を示すために色分けされています。

ブロックの上にマウスカーソルを合わせると、各テストカテゴリごとにテスト失敗率の内訳が表示されます。

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

[Overall Summary] ダッシュレット	
アイテム	**説明**
[Total Sensors] エリア	ネットワーク内のすべてのセンサーとそのステータスの全体像が表示されます。センサーのステータスタイプは次のいずれかです。 • [Idle]：センサーはオンボードされており、スケジュールされたテストはありません。 • [Running]：センサーはオンボードされており、テストスイートまたはテストテンプレートに含まれています。 • [Unreachable]：センサーからハートビートが受信されませんでした。 ステータスタイプの横にあるハイパーリンク番号をクリックすると、スライドインペインが開き。そのステータスのセンサーが表示されます。 スライドインペインで[Name]カラムの下にあるセンサー名をクリックすると、そのセンサーの360度ビューが表示されます。「ワイヤレスセンサーを使用したネットワーク正常性のモニターとトラブルシューティング（394ページ）」を参照してください。

[Overall Summary] ダッシュレット	
アイテム	説明
全体テスト	すべてのセンサーで実行されたテストの合計数と、以下のテストカテゴリに基づくテスト結果の内訳が表示されます。 [Onboarding] **RF アセスメント** **ネットワーク サービス** **パフォーマンス** **App. 接続性** **電子メール** テストカテゴリをクリックすると、そのテスト結果に関する追加の詳細情報が表示されるスライドインペインを開くことができます。 スライドインペインで、左側のテストタイプのタブをクリックすると、そのテストタイプのデータが記載されたスライドインペインが表示されます。スライドインペインには次の情報が表示されます。 • テスト結果、将来のトレンド、およびテストで使用された AP のリストが表示されたチャート。 （注） テストカテゴリが**RF アセスメント**の場合、チャートには、テスト結果ではなく、KPI データレートと SNR が表示されます。 • データタイプのカテゴリ：**上位のエラー理由**（該当する場合）、**上位の AP**、**上位のロケーション**、**上位の帯域**、および**上位の SSID**（該当する場合）。 • テストを実行したセンサーの詳細データが格納されたテーブル。 データタイプカテゴリからデータセグメントをクリックすると、テーブルに表示するデータをフィルタリングできます。
 しきい値の編集	テスト失敗率の重大度を示す色分けされた範囲のしきい値は、カスタマイズできます。 ● > 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. 編集アイコン（  ）をクリックします。 2. [Edit Threshold] メニューで、色分けされた各範囲のフィールドにパーセンテージ値を入力します。 3. [Apply] をクリックします。

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

[Test Results] ダッシュレット	
アイテム	**説明**
[Latest] タブと [Trend] タブ	これらのタブでは、ダッシュレットに表示するデータの範囲を定義します。 • [Latest]：ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。 • [Trend]：過去 24 時間のデータが表示されます。
 [Heatmap View] と [Card View] トグル	このトグルボタンで、ダッシュレットのビューを [Heatmap View] と [Card View] で切り替えることができます。 デフォルトでは、[Heatmap View] が表示されます。
 [Heatmap View]	次の統計カテゴリの上位 5 ランキングがダッシュレットの上部に表示されます。 • [Worst Location, Buildings, Floors] または [Sensors]：テスト失敗率が最も高かったサイト、ビルディング、フロア、またはセンサー。 • [Largest Health Drop by Location, Buildings, Floors] または [Sensors] ：正常性の低下が最も急激なサイト、ビルディング、フロア、センサー。 • [Most Common Test Failure]：テスト失敗率が最も高かったテストタイプ。 各統計情報カテゴリの上位スポットのみが表示されます。[Show Data for Impact Top 5] をクリックすると、完全なランキングが表示されます。 ランキングの下には、センサーテストエラーの結果がヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。 • ランキングやヒートマップに表示するデータをソートするには、[Find the most problematic] エリアのドロップダウンリストを使用します。最初のドロップダウンリストでは、ロケーションまたはセンサー別にデータをソートできます。2番目のドロップリストでは、テストタイプ別にデータをソートできます。 • 特定のロケーションまたはセンサーのヒートマップをフィルタリングするには、検索フィールドを使用します。 • ブロックの上にカーソルを合わせると、テスト失敗の正確なパーセンテージ値が表示されます。 • 色分けされたブロックをクリックすると、スライドインペインが開き、交差する部分のテスト結果に関する詳細が表示されたます。

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

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

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

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboards]** > **[Wireless Sensors]** の順に選択します。

[Sensor Dashboard] が表示されます。

ステップ 2 [Sensors Dashboard] で次のいずれかを行います。

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

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

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

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

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

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

センサーの 360 度ビューが表示されます。

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

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

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

イベントログの表示やダウンロードには、次の手順を実行します。

a) ヘッダーの最後にある [View Logs] をクリックします。
[Event Logs] スライドインペインが現れ、イベントログが表示されます。

b) イベントログの保存先となるサポートバンドルファイルを生成するには、[Event Logs] スライドインペインで、[Request Support Bundle] をクリックします。

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

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

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

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

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

テスト結果カテゴリ
センサーテスト失敗の結果は、テスト対象の AP ごとにヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。 • テストタイプ別にデータをソートするには、[Test Type] ドロップダウンリストを使用します。 • 特定の AP のヒートマップをフィルタ処理するには、検索フィールドを使用します。 • ブロックの上にカーソルを合わせると、テスト失敗の正確なパーセンテージ値が表示されます。 • [Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。   • [Latest]：ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。   • [Trend]：過去 24 時間のデータが表示されます。

センサーパフォーマンスのトレンドカテゴリ
テストタイプに基づいて、センサーのパフォーマンスデータを折れ線グラフまたはチャートで表示します。時間ベースのテストタイプの場合、比較ビューを使用すると、現行センサー、最高パフォーマンスのセンサー、および最悪パフォーマンスのセンサーのパフォーマンスを表示できます。 • 特定のテストタイプのデータを表示するには、[Test Type] ドロップダウンリストを使用します。 • 時間ベースのテストタイプの場合は 、[+ Add Custom Location] をクリックすると、メニューを使用して、特定のロケーションのセンサーパフォーマンスデータを追加できます。サイト、ビルディング、またはフロアのセンサーパフォーマンスを選択できます。

ネイバー AP カテゴリ
センサーのネイバー AP とその RSSI が、リストビューとマップビューで表示されます。 周波数帯域に基づいて AP をフィルタ処理するには、[Band] エリアのオプションボタンを使用します。 （注） センサーは、30 分ごとにネイバー AP をスキャンします。

センサーとバックホール設定の管理

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 を有効にでき、これらのセンサーの名前を変更できます。

始める前に

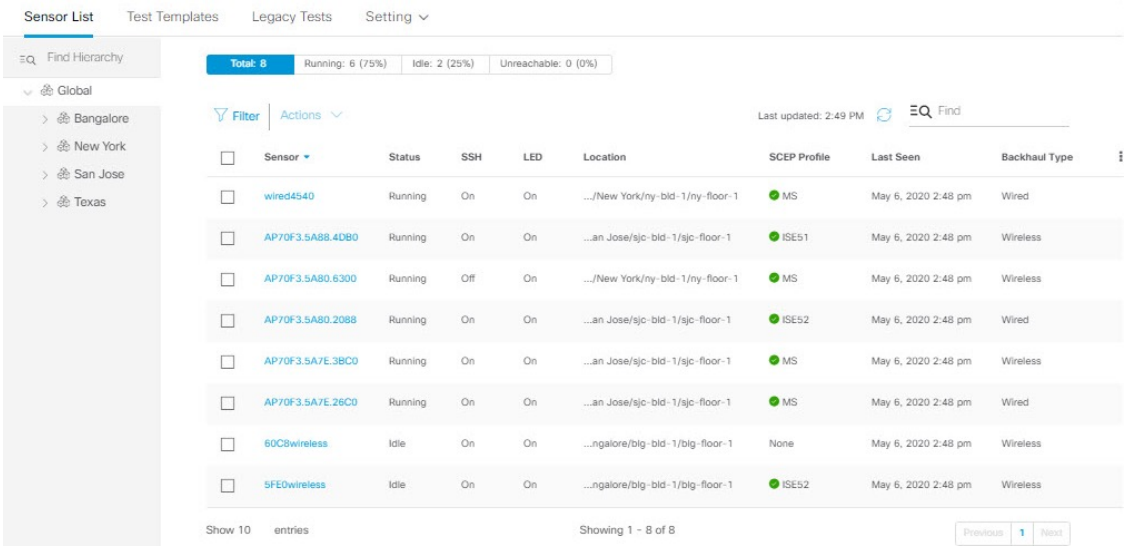
センサーがサイトに割り当てられていることを確認します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Settings]** > **[Sensors]** の順に選択します。

[Sensor List] ウィンドウが表示されます。

図 *48 : [Sensor List]* ウィンドウ



ステップ 2 左側のペインで、表示するネットワーク階層を指定します。

ステップ 3 テーブルの上にあるカテゴリをクリックすると、基準に適合するセンサーが表示されます。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]：オンボード済みであるが、応答していないセンサーが表示されます。

ステップ 4 テーブルに表示するデータをカスタマイズできます。

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

ステップ 5 センサーの SSH 設定を行うには次の手順を実行します。

a) センサーのチェックボックスをオンにします。
b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit SSH] を選択します。

[Edit SSH] スライドインペインが表示されます。

c) [EDIT SSH] スライドインペインで、[SSH] トグルをクリックして SSH を有効にします。
d) [Username] および [Password] フィールドに、使用する SSH ログイン情報を入力します。
e) [Save] をクリックします。

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

a) センサーのチェックボックスをオンにします。
b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit LED] を選択します。

[Edit SSH] スライドインペインが表示されます。

c) [Edit LED] スライドインペインで、 [LED] トグルをクリックして、ステータス LED を有効または無効にします。

ステップ 7 [Save] をクリックします。

ステップ 8 センサーの名前を変更するには、次の手順を実行します。

a) センサーのチェックボックスをオンにします。

b) [Actions] ドロップダウンリストで [Edit Sensor Name(s)] を選択します。

[Edit Sensor Name（s）] スライドインペインが表示されます。

c) [Edit Sensor Name（s）] スライドインペインで、[Name] フィールドに名前を入力します。

d) [Save] をクリックします。

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

a) センサーのチェックボックスをオンにします。

b) [Actions] ドロップダウンリストで [Enroll using SCEP] を選択します。

[Enroll using SCEP] スライドインペインが表示されます。

c) [Select SCEP Profile] ドロップダウンリストで SCEP プロファイルを選択します。

詳細については、「SCEP プロファイルの管理」を参照してください。

d) [Username] と [Password] を選択し、必要な詳細情報を入力します。ユーザー名で [Custom] オプションを選択する場合は、[No Password] を選択します。

e) [Save] をクリックします。

f) ステータスを確認するには、[Sensor List] ウィンドウの [SCEP Profile] 列を確認します。緑のチェックマーク（✔）は成功、赤の [X] アイコンは失敗を表します。✔ または **X** アイコンにカーソルを合わせると、詳しい情報が表示されます。

バックホール設定の管理

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、Catalyst 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、センサーデバイスでの永続的なワイヤレスバックホール接続 （400 ページ） を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Settings]** > **[Sensors]** の順に選択します。

[Sensor List] ウィンドウが表示されます。

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

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

a) [Add Backhaul] をクリックします。

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

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

c) [Wired Backhaul] 領域で、次の設定を行います。

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

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザー名と証明書バンドルパスワードを入力します。
  - [PEAP-TLS]：[Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

    [Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザー名と証明書バンドルパスワードを入力します。

d) [Wireless Network Name（SSID）] 領域で、ワイヤレスネットワーク（SSID）を選択して、次の設定を実行します。

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

    [WPA2 Personal] を選択した場合は、[Passphrase] テキストボックスにパスフレーズを入力します。

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

e) [Save] をクリックします。

ステップ 4 既存のバックホール設定を編集するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Edit] を選択します。

ステップ 5 バックホール設定を削除するには、次の手順を実行します。

a) バックホール設定のチェックボックスをオンにします。

b) [Actions] ドロップダウンリストにカーソルを合わせて、[Delete] を選択します。

センサーデバイスでの永続的なワイヤレスバックホール接続

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

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

  有線センサーではベース無線 + 0x10（テスト SSID）MAC アドレスがテスト用に使用されます。
- センサーではデュアル同時無線動作が使用されます。1 つはバックホール接続用、もう 1 つはワイヤレステスト用です。
- スキャンを実行している間、および別の帯域をテストするためにインターフェイスを切り換えている間は、バックホール接続が中断します。
- バックホール接続の中断の頻度は、テスト設定に応じて異なります。
- バックホールとテスト SSID の帯域が同じである場合、バックホール接続は永続になりません。

SCEP プロファイルの管理

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

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Settings]** > **[Sensors]** の順に選択します。

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

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

a) [Add SCEP Profiles] をクリックします。

[Create SCEP Profile] ウィンドウが表示されます。

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

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

（注） [ISE] の場合は、次の情報を入力します。

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

[Microsoft CA]の場合は、次の情報を入力します。

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

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

c) [Save] をクリックします。

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

a) SCEP プロファイルの横にあるチェックボックスをオンにします。

b) [Actions] ドロップダウンリストで [Edit] を選択します。

ステップ 5 SCEP プロファイルを削除するには、次の手順を実行します。

a) SCEP プロファイルの横にあるチェックボックスをオンにします。

b) [Actions] ドロップダウンリストで [Delete] を選択します。

センサー主導テスト

テンプレートを使用したセンサー主導テストの作成と実行

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

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

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

始める前に

- Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[Inventory] で表示されるようにしてください。ワイヤレス Cisco Aironet 1800s アクティブセンサーのプロビジョニング（382 ページ）を参照してください。
- センサーテストテンプレートを再起動すると、そのテンプレートにあるすべてのセンサーで同時にテストの実行が開始されるため、結果のグラフに周期的なパターンが現れます。

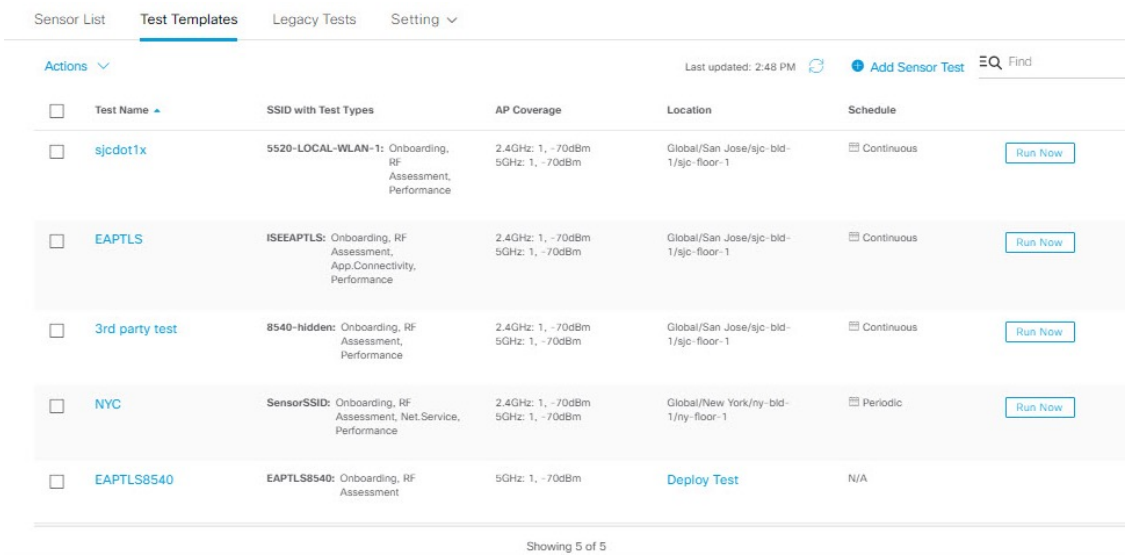
手順

ステップ 1 メインメニューから次を選択します。 **アシュアランス** > **センサー**。

ステップ 2 [Test Templates] タブをクリックします。

[Test Templates ウィンドウが表示されます。

図 *49 : [Test Templates]* ウィンドウ



ステップ 3 新しいセンサーテストテンプレートを作成するには、**[+ Add Sensor Test]** をクリックします。センサーテストテンプレートを作成するためのワークフローが表示されます。

ステップ 4 [Set up Sensor Test] ウィンドウで、次の設定を行います。

- [Test Template Name]：テストの名前を入力します。

（注） 文字、数字、アンダースコア、ハイフン、ピリオドのみ使用できます。

- [Ssid Selection]：センサーテストを行う SSID のチェックボックスをオンにします。

ステップ 5 **[Enter SSID Credentials]** ウィンドウで、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 [Open] である SSID では、次のオプションを選択します。
  - [Open]：パススルー方式の Web 認証を使用した SSID の場合は、電子メールアドレスを入力します。
  - [ISE Guest Portal]：ISE ゲストポータルのラベルを選択します。
  - [Clearpass Guest Portal]：Clearpass ゲストポータルのラベルを選択し、[Apply] をクリックします。
- **WPA2 パーソナル**セキュリティを使用した SSID の場合は、パスワードを入力します。
- **WPA2 エンタープライズ** セキュリティを使用した SSID の場合は、EAP メソッド、ユーザー名、およびパスワードを入力します。

ステップ 6 プロキシ設定を有効にするには、次の手順を実行します。

1. **[Add Proxy Settings]** チェックボックスをオンにします。
2. 次のプロキシ設定を行います。
   - [Proxy Server]
   - [Proxy Port]
   - [Proxy UserName]
   - [Proxy Password]

ステップ 7 **[Define Sensor Test Category Details]** ウィンドウで、対象にするテスト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) [Network Services Tests] テストカテゴリの場合は、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) [Performance Tests] テストカテゴリの場合は、次のテストタイプから選択します。
   - [Internet (NDT)]：ネットワーク診断ツール（NDT）を使用して速度テストを実行します。

     ネットワーク診断テスト（NDT）サーバーがある場合は、所定のフィールドに NTD サーバーの IP アドレスを入力します。NDT サーバーがプロキシサーバー経由で到達可能である場合は、所定のフィールドにプロキシサーバーの IP アドレスを入力します。
   - [iPerf3]：iPerf3 テストは、ネットワークパフォーマンスの測定に使用されるツールです。この機能を使用すると、一定量のトラフィックでネットワークの速度テストを実行して、トラフィックが通過できるかどうかをテストできます。

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

     iPerf3 の制限事項

- iPerf3 サーバーは最大 5 つまで追加できます。
- 各 iPerf3 サーバーについて、テンプレートごとに最大 5 つのポートを使用するように設定できます。iPerf3 テストを実行するポートはセンサーでランダムに選択されます。
- 特定の iPerf3 サーバーにおいて、2 つのセンサーを同じポートに同時に接続することはできません。
- 「iPerf : サーバーがビジー状態（iPerf: Server Busy）」エラーメッセージは、iPerf3 テストを実行しているセンサーの数に対応する十分な iPerf3 インスタンスがないことを示します。

  この問題を解決するには、次のいずれかを行います。

  - iPerf3 サーバーインスタンスを追加します。これを行うには、既存のサーバーで iPerf3 テストをサポートするポートを拡張します。
  - iPerf3 テストを実行するように設定されているセンサーの数を減らします。これを行うには、iPerf3 テスト用に別個のテンプレートを作成します。

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

  IPSLA テストを実行するには、ドロップダウンリストで、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) [Application Tests] テストカテゴリの場合は、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) [Email] テストカテゴリの場合は、次のテストタイプから選択します。

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

ステップ 8 [Select AP Coverage] ウィンドウで、次の手順を実行します。

a) テストする周波数帯域のチェックボックス（**2.4GHz** と **5GHz**）をオンにします。
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 の数を選択します。

（注） AP を 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、目的の RSSI しきい値までスライダをドラッグします。

ステップ 9 **[Summary]** ウィンドウで、テンプレートの設定を確認します。

再設定するには、**[SSIDs]** および **[AP Coverage]** ダッシュレットで **[Edit]** をクリックします。

ステップ 10 [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 11 **が完了しました。Sensor Test Created]** 確認ウィンドウで [Deploy Test to Locations] をクリックして、テストテンプレートを実行するロケーションとスケジュールを設定します。

重要 テストを展開せずに [Test Templates] ウィンドウに戻る場合は、[Location] 列から [Deploy Test] をクリックしてテスト展開の次の手順に進んでください。

ステップ 12 **[Select Location]** ウィンドウの左側のツリー階層で、テストテンプレートを展開するサイトのチェックボックスをオンにします。

ステップ 13 [Set Schedule] ウィンドウで、次のいずれかのテスト頻度オプションを選択します。

- [Periodic]：指定した間隔でテストを実行します。[Interval] ドロップダウンリストから、間隔を選択します。
- [Scheduled]：指定した期間中、指定した曜日にテストを実行します。
  1. [S]、[M]、[T]、[W]、[T]、[F]、[S] の各ボタンをクリックして、テストを実行する曜日を選択します。
  2. 選択した曜日に対して、**[From]** タイムピッカーからテスト期間の開始時刻と終了時刻を指定します。
  3. [Select Value] ドロップダウンメニューで、該当するテスト期間を選択します。
  4. 選択した曜日に別のテスト期間を追加するには、[+ Add] をクリックして、テスト期間を設定するための新しい行を追加します。
  5. テスト期間を削除するには、ごみ箱アイコンをクリックします。
- [Continuous]：テストは無期限に実行され、完了後に繰り返されます。

ステップ 14 **[Summary]** ウィンドウで、展開の詳細を確認します。

詳細を更新するには、**[Location]** および **[Schedule]** ダッシュレットで **[Edit]** をクリックします。

ステップ 15 [Deploy Test] をクリックします。

IP SLA パフォーマンステストを実行する予定である場合は、[Warning] ダイアログボックスが表示されます。**[Deploy]** をクリックして、選択したサイトの ワイヤレスコントローラ で IP SLA を有効にすることを確認します。これにより、センサーは AP に対して IP SLA テストを実行できます。

テストテンプレートは、**[Test Templates]** ウィンドウの **[Test Templates]** テーブルに表示されます。

ステップ 16 テストを実行するには、テストテンプレートの対応する **[Run Now]** をクリックします。

センサー主導テストのテンプレートの管理

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

始める前に

センサー主導テストのテンプレートを作成します。テンプレートを使用したセンサー主導テストの作成と実行 （402 ページ）を参照してください。

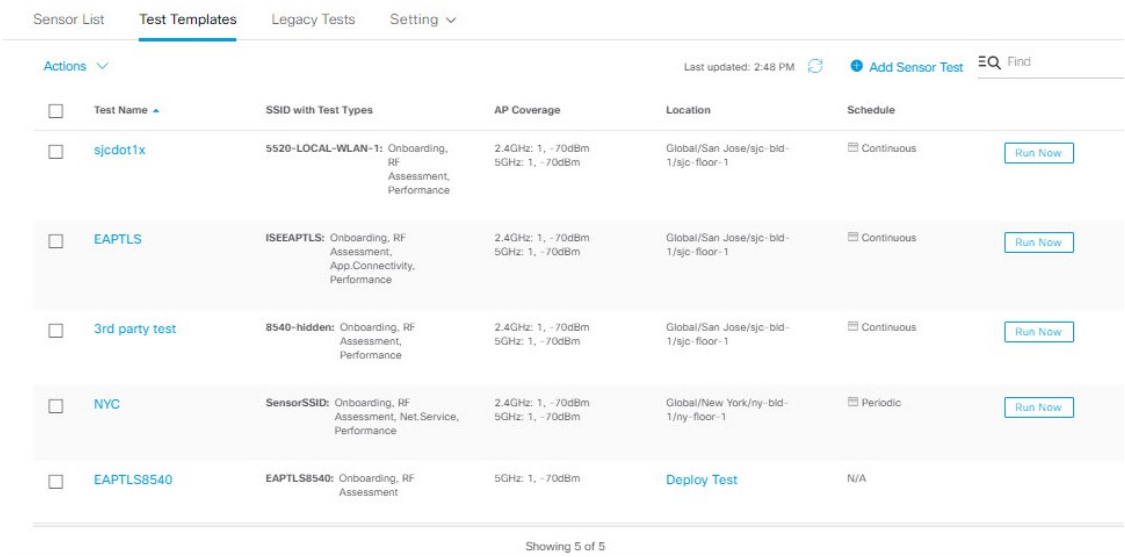
手順

ステップ 1 メインメニューから次を選択します。 **アシュアランス** > **センサー**。

ステップ 2 [Test Templates] タブをクリックします。

[Test Templates ウィンドウが表示されます。

図 *50 : [Test Templates]* ウィンドウ



ステップ 3 テストテンプレートを複製するには、次の手順を実行します。

a) 複製するテストテンプレートのチェックボックスをオンにします。
b) [Actions] ドロップダウンリストで [Duplicate] を選択します。
c) **[Input the new Test Name]** ダイアログボックスで、複製したテストテンプレートの名前を入力します。
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]** 列からテストテンプレートに対応する **[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) 削除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] ドロップダウンリストで [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。

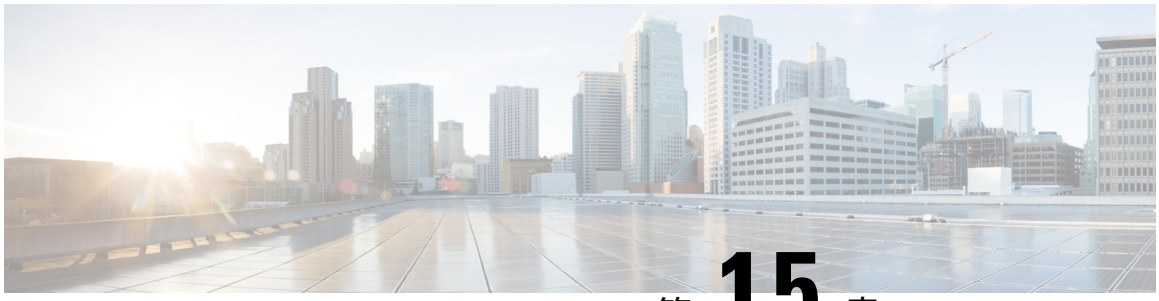
ステップ 5 テストテンプレートの展開を解除するには、次の手順を実行します。

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] ドロップダウンリストで [Undeploy] を選択します。
c) **[Warning]** ダイアログボックスで **[Undeploy]** をクリックします。

（注） テストテンプレートがIP SLAパフォーマンステストを実行するように設定されている場合は、**[Undeploy]** をクリックして、選択したサイトの ワイヤレスコントローラ で IP SLA を無効にすることを確認します。これにより、センサーは AP に対して IP SLA テストを実行しません。

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 15 章

Wi-Fi 対応状況のモニター

- Wi-Fi 対応状況の評価 （409 ページ）
- Wi-Fi ネットワークの対応状況の確認 （409 ページ）

Wi-Fi 対応状況の評価

Wi-Fi の対応状況評価機能によって、次のことがわかります。

- Wi-Fi 6E、6、7 に対応できるクライアントの割合。
- Wi-Fi 6E、6、7 対応の AP インフラストラクチャの割合。
- 前述の情報に基づいて、Wi-Fi 6E、6、7 ネットワークのメリットを最大限に活用できるようにするアクションに関する推奨事項が提供されます。

これらの推奨事項を提供するために、Catalyst Center 以下を評価します。

- ワイヤレスクライアントの Wi-Fi 機能を評価します。
- AP インベントリを収集して、Catalyst Center によって管理されている AP を特定し、これらの AP の Wi-Fi 機能を評価します。
- ネットワーク内にある ワイヤレスコントローラ のタイプと、ワイヤレスコントローラ にインストールされているソフトウェアが Wi-Fi 6E、6、7 に対応しているかどうかを判別します。
- 無線 LAN の設定と、Wi-Fi 6E、6、7 の機能が有効になっているかどうかを判断します。

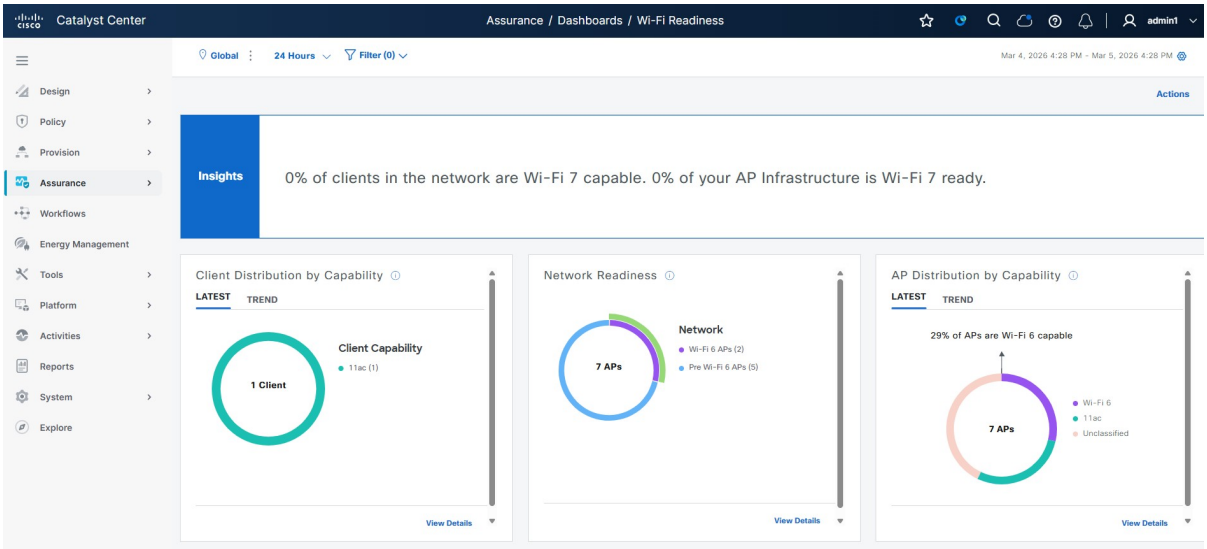
Wi-Fi ネットワークの対応状況の確認

この手順を使用して、Wi-Fi 7、Wi-Fi 6E、および Wi-Fi 6 ネットワークの対応状況を確認します。

手順

ステップ 1 メインメニューから次を選択します。 **Assurance** > **Wi-Fi 対応状況**。

[Wi-Fi Readiness] ダッシュボードが表示されます。



ステップ 2 上部のメニューバーで場所オプション（ Global ）をクリックして、サイト階層からサイト、建物、またはフロアを選択します。

ステップ 3 ロケーションアイコンの横にある をクリックして、以下を切り替えます。

- [サイトマップ（Site Map）]：ネットワーク階層の地理的ビューを提供します。
- [サイトテーブル（Site Table）]：正常性スコアやデバイス数を含む、すべてのサイトのリストベースビューを提供します。

[Location] ペインには次の機能があります。

アイテム	説明
 トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトと建物が表形式で表示されます。 ドロップダウンリストをクリックすると、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [建物/屋外エリアの表示（Building/Outdoor Area view）]：リストを建物レベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。
	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。
 トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。
	マップビューまたはテーブルビューを非表示にするには、この閉じるアイコンをクリックします。
 **時間範囲**の設定	ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 **1.** ドロップダウンメニューで範囲の長さ（[3 Hours]、[24 Hours]、または [7 days]）を選択します。 **2.** [Start Date] と時刻、[End Date] と時刻を指定します。 **3.** [Apply] をクリックします。
[Filter] アイコン	[SSID] および [Band] オプションが含まれます。ドロップダウンリストで、SSID と帯域周波数の横にあるチェックボックスをオンにして選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。
[Actions] ドロップダウン リスト	ダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。 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 （434 ページ）およびカスタムダッシュボードの作成 （431 ページ）を参照してください。

ステップ 4 ネットワークに関する情報を取得するには、[Insights] 領域を使用します。次の情報が提供されます。

- Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 対応クライアントの割合。
- Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 対応の AP インフラストラクチャの割合。
- 上記の情報に基づいて、Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 ネットワークのメリットを最大限に活用するために行うことができるアクションについての推奨事項が提供されます。

ステップ 5 **[Client Distribution By Capability]** ダッシュレットを使用して、Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 間のクライアントの配信機能を比較でき、Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 対応クライアントがネットワークに参加しているかどうかを確認できます。

クライアントが関連付けられている AP に基づいて、クライアントは Wi-Fi 7 機能で動作する場合もあれば、それより低い能力で機能する場合もあります。たとえば、11ac AP に関連付けられた Wi-Fi 6 クライアントは、11ac クライアントとして機能します。

[Client Distribution By Capability] ダッシュレット

Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6など、ネットワーク内のクライアントで使用可能なすべてのワイヤレス機能を表示できます。

このダッシュレットには次の 2 つのタブがあります。

- [Latest]：デフォルトで表示されます。
  - の円は、ネットワークに参加しているクライアントの実際のワイヤレス機能を示しています。ワイヤレスクライアントは次のいずれかのプロトコルで動作することができます。
    - [Wi-Fi 7]：802.11be 対応クライアント。
    - [Wi-Fi 6E]：802.11ax 6 GHz 対応クライアント。
    - [Wi-Fi 6]：802.11ax 対応クライアント。
    - [11ac]：802.11ac Wave1 および Wave2 対応クライアント。
    - [11n]：802.11n 対応クライアント。
    - [11abg]：802.11a、b、または g 対応クライアント。
    - [Unclassified]：次の理由で [Unclassified] に一覧表示されるクライアントがあります。
      - ネットワーク遅延のため、クライアントデバイスの機能が報告されません。
      - クライアントデバイスが接続されている AP またはワイヤレスコントローラに、正しいソフトウェアバージョンがインストールされていません。

  チャートのいずれかの色にカーソルを重ねると、その色に関連付けられたクライアントの数が表示されます。
- [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートでは、一定の時間範囲で Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6、または [Unclassified] プロトコルと関連付けられているクライアントの数が表示されます。

  チャートにカーソルを重ねると、クライアントの合計数と指定された日時におけるクライアントのプロトコルが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

ステップ 6 [Network Readiness] ダッシュレットを使用して、Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 に対応し、そのモードで動作するように設定（有効化）されている AP の数を確認します。

[Network Readiness] ダッシュレット
Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6など、ワイヤレスネットワークと関連付けられているクライアントで使用可能なすべてのワイヤレス機能を表示できます。 • 円の**外側**のセグメントは、6 GHz 帯域が有効になっている Wi-Fi 6E AP、または 11ax が無効になっている Wi-Fi 6 AP の数を示しています。 （注） Wi-Fi 6E AP は、ワイヤレスコントローラ および AP が 6 GHz 帯域をサポートするソフトウェアバージョンを実行している場合にのみ、Wi-Fi 6E モードで動作できます。 • **内側**の円は、Wi-Fi 6E、Wi-Fi 6 対応の AP および非 Wi-Fi 6（11ac/n/a/b/g）対応の AP の数を示しています。 （注） Wi-Fi 6 AP は、次の条件で Wi-Fi 6 モードで動作できます。 • Wi-Fi 6 AP で 11ax 設定が有効になっている。 • ワイヤレスコントローラと AP が Wi-Fi 6（11ax）をサポートするソフトウェアバージョンを実行している。 [View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色セグメントをクリックすると、[AP] タブと [WLC] タブが表示されます。[AP] タブと [WLC] タブをクリックすると、無線レベルと帯域レベルでの Wi-Fi 6 対応がそれぞれ表示されます。

ステップ 7 [AP Distribution by Protocol] ダッシュレットを使用して、Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6 をサポートするハードウェア能力がある AP の数を確認できます。

[AP Distribution by Protocol] ダッシュレット

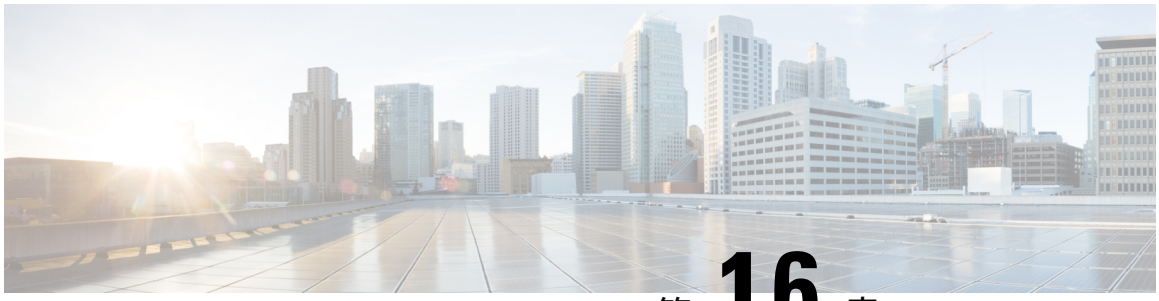
このダッシュレットには次の 2 つのタブがあります。

- [Latest]：デフォルトで表示されます。Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6をサポートする AP の数が表示されます。
  - [Wi-Fi 7]：802.11be 対応クライアント。
  - [Wi-Fi 6E]：802.11ax 6 GHz 帯域対応 AP。
  - [Wi-Fi 6]：802.11ax 対応 AP。
  - [11ac]：802.11ac 対応 AP。
  - [11n]：802.11n 対応 AP。
  - [11abg]：802.11a/b/g 対応 AP。

  チャートのいずれかの色にカーソルを重ねると、その色に関連付けられた AP の数が表示されます。
- [Trend]：[Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートでは、一定の時間範囲でさまざまなプロトコル（Wi-Fi 7、Wi-Fi 6E、Wi-Fi 6）に関連付けられている AP の数が表示されます。

  チャートにカーソルを重ねると、AP の合計数と指定された日時における AP のプロトコルが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



第 16 章

Power over Ethernet の監視

- Power Over Ethernet について （417 ページ）
- PoE テレメトリの設定ワークフロー （417 ページ）
- PoE テレメトリに使用するデバイスでの NETCONF の設定 （419 ページ）
- PoE テレメトリのテレメトリ設定の更新 （422 ページ）
- ネットワーク内の PoE 対応デバイスのモニター （422 ページ）

Power Over Ethernet について

Catalyst Center Power over Ethernet（PoE）を使用してネットワーク内の PoE 対応デバイスをモニターできます。また、PoE を供給するスイッチの電源の概要をモニターして、スイッチの電力バジェット、使用済み電力、電力残量、電力使用状況などの情報を提供します。PoE では、スイッチの割り当て済み電力と電力負荷も表示されます。

PoE テレメトリの設定ワークフロー

Assurance で PoE テレメトリと分析を有効にするには、必要な設定タスクを行う必要があります。基本的な設定ワークフローのタスクは次のとおりです。

1. PoE テレメトリに使用するネットワークデバイスで NETCONF を設定します。

   詳細については、「PoE テレメトリに使用するデバイスでの NETCONF の設定 （419 ページ）」を参照してください。

2. Catalyst Center でテレメトリ設定を更新します。

   詳細については、「PoE テレメトリのテレメトリ設定の更新 （422 ページ）」を参照してください。

設定ワークフロー

PoE テレメトリの設定ワークフローは、Catalyst Center のソフトウェアバージョンと設定、および PoE テレメトリをサポートするネットワークデバイスによって異なります。

Catalyst Center の新規インストールを行う場合は、次の表を参照してください。

Catalyst Center の新規インストール	
ネットワークデバイス設定	必須の設定タスク
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Catalyst Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Catalyst Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が有効になっている。	1. Catalyst Center でテレメトリ設定を更新します。

以前のリリースから Catalyst Center にアップグレードする場合は、次の表を参照してください。

以前のリリースからのアップグレード	
ネットワークデバイス設定	必須の設定タスク
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Catalyst Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.2 から 16.12.3s に SWIM でアップグレードされる。 • NETCONF が有効になっている。	1. Catalyst Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が無効になっている。	1. デバイスで NETCONF を有効にします。 2. Catalyst Center でテレメトリ設定を更新します。
• IOS XE のバージョンが 16.12.3s である。 • NETCONF が有効になっている。	1. Catalyst Center でテレメトリ設定を更新します。

PoEテレメトリをサポートしているネットワークデバイスの [Inventory] に変更がある場合は、次の表を参照してください。

インベントリ内のネットワークデバイスの変更	
ネットワークデバイスの変更	**必須の設定タスク**
インベントリからデバイスを削除して再度追加する。Catalyst Center	**1.** デバイスで NETCONF を有効にします。 **2.** Catalyst Center でテレメトリ設定を更新します。
インベントリに新しいデバイスを追加する。Catalyst Center	**1.** デバイスで NETCONF を有効にします。 **2.** Catalyst Center でテレメトリ設定を更新します。
インベントリの交換用デバイスを使用する。Catalyst Center	**1.** デバイスで NETCONF を有効にします。 **2.** Catalyst Center でテレメトリ設定を更新します。

PoE テレメトリに使用するデバイスでの NETCONF の設定

この手順では、PoEテレメトリに使用するネットワークデバイスでNETCONFを設定する方法を示します。PoEテレメトリを使用するには、サポートするネットワークデバイスでNETCONFが有効になっている必要があります。

始める前に

Catalyst Center とネットワークデバイスの設定によっては、PoE テレメトリを設定するためにこの手順を実行する必要がない場合もあります。詳細については、「PoE テレメトリの設定ワークフロー （417 ページ）」を参照してください。

手順

ステップ 1 既存のネットワークデバイスの NETCONF ポートを設定します。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

b) NETCONF が有効になるように設定するネットワークデバイスのチェックボックスをオンにします。

c) **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

d) [Type] ドロップダウン リストから、[Network Device] を選択します。

e) [NETCONF] 領域を展開します。

f) [Port] フィールドに、「**830**」と入力します。

（注） NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。

g) [Update] をクリックします。

デバイスの NETCONF ポートが設定されます。

ステップ 2 [Template Editor] で NETCONF 設定のプロジェクトを作成します。

a) メインメニューから次を選択します。**[Tools]** > **[Template Editor]** の順に選択します。

[Template Editor] ウィンドウが表示されます。

b) 左ペインで アイコンをクリックし、[Create Project] を選択します。

c) [Name] フィールドに、プロジェクトの名前を入力します。

d) [Add] をクリックします。

プロジェクトが [Template Editor] の左ペインに追加されます。

ステップ 3 NETCONF 設定のプロジェクトでテンプレートを作成します。

a) 左ペインで、プロジェクトの右にある アイコンにカーソルを合わせ、[Add Template] を選択します。

b) [Name] フィールドに、テンプレートの名前を入力します。

c) [Device Type（s）] フィールドで、[Edit] をクリックします。

d) スイッチとハブを追加するには、[Switches and Hubs] のチェックボックスをオンにしてテンプレートを適用します。

（注） スイッチの正確なモデルを指定する場合は、[Switches and Hubs] を展開し、特定のスイッチモデルのチェックボックスをオンにします。

e) [Back to Add New Template] をクリックします。

f) [Software Type] ドロップダウンリストをクリックし、[IOS-XE] を選択します。

g) [Add] をクリックします。

テンプレートが作成されて表示されます。

ステップ 4 テンプレートの内容を追加します。

a) テンプレートで次のように入力します。

```
netconf-yang
```

b) [Actions] ドロップダウンリストで [Save] を選択します。

テンプレートの内容が保存されます。

c) [Actions] ドロップダウンリストで [Commit] を選択します。
d) [Commit Note] テキストボックスに、メモを入力します。
e) [Commit] をクリックします。

ステップ 5 ネットワークプロファイルを作成してテンプレートを関連付けます。

a) メインメニューから次を選択します。**[Design]** > **[Network Profile]**の順に選択します。

[Network Profiles] ウィンドウが表示されます。

b) [+Add Profile] をクリックして [Switching] を選択します。
c) [Profile Name] フィールドに、ネットワークプロファイルの名前を入力します。
d) [Day-N Templates] タブをクリックします。
e) [Add] をクリックします。
f) [Device Type] ドロップダウンリストで [Switches and Hubs] を選択します。
g) [Template] ドロップダウンリストで、手順 3 で作成したテンプレートを選択します。
h) [Save] をクリックします。

ネットワークプロファイルが作成され、[Network Profiles] ウィンドウに表示されます。

ステップ 6 ネットワークプロファイルのサイトを割り当てます。

a) [Sites] 列で、[Assign Site] をクリックします。
b) ネットワークデバイスが割り当てられているサイトのチェックボックスをオンにします。
c) [Save] をクリックします。

ステップ 7 NETCONF 設定をネットワークデバイスにプロビジョニングします。

a) メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

b) PoE テレメトリのネットワークデバイスのチェックボックスをオンにします。
c) [Actions] ドロップダウンリストから、**[Provision]** > **[Provision Device]** の順に選択します。
d) [Assign Site] ステップで、[Next] をクリックします。
e) [Advanced Configuration] ステップで、[Provision these templates even if they have been deploy before] チェックボックスをオンにします。
f) [Next] をクリックします。
g) [Summary] ステップで、[Deploy] をクリックします。
h) [Apply] をクリックします。

プロビジョニングが開始され、NETCONF 設定がネットワークデバイスにプッシュされます。

PoE テレメトリのテレメトリ設定の更新

この手順では、Catalyst Center でテレメトリ設定を更新する方法を示します。これは、NETCONF ポートを設定し、PoE テレメトリに使用するネットワークデバイスに NETCONF 設定をプッシュした後に必要な手順です。

始める前に

PoE テレメトリ用に設定するネットワークデバイスで NETCONF ポートが確立され、NETCONF が適切に設定されていることを確認します。詳細については、「PoE テレメトリに使用するデバイスでの NETCONF の設定 （419 ページ）」を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウが表示されます。

ステップ 2 PoE テレメトリ用に設定されているネットワークデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Telemetry]** > **[Update Telemetry Settings]** の順に選択します。

ステップ 4 [Force Configuration Push] チェックボックスをオンにします。

（注） このオプションを選択すると、設定の変更がデバイスにプッシュされます。

ステップ 5 [Next] をクリックします。

ステップ 6 次のオプションボタンをクリックして、テレメトリ設定を更新するスケジュールを設定します。

- [Now]：このオプションを選択すると、テレメトリ設定がすぐに更新されます。
- [Later]：このオプションを選択すると、テレメトリ設定の更新をスケジュールすることができます。日付と時刻を指定します。

ステップ 7 [Apply] をクリックします。

ネットワーク内の PoE 対応デバイスのモニター

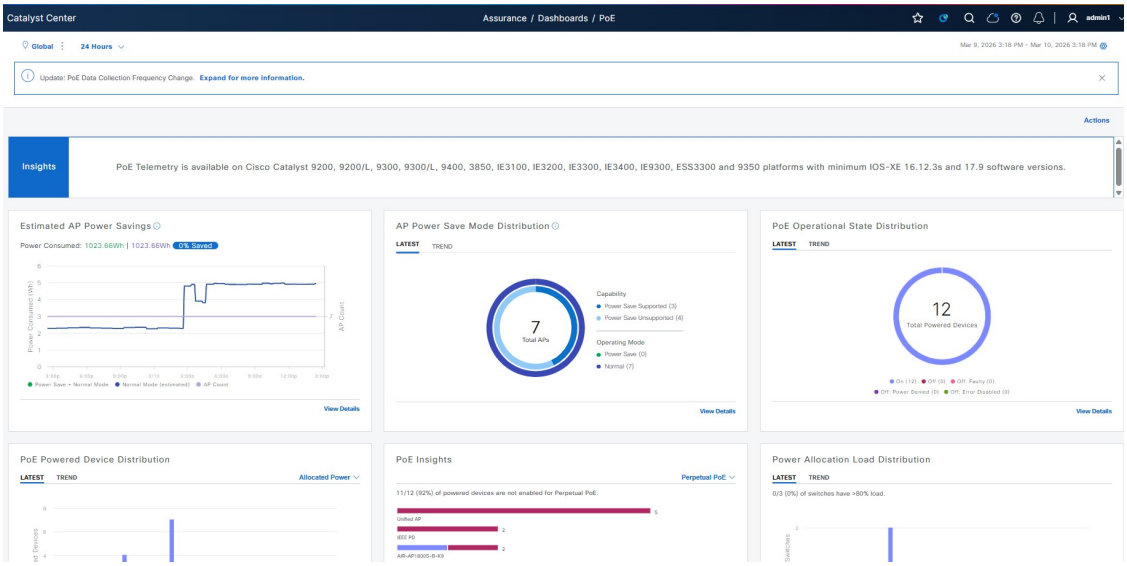
ネットワーク内の PoE 対応デバイスのグローバルビューを取得するには、次の手順を使用します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[PoE]** の順に選択します。

[PoE] ダッシュボードが表示されます。

図 *51 : [PoE]* ダッシュボード



ステップ 2 上部のメニューバーで場所オプション（ Global ）をクリックして、サイト階層からサイト、建物、またはフロアを選択します。

ステップ 3 ロケーションアイコンの横にある をクリックして、以下を切り替えます。

- [サイトマップ（Site Map）]：ネットワーク階層の地理的ビューを提供します。
- [サイトテーブル（Site Table）]：正常性スコアやデバイス数を含む、すべてのサイトのリストベースビューを提供します。

[Location] ペインには次の機能があります。

[Location] オプション	
アイテム	説明
 トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。 ドロップダウンリストをクリックすると、次のオプションを選択できます。 • [Hierarchical Site View]：リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [建物/屋外エリアの表示（Building/Outdoor Area view）]：リストを建物レベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。
	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。
 トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。
	マップビューまたはテーブルビューを非表示にするには、この閉じるアイコンをクリックします。

ステップ 4 上部のメニューバーにある時間範囲設定（ ）をクリックして、ダッシュボードに表示するデータの時間範囲を指定します。

a) ドロップダウンメニューで、[3 hours]、[24 hours]、[7 days] のいずれかの時間範囲を選択します。
b) [Start Date] と時刻、[End Date] と時刻を指定します。
c) [Apply] をクリックします。

ステップ 5 上部のメニューバーにある [Actions] ドロップダウンリストをクリックすると、次の機能を実行できます。

- [Export Dashboard]：PoE ダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- [Edit Dashboard]：ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 （434 ページ） およびカスタムダッシュボードの作成 （431 ページ） を参照してください。

ステップ 6 次の機能には [PoE] ダッシュレットを使用します。

AP 省電力モード分布

[AP Power Save Mode Distribution] には、AP 省電力機能、および省電力モードと通常モードの AP の平均数が表示されます。

[Latest] タブには、省電力機能および省電力モードと通常モードをサポートする AP の数が表示されます。

[Trend] タブには次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注）
表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00ー11:00の間に受信されたデータは、10:00のタイムスタンプで表示されます。このデータポイントは、対応する期間の終了後に使用可能になります。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインの色分けされたチャートにカーソルを合わせると、特定の時間に省電力モードと通常モードの省電力機能で配布された AP の総数が表示されます。上位サイトの AP の数と上位のデバイスタイプに基づいて、チャートの下に表示されるテーブルのデータをフィルタ処理できます。

AP の省電力

AP の省電力モードでは、AP の無線をシャットダウンするか、無線空間ストリームを減らすことで消費電力を削減できます。また、その時間範囲中に消費および節約された総電力が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注）
表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00ー11:00の間に受信されたデータは、10:00のタイムスタンプで表示されます。このデータポイントは、対応する期間の終了後に使用可能になります。

[View Details] をクリックすると、[AP Power Savings] スライドインペインに追加の詳細情報が表示されます。スライドインペインの色分けされたチャートには、ある時間範囲における AP の消費電力が表示されます。チャートにカーソルを合わせると、AP の総数、省電力モードおよび通常モードで一定期間に節約された電力が表示されます。

PoE AP 電力モードの分布

完全に電力が供給されている AP と部分的に電力が供給されている AP の分布が表示されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注）
表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

PoE 動作状態の分布

ネットワーク内の PoE 対応デバイスの数が表示されます。PoE で供給されているかどうかに基づいて、色分けされたチャートでデバイスの数が示されます。PoE で供給していないデバイスについては、その理由に応じてさらに分類されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

（注）
表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

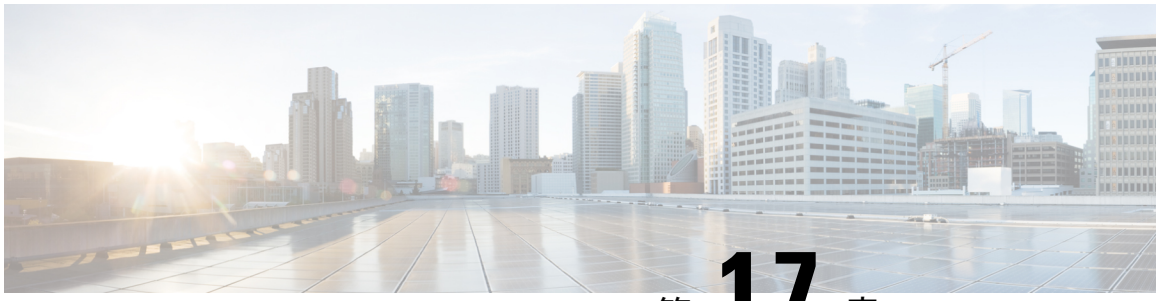
PoE 受電デバイスの分布
現在 PoE を使用しているデバイスのうち、特定の基準に当てはまるデバイスの割合が表示されます。ドロップダウンリストを使用して次の基準を指定します。 • 割り当て済み電力 • 受電デバイスクラス [Latest] タブには、10 分間のスナップショットビューが表示されます。 [Trend] タブには次の情報が表示されます。 • 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。 • 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 （注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00ー11:00の間に受信されたデータは、10:00のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。 [View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

電力割り当て負荷分散
PoE の電力負荷に基づくスイッチの割合が表示されます。 [Latest] タブには、10 分間のスナップショットビューが表示されます。 [Trend] タブには次の情報が表示されます。 • 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。 • 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 （注） 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ー 10:10 の間に受信されたすべてのデータは、時刻値 10:00 で表示されます。同様に、毎時ウィンドウでは、10:00 ー 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。 [View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

PoE インサイト
現在 PoE を使用しているデバイスのうち、次の PoE テクノロジーをサポートするか IEEE に準拠するように設定されているデバイスの割合が表示されます。 • **無停止型 POE** • **高速 PoE** • **IEEE 準拠** • **UPOE+** ドロップダウンリストを使用して、特性を選択します。 [View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

電力使用量
現在 PoE を使用しているデバイスごとの合計電力使用量と割り当て電力が表示されます。ドロップダウンリストを使用して [Consumption] または [Allocation] ビューを選択すると、[Latest] および [Trend] タブにそれぞれのデータが表示されます。 [Latest] タブには、10 分間のスナップショットビューが表示されます。円グラフには、[PoE Power Allocation]、[System Power Allocation]、[Available Power] などの [Power Allocation] の詳細と [PoE Power Consumption] や [System Power Consumption] などの [Power Consumption] の詳細がワット単位で表示されます。 [Trend] タブには次の情報が表示されます。 • 時間範囲の設定で 24 時間を選択した場合、トレンドチャートには電力使用の 24 時間の範囲全体で 10 分のデータポイントが表示されます。 • 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 [View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、一定期間におけるデバイスの [System Power] の情報（[System Power Consumption] および [System Power Allocation]）と [PoE Power] の情報（[PoE Power Consumption] および [PoE Power Allocation]）をチャートの下に表示されるテーブルで確認できます。 水平バーとして表示されるデータを選択して、電力使用量、デバイスロール、および場所に基づいて表示される前述のテーブルをフィルタ処理できます。

PoE ポートの可用性
PoE の電力負荷に基づいてポートの可用性が表示されます。 [Latest] タブには、10 分間のスナップショットビューが表示されます。 [Trend] タブには次の情報が表示されます。 • 時間範囲の設定で 24 時間以下の時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。 • 時間範囲の設定で 7 日間を選択した場合、トレンドチャートには、時間範囲全体に対して 12 時間のデータポイント（1 時間のデータから集約）が表示されます。 [View Details] をクリックして、追加の詳細を含む スライドインペイン を開きます。スライドインペインからチャートの1時間のデータポイントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



第 17 章

ダッシュボードの管理

- ダッシュボードについて （431 ページ）
- カスタムダッシュボードの作成 （431 ページ）
- ダッシュボードの表示 （432 ページ）
- ダッシュボードの編集または削除 （433 ページ）
- ダッシュボードの複製 （433 ページ）
- ダッシュボードをお気に入りに設定 （434 ページ）
- ダッシュレットの位置の変更 （434 ページ）
- フィルタグループの設定 （435 ページ）

ダッシュボードについて

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

カスタムダッシュボードは、それを作成したユーザーアカウントにのみ表示されます。作成者であるユーザー以外のユーザーには表示されません。

カスタムダッシュボードの作成

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。

ステップ 2 [+ Create a Dashboard] をクリックします。

ステップ 3 **[Create a Dashboard]** ダイアログ ボックスで、ダッシュボードのタイトルを入力します。

ステップ 4 [Save] をクリックします。
空白のダッシュボードが表示されます。

ステップ 5 ダッシュボードでは、次の手順を実行できます。

a) [+ Add a Dashlet] をクリックして、このダッシュボードに内容を追加します。

b) ダッシュボードに追加するダッシュレットの横にあるチェックボックスをオンにします。

（注） ドロップダウンリストからカテゴリを選択するか、右側にある検索ボックスを使用して、ダッシュレットを検索します。

c) [Add] をクリックしてダッシュレットをダッシュボードに追加します。

ステップ 6 （任意）ダッシュレットをドラッグアンドドロップすると、ダッシュボード上でのダッシュレットの場所を変更できます。

ステップ 7 ダッシュボードからダッシュレットを削除するには、次の手順を実行します。

a) ダッシュレットの右上隅にあるゴミ箱アイコンをクリックします。

b) ダイアログボックスで、[Delete] をクリックします。

ステップ 8 [Save] をクリックしてダッシュボードを保存します。

ダッシュボードの表示

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboard Library]** の順に選択します。**[Dashboard Library]** ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

（注） ダッシュボードを [Date Modified] で並べ替えると、ダッシュボードに変更が加えられていない場合でも、ダッシュボードを最後に開いた日時で並べ替えられます。

ステップ 2 お気に入りとしてマークされているダッシュボードを表示するには、[Favorite Dashboards] タブをクリックします。

ステップ 3 表示するダッシュボードをクリックします。

ステップ 4 ダッシュボードのコントロールで、[Show] または [Hide] をクリックし、必要に応じてマップを表示または非表示にします。

ステップ 5 （任意）フィルタから適切な値を選択して、期間、サイト、またはドメイン別にダッシュボードデータをフィルタ処理します。

ダッシュボードの編集または削除

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 編集または削除するダッシュボードをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- 変更するには、[Actions] メニューで [Edit Dashboard] を選択します。ダッシュレットを追加または削除し、ダッシュレットをダッシュボード内の別の位置にドラッグできます。設定が終了したら、[Save] をクリックします。
- ダッシュボードを削除するには、[Actions] メニューで [Delete Dashboard] を選択します。確認ダイアログで [Delete] をクリックします。

ダッシュボードの複製

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboard Library]** の順に選択します。
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 ダッシュボードの複製アイコン（スターアイコンの隣）をクリックします。

ステップ 3 [Duplicate a Dashboard] ダイアログボックスで、ダッシュボードコピーのタイトルを入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 コピーしたこのダッシュボードは、ダッシュレットを追加、削除、または再配置することで変更できます。

ステップ 6 [Save] をクリックしてダッシュボードを保存します。
確認用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設定

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Dashboard Library]** の順に選択します。

[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[Sort By] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[Find] フィールドにその名前を入力して検索することができます。

ステップ 2 ダッシュレット名の横にある ☆ をクリックすると、お気に入りとして登録されます。

（注） [Favorite Dashboards] タブをクリックすると、お気に入りにしたダッシュボードにアクセスできます。

ダッシュレットの位置の変更

Assurance 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。

手順

ステップ 1 次のいずれか 1 つのタスクを実行します。

- [Health]メインメニューから次を選択します。**Assurance** > 。

  [Overall Health] ダッシュボードが表示されます。

- メインメニューから次を選択します。**Assurance** > **[Health]** > **[Network Health]**。

  [Network Health] ダッシュボードが表示されます。

- メインメニューから次を選択します。**Assurance** > **[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。

- メインメニューから次を選択します。**Assurance** > **[Health]** > **[Application Health]**。

[Application Health] ダッシュボードが表示されます。

ステップ 2 [Actions] ドロップダウンリストをクリックし、[Edit Dashboard] を選択します。
ダッシュボードが更新され、編集可能になります。

ステップ 3 移動するダッシュレットをクリックしてダッシュボードの別の位置にドラッグします。

ステップ 4 [Save] をクリックします。

フィルタグループの設定

次の手順に従って、[Client] ダッシュボードおよび [Network Template] ダッシュボードに対して範囲を定義し、特定のフィルタを設定します。

手順

ステップ 1 メインメニューから次を選択します。 **[Assurance]** > **[Filter Group Settings]**。

[Filter Group Settings] ウィンドウが表示されます。

ステップ 2 [Add New] をクリックします。

ステップ 3 [Add New] スライドインペインで、フィルタグループを設定します。

a) [Filter Group Name]フィールドに、フィルタグループ名を入力します。

b) [Filter Group Type] ドロップダウンリストで、フィルタグループタイプとして [Client] または [Network] を選択します。

c) [Add a Filter] をクリックします。

d) [Filter] ドロップダウンリストで、フィルタの横にあるドロップダウンリストからフィルタおよび該当する値を選択します。選択したフィルタグループタイプに基づいてフィルタの一覧が表示されます。

クライアントフィルタグループでサポートされているフィルタ：[Site]、[Device Type]、[SSIDs]、[MAC Address]、[IP Address]、[Host Name]。

ネットワークフィルタグループでサポートされているフィルタ：[Site]、[Network Device Type]、[Network OS]、[Host Name]、[IP Address]。

e) [Confirm] をクリックします。



第 18 章

ネットワークのトレンドの観察およびインサイトの取得

- ネットワークのトレンドとインサイトについて （437 ページ）
- ワイヤレス AP のパフォーマンスアドバイザリの表示 （438 ページ）
- ネットワークのトレンドの表示とインサイトの取得 （442 ページ）
- ネットワークヒートマップでのアクセスポイントおよびスイッチの比較 （448 ページ）
- ネットワーク内のピアとの KPI 値の比較 （451 ページ）
- 建物、AP モデルファミリ、ワイヤレス エンドポイント タイプの比較 （453 ページ）
- ベースラインを使用したネットワークパフォーマンスの表示と監視 （457 ページ）
- AI 拡張 RRM ダッシュボードを使用した RF ネットワークの表示 （460 ページ）

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 は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。
- [AP Performance Advisories]：一貫してクライアント エクスペリエンスが低い AP を検出し、根本原因と推奨されるアクションを提供します。
- **比較分析**には、次の機能があります。
  - [AI-Driven AP Comparisons in Network Heatmaps]：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-Driven Peer Comparisons]：選択した主要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。
  - **AI 駆動型のネットワークの比較**：選択した KPI 全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリ、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

ワイヤレス AP のパフォーマンスアドバイザリの表示

Cisco AI Network Analytics は、機械学習アルゴリズムを使用して、潜在的にクライアント エクスペリエンスが低いワイヤレス AP を特定します。AP は長期間にわたって継続的に分析され、最適ではないクライアントエクスペリエンスを提供していると疑われる AP は、根本的な原因と提案される改善点によってグループ化されます。修正可能な根本的な問題を診断するために使用できる一連の無線およびネットワーク機能で構成されるインサイトが生成されます。インサイトには次の主要なコンポーネントがあります。

- さまざまなクライアントエクスペリエンス KPI によってパフォーマンスの低い AP を検出します。
- 根本原因分析（RCA）の基礎として、重要であり、顧客によって実行可能な、不十分なクライアント エクスペリエンスまたは優れたクライアント エクスペリエンスを持つ AP を区別できる適切な機能を見つけます。

AP は、2.4 GHz、5 GHz、および 6 GHz の別々の周波数帯域で分析されます。SNR、RSSI、リンク速度、パケット再試行、パケット障害など、さまざまな KPI の統計分析を使用して、不十分なクライアント エクスペリエンスが検出されます。

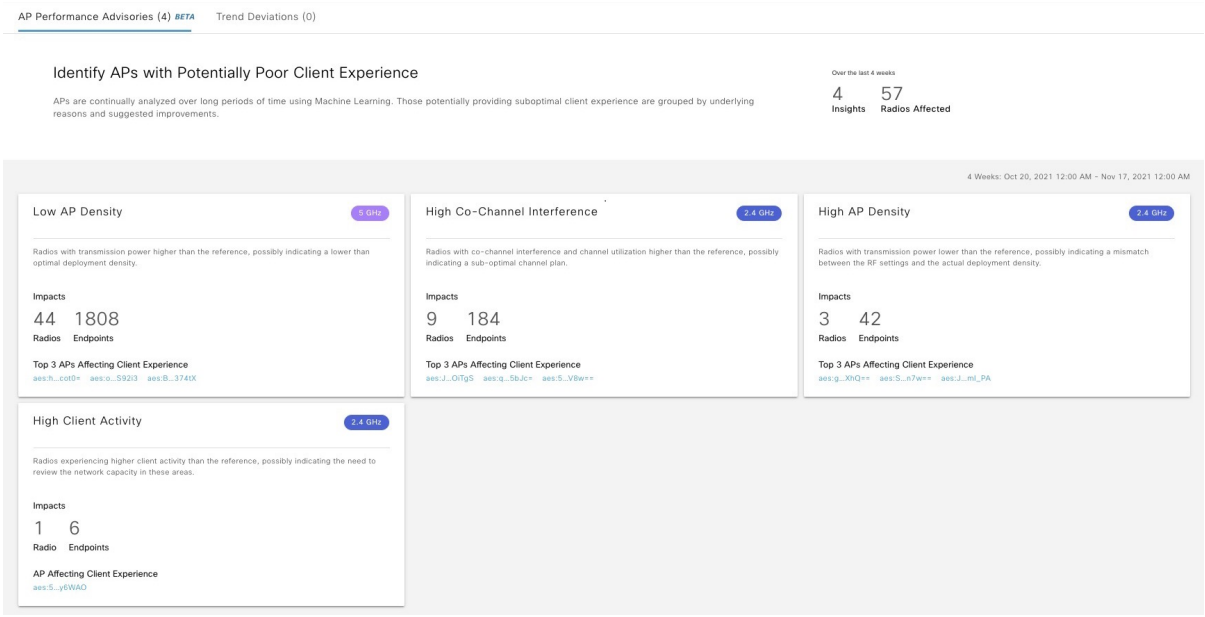
この手順を使用して、 AP パフォーマンスアドバイザリを表示し、4 週間のデータの分析に基づいてクライアント エクスペリエンスが低い最もアクティブな AP を強調表示します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Trends and Insights]** > **[AP Performance Advisories]** の順に選択します。

ステップ 2 [AP Performance Advisories] タブをクリックすると、一般的な根本原因分析カテゴリと影響を受ける無線に関するさまざまなタイプのインサイトの概要が表示されます。

図 *52 : AP* パフォーマンスアドバイザリ



よくある根本原因分析で発生する可能性のあるインサイトを以下に示します。

- 外部 RF 負荷
- クライアントアクティビティが多い外部 RF 負荷
- 頻繁なチャネル変更
- 高 RF 負荷
- 高いチャネル使用率
- 高いクライアントアクティビティ
- 高いクライアントの負荷
- 高い AP 展開密度
- 低い AP 展開密度
- 低い AP 展開密度および外部干渉
- 低い AP 展開密度および高負荷

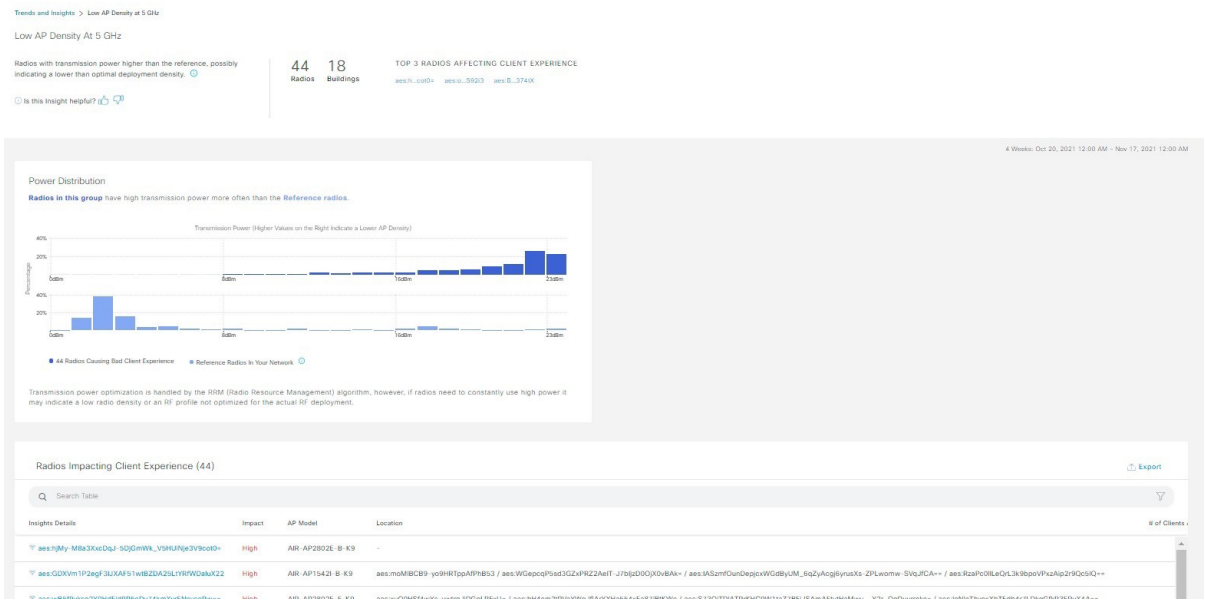
ステップ 3 [AP Performance Advisories] ダッシュボードでは次のインサイトサマリーを確認できます。

[Network Overview] ウィンドウ	
アイテム	**説明**
インサイトサマリー	特定の周波数帯に関するインサイト（低 AP 密度、高クライアントアクティビティなど）の名前と問題定義を表示します。

[Network Overview] ウィンドウ	
アイテム	説明
影響	インサイトごとに影響を受ける [Radios] と [Endpoints] の数を表示します。
クライアントエクスペリエンスに影響する上位 3 つの AP	特定の周波数帯で影響を受ける上位 3 つの AP を表示します。これらは、手順 5 に示す詳細ページへのハイパーリンクです。

ステップ 4 情報に関する各 [Insight] ダッシュレットをクリックすると、よくある根本原因分析、およびこのカテゴリのすべての無線に対する推奨アクションが表示されます。

図 *53* : 影響を受ける無線に関する *[Insights Summary]* ダッシュボード



[Insight] ダッシュボード	
アイテム	説明
SUMMARY	4 週間にわたって分析された無線の総数、建物の数、影響を受けた上位 3 つの AP を表示します。
[KPI] チャート	すべての無線での KPI の分布を示す RCA カテゴリに応じて、複数の KPI チャートを表示します。チャートを使用して、この一般的な RCA を使用した無線のパフォーマンスを、クライアントエクスペリエンスの問題が検出されていない参照の無線と比較対照できます。
[Radios Impacting Client Experience] テーブル	インサイトの詳細、影響（低、中、または重大）、AP モデル、場所、影響を受けるクライアントの数、およびクライアントエクスペリエンスに影響を与える KPI が含まれます。

[Insight] ダッシュボード	
アイテム	説明
[Export]	CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。

ステップ 5 [Radios Impacting Client Experience] テーブルで、ハイパーリンク付き AP をクリックすると、特定の AP に関する次の詳細なインサイトサマリーが表示されます。

図 *54 : AP* に関するインサイトサマリー



[Insight] ダッシュボード	
アイテム	説明
上部バー	AP モデル、場所、影響を受けるクライアント、および [Assurance Device] ウィンドウにハイパーリンクされた追加の AP の詳細などの情報を表示します。また、クライアントエクスペリエンスを向上させるために、特定された根本原因と異常な KPI に固有の推奨アクションも提供します。
[Client Experience KPIs]	• ヒストグラムは、クライアントエクスペリエンスに影響を与えるさまざまな KPI の分布を示し、個々の AP と顧客のネットワーク全体の参照 AP（クライアント エクスペリエンスの問題が観察されていない AP）を比較しやすくします。 • デフォルトでは、異常が検出された KPI のみが表示されます。SNR、RSSI、リンク速度、パケットの再試行、パケットの失敗など、KPI の分布を表示する KPI の数を増やすことができます。 • カーソルをヒストグラムの bin 値の上に置くと、AP の参照セットと比較して、選択した AP で観測された発生率の追加の詳細を表示できます。

[Insight] ダッシュボード	
アイテム	説明
[Radio Specific Root-Cause Context]	• ヒストグラムは、無線に影響を与えるさまざまな根本原因分析KPIの分布を示します。デフォルトでは、異常が検出されたKPIのみが表示されます。 • SNR、RSSI、リンク速度、パケットの再試行、パケットの失敗など、RCA KPIの分布を表示するKPIの数を増やすことができます。 • カーソルをヒストグラムのbin値の上に置くと、無線の参照セットと比較して、選択した無線で観測された発生率の追加の詳細を表示できます。

ネットワークの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。

手順

ステップ1 メインメニューから次を選択します。**Assurance** > **[Trends and Insights]** > **[Trend Deviations]**の順に選択します。

[Network Insights] ウィンドウに、[Capacity]（デフォルト）、[Coverage]、[Throughput] のフィルタが表示されます。テーブルのデータを更新するには、該当するフィルタをクリックします。

（注） フィルタは動的です。フィルタに使用可能なインサイトがない場合、そのフィルタは表示されません。

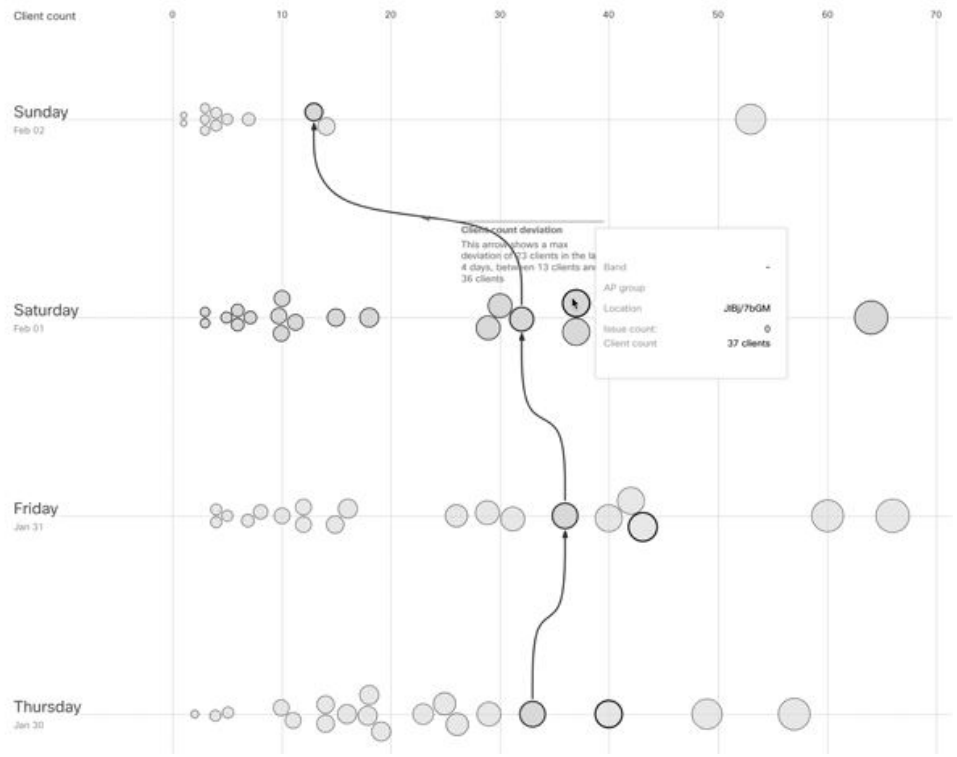
[Insights] テーブル	
アイテム	説明
Occurrence	このトレンドが観測された期間（[May 27 - June 03 2023] など）。
[Insight Type]	[Daily] および [Weekly] のインサイトタイプのリスト。
Insight	特定の期間に観測されたすべての AI 駆動型のインサイトのリスト。
カテゴリ	インサイトが観測されたカテゴリ。インサイトの KPI は次のカテゴリに分類されています。 • [Capacity]：無線クライアント数、チャネル変更数 • [Coverage]：干渉、平均クライアント SNR、平均クライアント RSSI、トラフィック、使用率 • [Throughput]：総無線スループット
Frequency band	インサイトが観測された AP で使用されていた周波数帯。 値は [2.4 GHz]、[5 GHz]、[6GHz] またはすべての周波数帯です。
KPI	特定のインサイトの 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。

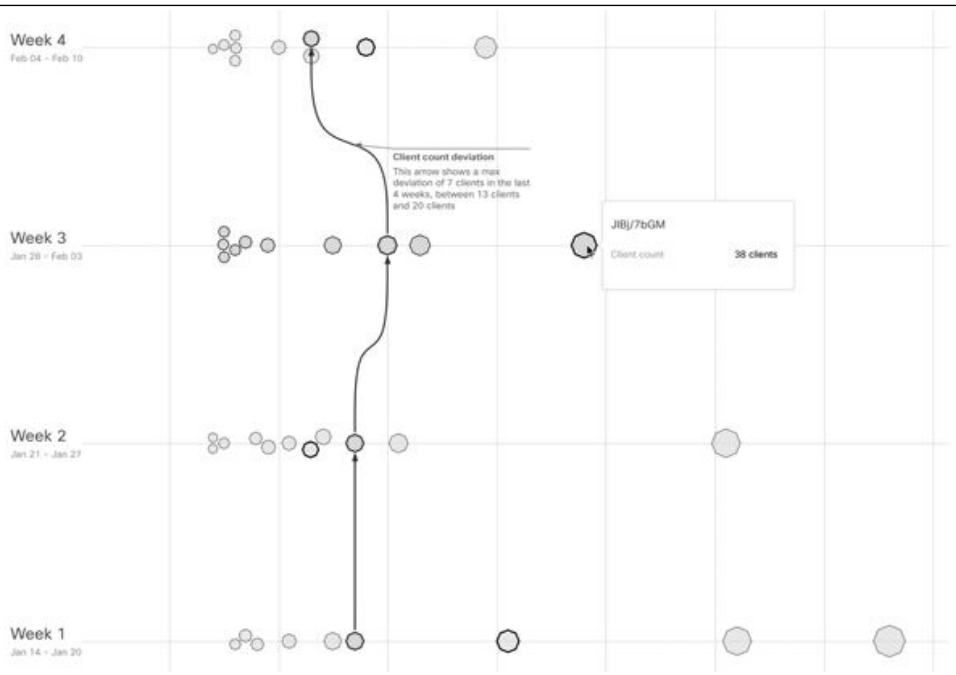
ステップ 2 [Insight] 列でインサイトをクリックすると、スライドインペイン が開いて、次の情報が表示されます。

[Insight Details] スライドインペイン	
アイテム	説明
Cisco AI	インサイトの計算方法に関する情報が表示されます。 人工知能の概要については、[Learn More]https://www.cisco.com/c/en/us/solutions/artificial-intelligence.html をクリックしてください。
Insight Summary	蜂群グラフで確認されるトレンドに関する簡単なサマリー。このサマリーには、サイトまたは AP の名前、クライアント数、無線帯域周波数、および乖離が観測された時間帯などの情報が表示されます。
Weekly Client Load	週あたりのクライアント負荷。

[Insight Details] スライドインペイン	
アイテム	説明
トラブルシューティング	重大な問題になる前にトレンドのトラブルシューティングと修正を実施するためのリンクがあります。 • [Network Heatmap] をクリックすると、ヒートマップが開き、蜂群グラフで強調表示されている AP またはビルディングに関する情報が提供されます。トレンドが観測された特定の月のヒートマップが表示されます。 • [Intra-Site]：ヒートマップが起動し、特定の AP が優先順位に従って強調表示されたリストが表示されます。 • [Inter-Site]：ヒートマップが起動し、ビルディング（サイト）内の AP のフィルタ処理されたビューが表示されます。 • AP の名前をクリックすると、その AP の [Device 360] ページが開きます。
問題数	問題数のグラデーション。

[Insight Details] スライドインペイン	
アイテム	説明
チャート	

[Insight Details] スライドインペイン	
アイテム	説明
	蜂群チャートには、次の図のように、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 日（[Daily Insights]）および週（[Weekly Insights]）の時間間隔で表示されます。一定期間にわたってネットワークの動作に系統的逸脱がある場合に、その傾向がチャート内の矢印で表示されます。 **図 *55 :* 蜂群チャート** [Daily Insights]  [Weekly Insights]

[Insight Details] スライドインペイン	
アイテム	説明
	 （注） • 蜂群チャート内の各円は、次のことを表しています。 • **サイト内**：円は無線を表します。 • **サイト間**：多角形はビルを表します。 • 円のサイズは、AP 内のクライアントの数を表します。小さな円には少数のクライアントが、大きな円には多数のクライアントが含まれます。

ステップ 3 チャート内の円の上にカーソルを置くと、AP の名前と MAC アドレス、帯域周波数、AP グループ、AP の場所、問題の数、クライアント数、および KPI 値などの情報が表示されます。

（注） グローバルサイトでは、チャート内の円の上にカーソルを置くと、トレンドが観測されたビルやクライアント数に関する情報が表示されます。

ネットワークヒートマップでのアクセスポイントおよびスイッチの比較

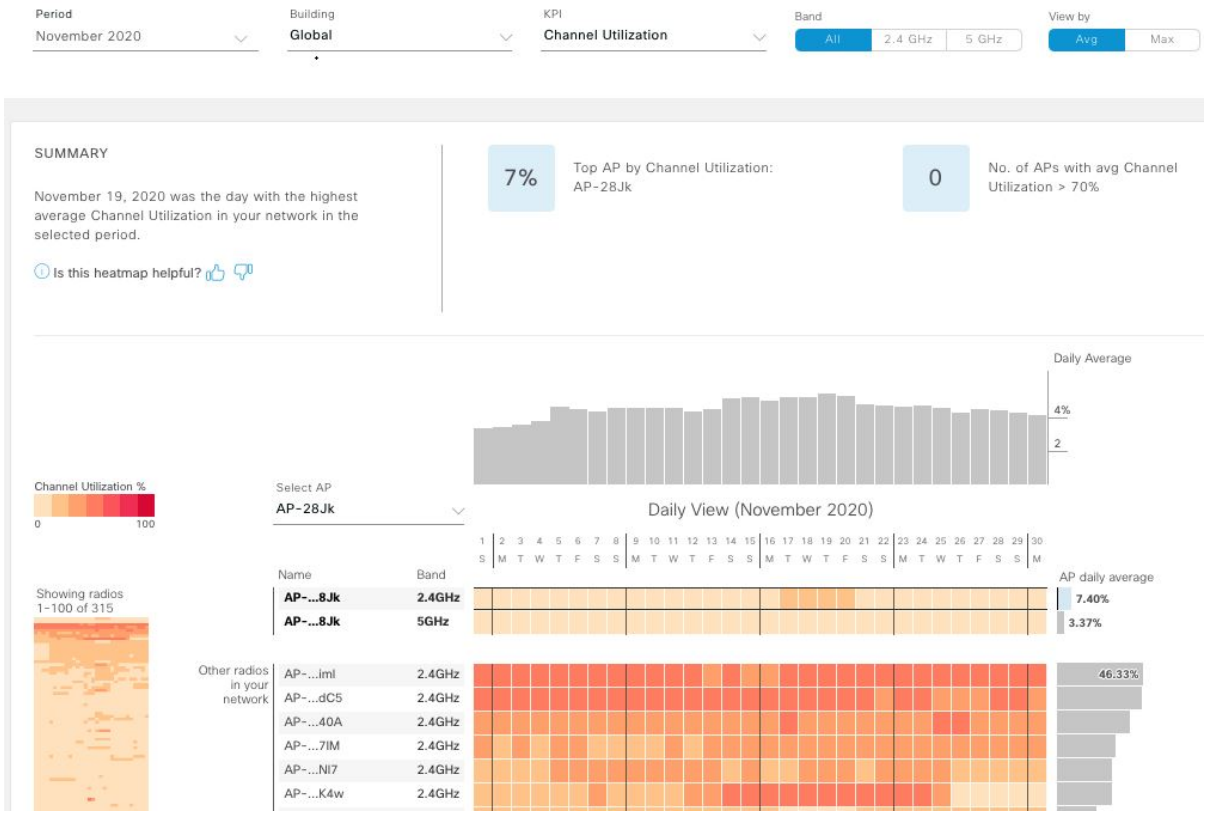
ネットワークヒートマップを使用して、特定の月に関してネットワーク内のすべての AP を視覚的に比較し、トレンドを把握し、インサイトを取得します。さまざまなKPIと帯域周波数で AP を比較することを選択できます。取得したインサイトにより、最も輻輳が多い KPI、最も輻輳のある AP、および それらの AP のうち使用中の AP に関する情報が得られます。この情報により、トレンドが観察されたサイトまたはビルにさらにドリルダウンすることができます。AP または AP のグループを特定したら、それらの AP の動作履歴（1 日、1 週間、および月全体）を判断できます。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **[Network Heatmap]** の順に選択します。

[Network Heatmap] ウィンドウには次の情報が表示されます。

図 *56 : [Network Heatmap]* ウィンドウ



[Network Heatmap] ウィンドウ	
アイテム	説明
Show	ドロップダウンリストで選択したデバイスタイプに基づいてヒートマップ情報が表示されます。[Access Points]（デフォルト）または [Switches] を選択できます。
[KPI] ドロップダウンリスト	ドロップダウンリストで選択した KPI のヒートマップに情報が表示されます。 [Access Points] の場合、デフォルトの KPI は [Client Count] です。 [Switches] の場合、デフォルトの KPI は [Temperature: All Sensors] です。
[Swtich Family] ドロップダウンリスト	ドロップダウンリストで選択したスイッチファミリに基づいてヒートマップに情報が表示されます。 このドロップダウンリストは、[Show] ドロップダウンでデバイスタイプとして [Switches] を選択した場合にのみ表示されます。
Time Range	[Time Range] ドロップダウンをクリックして [Month] または [Day] を選択すると、指定した月または日の情報がヒートマップに表示されます。
Location	グローバルネットワーク全体またはドロップダウンリストで選択した特定のサイトと建物の情報がヒートマップに表示されます。デフォルトは [global] です。
[Band]	選択した域周波数のヒートマップに情報が表示されます。[2.4 GHz]、[5 GHz]、[6 GHz] のいずれかを選択できます。デフォルトでは、3 つの帯域周波数がすべて選択されています。
[View By]	選択したオプションに基づいてヒートマップの情報が表示されます。 [View By] リストに表示されるオプションは、選択した KPI に応じて異なります。 KPI に応じて、[Avg]、[Min]、または [Max] を並べ替えのオプションとして選択できる場合、[Avg] または [Max] を選択できる場合のほか、いずれのオプションも提供されない場合もあります。
[Summary] 領域	ヒートマップ分析から得られたインサイトの概要が表示されます。 • 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 またはスイッチの数。 • 無線あたりのクライアント数が 50 を超えた AP またはスイッチの数。
[Feedback] アイコン	 アイコンをクリックして、このページの情報が役に立ったかどうかについてコメントを入力し、[Submit] をクリックしてください。

[Network Heatmap] ウィンドウ	
アイテム	説明
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で選択した KPI に応じて、KPI のパフォーマンスに関する情報が色のグラデーションで表示されます。濃い色のブロックは、有意な KPI スコアを示します。たとえば、低い RSSI スコアは、高い RSSI スコアよりも有意になります。クライアント数が多いスコアは、クライアント数の少ないスコアよりも有意になります。
[Search AP] ドロップダウンリスト	AP を検索および選択します。 **1.** [Search AP] ドロップダウンリストをクリックし、検索フィルタに AP 名を入力します。 検索した AP がドロップダウンリストで強調表示されます。 **2.** 強調表示された AP をクリックして選択します。 AP の個々の無線が、ヒートマップに個別に表示されます。
[Network Daily Avg]、[Network Daily Min]、または [Network Daily Max] グラフ	選択する [View By] オプションに応じて、該当するグラフが表示されます。 • [Avg] を選択すると、日単位の平均値がグラフに表示され、最も高い日次平均値が強調表示されます。 • [Min]または [Max] を選択すると、日単位の最小値または最大値がグラフに表示され、それらの値がそれぞれ強調表示されます。 グラフのバーにカーソルを合わせると、それぞれの日の KPI 値が表示されます。
[Showing Radios] ヒートマップ	ヒートマップの圧縮ビューが表示されます。 デフォルトでは、この領域には、最初の 100 個の無線のヒートマップが表示されます。その他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。

[Network Heatmap] ウィンドウ	
アイテム	説明
[AP Heatmap] エリア	次の情報が表示されます。 • [Radios in Your Network]：AP の名前とクライアントによって使用された帯域周波数が表示されます。AP の横にあるアイコンをクリックすると、その AP の [Device 360] ウィンドウが開きます。 この領域には、[Band] のオプションで選択した帯域周波数に応じて、該当する帯域の AP が一覧表示されます。 • [AP Heatmap]：AP の動作履歴（1 時間、1 日、1 週間、および月全体）を確認できます。ブロック内の色の明度は、その有意性を示します。濃い色のブロックは、薄い色のブロックよりも有意性が高くなります。ヒートマップの各行が 1 つの AP を表します。 [Heatmap] 内のカラーブロックにカーソルを合わせると、AP に関する情報（名前と MAC アドレス、帯域周波数、場所、日次平均 KPI スコアなど）が表示されます。 • AP Daily Average または AP Daily Max：この領域には、[Sort By] オプションで選択した内容に応じて、各 AP のその月の平均 KPI スコアまたは最大 KPI スコアが表示されます。スコアが最も高い AP がリストの一番上に表示されます。 [AP Daily Average] または [AP Daily Max] 領域にカーソルを合わせると、AP のその月の平均 KPI または最大 KPI の値を確認できます。
Export	CSV ファイルにヒートマップデータをエクスポートするには、[Export] をクリックします。 ヒートマップに適用されている AP とフィルタが、エクスポートされたデータに適用されます。エクスポートは、日単位のビューでのみ有効になり、時間単位のビューでは有効になりません。

ステップ 2 その他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。

ネットワーク内のピアとの KPI 値の比較

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

（注） 比較に使用されるピアネットワークは同程度のサイズです。

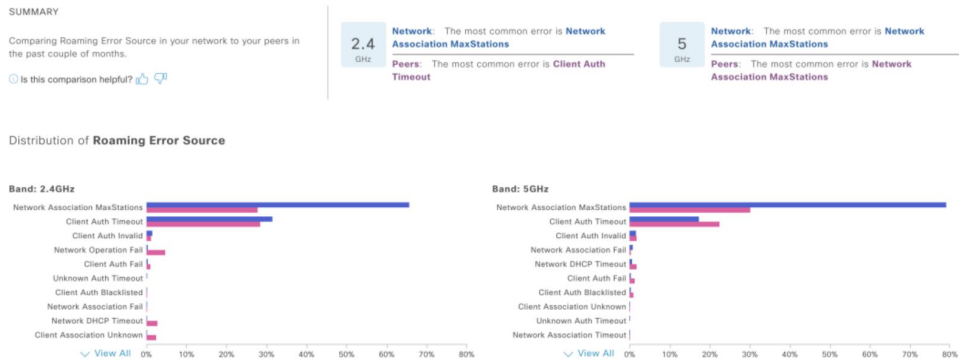
ピア比較では、直近 3 か月間のデータが使用されます。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **[Peer Comparison]** の順に選択します。

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

[Peer Comparison] ウィンドウ	
アイテム	**説明**
[KPI] ドロップダウンリスト	ドロップダウンリストで KPI を選択します。[Radio Throughput]（デフォルト）、[Cloud Apps Throughput]、[Radio Resets]、[Packet Failure Rate]、[Interference]、[Onboarding Error Source]、[Roaming Error Source]、[RSSI] のオプションがあります。
Show	自ネットワークとピアネットワークの間で KPI 値を比較する曜日を選択します。デフォルトは **[All Days]** です。
要約	AIネットワーク分析は、棒グラフを分析し、結果に関する簡単なサマリーを表示します。 • [2.4 GHz]：2.4 GHz 帯域周波数のネットワーク値とピア値のサマリー。 • [5 GHz]：5 GHz 帯域周波数のネットワーク値とピア値のサマリー。 • [6 GHz]：6 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	
アイテム	説明
ピア比較棒グラフ	デフォルトでは、次の図のように、[Band 2.4 GHz] および [Band 5 GHz] のグラフのネットワークでの 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 *57 :* ピア比較棒グラフ**  グラフの色は、次のことを表しています。 • **青**：自ネットワーク。 • **ピンク**：ピアネットワーク。

ステップ 2 自ネットワークとピアネットワークでの特定の日の KPI 値を表示するには、[Show] エリアで該当する日を選択します。

建物、AP モデルファミリ、ワイヤレス エンドポイント タイプの比較

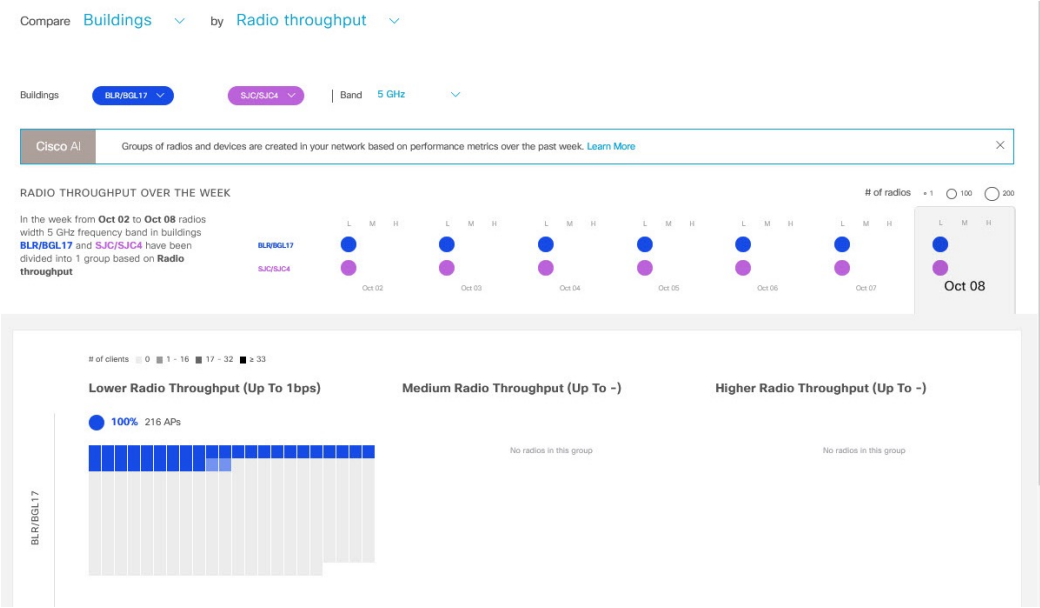
次の手順に従って、選択した重要業績評価指標（KPI）全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリ、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **ネットワークの比較**。

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

図 *58 : [Network Comparison]* ウィンドウ



[Network Comparison] ウィンドウ	
アイテム	**説明**
[Compare] ドロップダウンリスト	比較するネットワーク内のオブジェクトを選択します。次のオプションがあります。 • [Buildings]（サイト） • [AP Model Families] • [Wireless Endpoints]（Android デバイス、Android 携帯、iOS タブレット、iOS 携帯、Linux ワークステーションなど）

[Network Comparison] ウィンドウ	
アイテム	説明
[By KPI] ドロップダウンリスト	ネットワーク内のオブジェクトを比較するために使用する KPI を選択します。 [Buildings] の場合は、次のオプションがあります。 • [Radio Throughput] • [Channel Utilization] • [Average Client RSSI] • [Average Client SNR] • [Average Onboarding Time] • [Average Authorization Time] • [Average DHCP Time] • [Cloud Throughput] • [Media Throughput] • [Social Throughput] • [Interference] [AP Model Families] の場合は、次のオプションがあります。 • [Radio Throughput] • [Interference] • [Media Apps Throughput] • [Average Client RSSI] • [Channel Utilization] • [Average Client SNR] • [Cloud Throughput] • [Social Throughput] [Wireless Endpoints] の場合は、次のオプションがあります。 • [Average AAA Time] • [Average Onboarding Time] • [Average DHCP Time]

[Network Comparison] ウィンドウ	
アイテム	説明
[Buildings] [AP Model Families] または [Wireless Endpoints] ドロップダウンリスト	KPI 値を比較する最初のネットワークオブジェクト（建物、AP モデルファミリ、またはワイヤレスエンドポイント）を選択します。最初のネットワークオブジェクトは青色で表示されます。 KPI 値を最初のネットワークオブジェクトと比較する 2 番目のネットワークオブジェクトを選択します。2 番目のネットワークオブジェクトはピンク/紫色で表示されます。
[Band]	帯域周波数を選択します。[Band 2.4 GHz] または [Band 5 GHz] を選択できます。
[Summary/Timeline]	各ネットワークオブジェクトの曜日ごとの平均 KPI パフォーマンスが表示されます。
[Client Count] のグラデーション または [Device Count] のグラデーション	[Radio Throughput] や [Average Client RSSI] などの KPI については、この領域に各サイトの無線ごとのクライアント数が示されます。 [Onboarding Time] などの KPI については、この領域に各サイトのデバイス数が示されます。 ブロックの色の濃さでクライアント数またはデバイス数が示されます。暗い色のブロックは、薄い色のブロックに比べてクライアント数が多いことを表します。
[AP Clusters] または [Device Type Clusters]	この領域には、各ネットワークオブジェクトに 1 つずつ、2 つのクラスタのセットが表示されます。この領域では、2 つのネットワークオブジェクトのパフォーマンスを視覚的に比較できます。次の情報が提供されます。 • KPI のパフォーマンス（パーセンテージ）。 • ネットワーク内のオブジェクトの各サイトでのクラスタ化方法。 • KPI 値が低、中、高のネットワーク内のオブジェクト。 [Onboarding Time] や [Authorization Time] などの KPI については、このエリアに次のような情報が表示されます。 • 各サイトでクライアントがオンボーディングしたデバイスのタイプ（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 携帯、iOS デバイスなど）。 • 各デバイスタイプの数。 • KPI の時間が低、中、高のデバイスの数。

ステップ 2 クラスタ内の色付きブロックにカーソルを合わせると、日付、AP が存在する建物、AP のモデル番号、無線プロトコル、無線クライアント数など、AP に関する情報が表示されます。濃い色のブロックには、薄い色のブロックよりも多くのクライアントが存在します。

ベースラインを使用したネットワークパフォーマンスの表示と監視

Cisco AI Network Analytics は最先端の機械学習技術を使用して、特定のネットワークとサイトに関するベースラインを定義します。この情報に基づいて、Cisco AI Network Analytics は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判断し、最も重要な問題を特定します。

機械学習アルゴリズムから導出されたベースラインを使用してネットワークパフォーマンスを調査および監視するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Baselines]** の順に選択します。

[Baselines] ダッシュボードが表示されます。

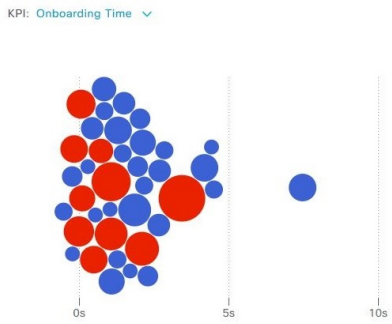
図 *59 : [Baselines]* ダッシュボード



ステップ 2 [Network Overview] ウィンドウで次の情報が表示されます。

[Network Overview] ウィンドウ	
アイテム	**説明**
SUMMARY	ネットワーク内の建物の総数、問題の影響を受ける建物の数、およびネットワーク内の ワイヤレスコントローラ が表示されます。
[AI Driven Issues]	特定のネットワーク環境の予測ベースラインからの乖離度に基づいてトリガーされ、Cisco AI Network Analytics によって検出された問題が表示されます。

[Network Overview] ウィンドウ	
アイテム	説明
 [Location] ドロップダウンリスト	ロケーションアイコンをクリックしてスライドインペインを開き、サイトまたは建物を選択します。ダッシュボード上の情報が、選択に応じて更新されます。
 [Time Range] の設定	ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次のタスクを実行します。 • ドロップダウンメニューで範囲の長さ（[24 hours] または [Custom Range]）を選択します。 • 開始日と終了日を指定します。 • [Apply] をクリックします。
[KPI] ドロップダウンリスト	ドロップダウンリストで KPI を選択します。次のオプションがあります。 • [Onboarding Time]（デフォルト） • [Onboarding Failures] • [DHCP Time] • [Authentication Time] • [Association Failures]
 [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、ネットワークの地理的位置に基づいたマップビューに表示されます。
 [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。

[Network Overview] ウィンドウ	
アイテム	説明
 [Beeswarm Chart]	このトグルボタンをクリックすると、選択したKPIに従ってネットワークのクライアントデバイスのパフォーマンスに関するインサイトを提供する蜂群チャートが表示されます。  この場合、蜂群チャート内のエンティティは建物であり、円で表されます。 蜂群チャート内の各円は、次のことを表しています。 • **青**：円は建物を表します。チャート内の円の上にカーソルを合わせると、ロケーション、KPI、SSID、ワイヤレスコントローラ、クライアント数などの情報が表示されます。 • **赤**：円は、問題の影響を受ける建物を表します。チャート内の円の上にカーソルを合わせると、ロケーション、KPI値、SSID、ワイヤレスコントローラ、クライアント数、AIに起因する問題などの情報が表示されます。 • 円のサイズは、接続されているクライアントの数を表します。小さな円には少数のクライアントが、大きな円には多数のクライアントが含まれます。

ステップ3 蜂群チャートで円をクリックすると、次の情報の建物ビューが表示されます。

建物ビュー
サイトまたは建物の特定の情報が表示されます。それぞれのドロップダウンリストからKPI、SSID、および ワイヤレスコントローラ を選択して、データを表示できます。 タイムラインスライダで、タイムラインの境界線をクリックしてドラッグすると、より詳細な時間範囲を指定できます。 タイムラインスライダの下にある色分けされたチャートを使用して、ネットワークのパフォーマンスを判断します。指定した期間内の選択したKPIの予測ベースラインからの偏差に基づいて問題を表示します。チャートの上にカーソルを移動して合わせて、選択した時点での期間、予測上限範囲と予測下限範囲を表示する同期化されたツールチップを表示します。 色分けは、次のことを表しています。 • **赤**は AI 駆動型の問題を表します • **青**は平均 KPI 期間を表します • **緑**は予測 KPI を表します [View Details] をクリックすると、追加の詳細情報が記載された スライドインペイン が開きます。その内容は、KPI チャートで選択されている KPI によって異なります。スライドインペイン には、平均 KPI 期間（[Onboarding Time]、[DHCP Time]、[Onboarding Failures]、[Authentication Time] など）および一意のクライアントが色分けされたチャートが表示されます。 サンキーグラフは、フロアとデバイスタイプ（クライアントデバイス）間の主要なフローを強調するために表示されます。チャートの下に、AP 名、オンボーディング、失敗したオンボーディング、失敗したオンボーディングの割合、クライアント数などが表示されます。 （注） テーブルに表示されるクライアント数は、30分間に観測された個々のクライアント数の測定値における、選択された時間間隔での平均です。

AI 拡張 RRM ダッシュボードを使用した RF ネットワークの表示

Cisco AI Network Analytics は、機械学習アルゴリズムを使用して、拡張無線リソース管理（RRM）が有効になっている建物内の無線周波数（RF）ネットワークの動作を定義します。

始める前に

- Assurance は、ユーザーのアクセス範囲を制限するサイトベースのロールベースアクセス制御（SRBAC）をサポートしています。[AI-Enhanced RRM] ダッシュボードを使用している間は、サイトとデバイスにアクセスできることを確認する必要があります。ユーザー

ロールと権限の詳細については、『Cisco Catalyst Center Administrator Guide』を参照してください。

- AI 活用型 RRM ダッシュボードを表示するには、AI RF プロファイルに場所を割り当てる必要があります。詳細については、『*Cisco Catalyst Center User Guide*』の「**Assign Location to an Existing AI RF Profile**」[英語] を参照してください。
- AI 活用型 RRM インサイトにアクセスするには、AI RF プロファイルに割り当てられた場所全体にデバイスをプロビジョニングする必要があります。詳細については、『*Cisco Catalyst Center User Guide*』の「**Provision Wireless Devices**」[英語] を参照してください。
- Cisco AI 活用型 RRM は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS XE 17.7.1 以降でのみサポートされています。
- [Run RRM Simulation]、[Insights]、および [Service Bundle] オプションが使用できるのは、スーパー管理者またはネットワーク管理者のみです。

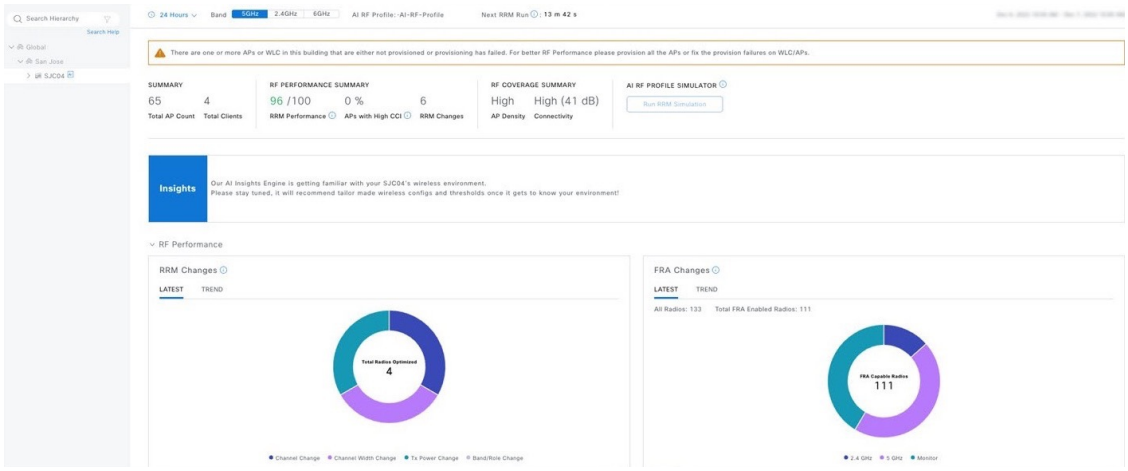
手順

ステップ 1 メインメニューから次を選択します。**[AI-Enhanced RRM]** > **[AI-Enhanced RRM]**の順に選択します。

ステップ 2 左ペインで、[Find Hierarchy] フィールドに名前を入力してサイトを検索するか、[Global] を展開してサイトを選択します。

[AI-Enhanced RRM] ダッシュボードが表示されます。

図 *60 : [AI-Enhanced RRM]* ダッシュボード



ステップ 3 次の機能には、[AI-Enhanced RRM] ダッシュボードの上部のメニューバーを使用します。

アイテム	説明
[Time Range]	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。使用可能な時間範囲は、[24 Hours]、[7 Days]、または [14 Days] です。

アイテム	説明
[Band]	[2.4GHz] 帯域、[5GHz] 帯域、[6GHz] 帯域を切り替えて、特定の帯域のデータを表示できます。
[AI RF Profile]	建物に割り当てられている現在の AI RF プロファイルを表示します。
[Next RRM Run]	AI 拡張 RRM の計算は 30 分ごとに発生します。RRM の決定は、計算後に更新され、デバイスにプッシュされます。

ステップ 4 [Summary] ダッシュレットを使用して、次の情報を確認できます。

アイテム	説明
Summary	ネットワーク内の AP 数とクライアントの総数を表示します。 ライセンス要件を満たしていない AP がある場合、このダッシュレットには、動作していない帯域の非準拠 AP の数を示す アイコンが表示されます。対応するハイパーリンクをクリックすると、詳細を含むダイアログボックスが表示されます。 ダイアログボックスで、[License Manager] をクリックして [License Manager] ウィンドウを開き、必要なライセンスを有効にすることができます。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Manage Licenses」を参照してください。
[RF PERFORMANCE SUMMARY]	• [RRM Performance]：同一チャネル干渉、ノイズ、SNR、無線使用率など、いくつかの KPI に基づいた複合メトリックを表示します。 • [APs with High CCI]：同一チャネル干渉が高い AP の割合を示します。 • [RRM Changes]：RRM チャネル変更、チャネル帯域幅変更、および Tx 電力変更イベントの合計数を時刻別に表示します。
[RF COVERAGE SUMMARY]	• [AP Density]：RF カバレッジの AP の密度を低、中、または高で示します。 • [AP Density]：RF カバレッジ内の AP の接続性を示します。

ステップ 5 [AI RF Profile Simulator] で、[Run RRM Simulation] をクリックして、RF 構成をシミュレートし、影響を視覚化し、RF プロファイルを作成します。

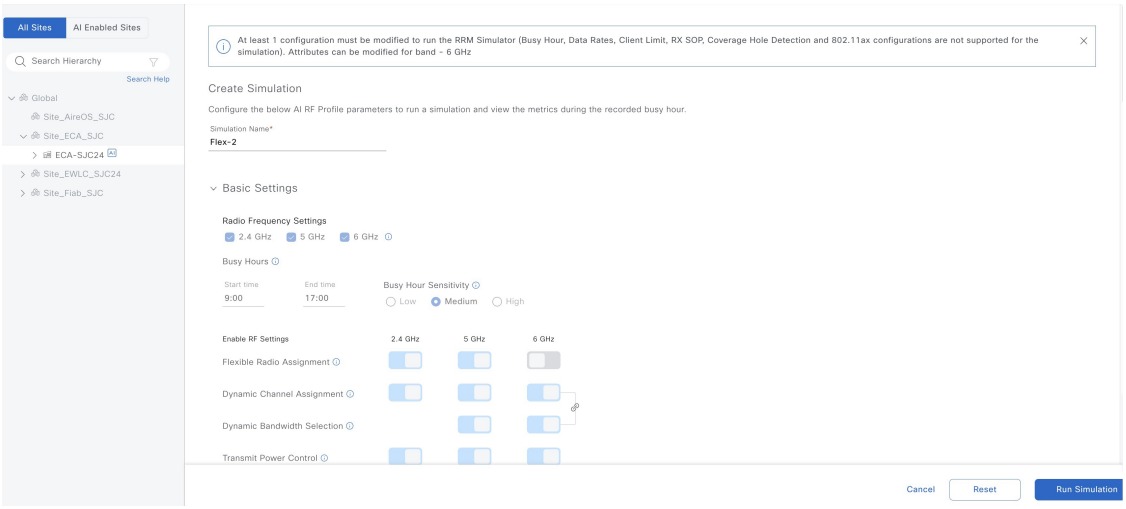
AI RF プロファイルシミュレータを使用すると、現在の RF プロファイルへの変更をシミュレートし、AI 活用型 RRM ダッシュレットに対して予測される結果を視覚化できます。

（注） RRM シミュレーションは、AI RF プロファイルで選択した無線帯域に基づいて実行され、シミュレータで変更することはできません。

a) [Welcome to RRM Simulator] ウィンドウで [Create Simulation] をクリックします。

現在の AI RF プロファイル情報が表示されます。

図 *61* : シミュレーションウィンドウの作成



b) 必要に応じて、シミュレーションに選択した帯域の下で属性を変更して、メトリックを表示できます。

（注）
- 5 GHz の場合、[Busy Hour]、[Data Rates]、[Client Limit]、[RX SOP]、[Zero Wait DFS]、[Coverage Hole Detection]、[802.11ax] などの属性は、シミュレーションでは考慮されません。
- 2.4 GHz の場合、[Busy Hour]、[Data Rates]、[Client Limit]、[RX SOP]、[Coverage Hole Detection]、[802.11 ax] などの属性は、シミュレーションでは考慮されません。
- 6 GHz の場合、[Busy Hour]、[Data Rates]、[Client Limit]、[RX SOP]、[Coverage Hole Detection]、[802.11 ax]、[802.11be] などの属性は、シミュレーションでは考慮されません。

c) [Reset] をクリックして、AI RF プロファイル属性値を対応するベース AI RF プロファイル値に変更します。

d) [Run Simulation] をクリックします。

（注） AI RF プロファイル属性を変更してからシミュレーションを実行してください。

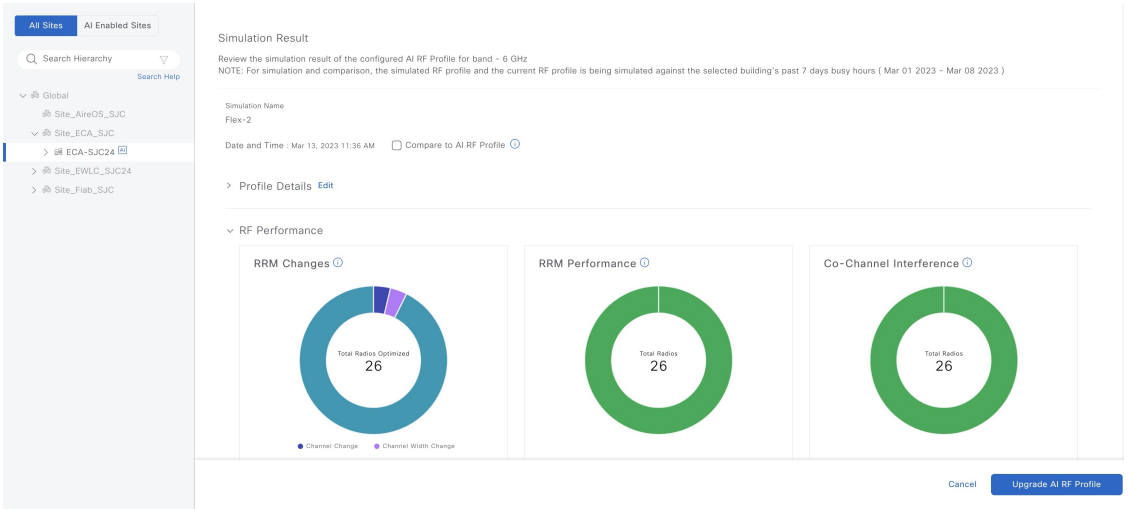
「Simulation in Progress」のメッセージが表示されます。

e) [Simulation Result] ウィンドウで、選択した帯域の AI RF プロファイルに設定されたシミュレーションを確認します。

- [Simulation Name]
- [Profile Details]
- [RF Performance]
- [RF Coverage]

AI RF プロファイル属性を編集するには、[Profile Details] エリアの [Edit] オプションをクリックします。

図 *62 : [Simulation Result]* ウィンドウ



f) シミュレートされた AI RF プロファイル構成と現在適用されている AI RF プロファイル構成を比較するには、[Compare to AI RF Profile] チェックボックスをオンにします。

g) [Upgrade AI RF Profile] をクリックします。

h) AI RF プロファイルが複数の場所に割り当てられている場合は、新しいプロファイル名を入力して [Save] をクリックすることにより、新しい RF プロファイルを推奨設定で作成し、割り当てます。

i) [Apply RRM Simulation Settings] ウィンドウで、展開するタスクをスケジュールします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。

（注） 即時展開またはスケジュール済み展開のタスクを送信した後、AI RF プロファイルの割り当てられた場所に基づいて、[Upgrading AI RF Profile] ダイアログボックスで必要な編集を行います。

- AI RF プロファイルが複数の建物に割り当てられている場合、新しい RF プロファイルが作成され、RF プロファイル名とタスク名を編集できます。
- AI RF プロファイルが 1 つの建物に割り当てられている場合、タスク名は編集できますが、RF プロファイル名は編集できません。

- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

（注） AI RF プロファイルをアップグレードすると、AP は ワイヤレスコントローラ とのアソシエーションを一時的に失い、クライアント接続が中断する可能性があります。

j) [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 6 [Insights] ダッシュレットを使用して、AI 活用型 RRM によって生成されたインサイトを確認します。インサイトは、AI RF プロファイルに適用できる構成の推奨事項です。

[Insights] ダッシュレットには、次の考えられるインサイトが表示されます。

- [Busy Hours]
- [Channel Width]
- Channel List
- [Enable FRA]
- 優先スキャンチャネル
- TPC しきい値

ステップ 7 [Insights] アイコンをクリックして、シスコが推奨するインサイトを表示します。

a) [Review Cisco AI Recommendations] ウィンドウで、選択したサイトで使用可能な推奨事項から AI RF プロファイルの設定を確認してチェックボックスをオンにします。
b) [Apply] をクリックします。
c) AI RF プロファイルが複数の場所に割り当てられている場合は、新しいプロファイル名を入力して [Save] をクリックすることにより、新しい RF プロファイルを推奨設定で作成し、割り当てます。
d) [Apply RRM Simulation Settings] ウィンドウで、展開するタスクをスケジュールします。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

（注） AI RF プロファイルをアップグレードすると、AP は ワイヤレスコントローラ とのアソシエーションを一時的に失い、クライアント接続が中断する可能性があります。

e) [Tasks] ウィンドウで、タスクの展開を監視します。

ステップ 8 次の機能のために [RF Performance] を展開します。

アイテム	説明
[RRM Changes] ダッシュレット	次の 2 つのタブがあります。 • [LATEST]：過去 30 分間の RRM チャネル変更、チャネル帯域幅変更、Tx 電力変更、帯域またはロール変更イベントの合計数を表示します。 • [TREND] ：時間範囲内で選択された時間に AP に行われたチャネル変更、チャネル帯域幅変更、Tx 電力変更、帯域またはロール変更イベントを表示します。 （注） • 帯域やロールの変更イベントは、**6 GHz** 帯域を対象としていません。 • チャネル帯域幅の変更イベントは、**2.4 GHz** 帯域を対象としていません。 グラフのいずれかの色のセグメントをクリックするか、[View Details] リンクをクリックして、[RRM Changes] を開きます。スライドインペイン **1.** グラフの色のセグメントにカーソルを合わせると、[Change Category] と [Total Affected APs] が表示されます。 **2.** グラフのセグメントをクリックして、チャートの下に表示される [Access Points] テーブルのデバイスデータを表示します。 • 無線機 • [Change Category] **3.** AP の横にあるオプションボタンをクリックして、RRM によって管理される変更カテゴリの [Event Reasoning] を表示します。 （注） [Access Points] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 **4.** [Export] をクリックして、AP テーブルデータをローカルマシンにダウンロードします。

アイテム	説明
[FRA Changes] ダッシュレット	次の無線モードについて、無線、フレキシブルラジオアサインメント（FRA）対応無線、およびFRA無線の合計数を表示します： • 2.4 GHz • 5 GHz • Monitor （注） FRA は 6 GHz を対象としていないため、**6 GHz** 帯域の場合、[FRA Changes] ダッシュレットは表示されません。 次の 2 つのタブがあります。 • [LATEST]：FRA 対応無線および FRA 無線の総数を表示します。また、2.4 GHz と 5 GHz 帯域での FRA 対応無線の移動を表示し、無線モードを監視します。 • [TREND]：2.4 GHz、5 GHz 帯域の FRA 無線の数を表示し、時間範囲で選択した時間内の無線モードを監視します。 グラフのいずれかの色のセグメントをクリックするか、[View Details] リンクをクリックすると、[FRA Changes Details] が開きます。スライドインペイン **1.** グラフの色のセグメントにカーソルを合わせると、対応する無線モードの中から FRA 無線の数が表示されます。 **2.** APデバイスデータは、グラフの色の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 [Radios] テーブルに表示されます。 • AP Name • Slot ID • COF % • 推奨モード • チャネル （注） [Radios] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 **3.** [Export] をクリックして、データをローカルマシンにダウンロードします。

アイテム	説明
[RRM Performance] ダッシュレット	次の 2 つのタブがあります。 • [LATEST]：過去 30 分間の [Poor]、[Fair]、および [Good] AP 正常性スコアに寄与した AP の総数を表示します。 • [TREND]：時間範囲内の AP カウントと選択された時間の割合について、AP の [Poor]、[Fair]、および [Good] RRM 正常性スコアを表示します。 グラフのいずれかの色のセグメントをクリックするか、[View Details] リンクをクリックして、[RRM Health] を開きます。スライドインペイン **1.** グラフの色のセグメントにカーソルを合わせると、AP とその無線の [Fair]、[Poor]、および [Good] RF パフォーマンススコアが表示されます。 **2.** グラフの色のセグメントをクリックして、チャートの下に表示される [Access Points] テーブルのデバイスデータを表示します： • AP Name • Slot ID • Neighbor • Interference • Noise • クライアント （注） [Access Points] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 **3.** [Export] をクリックして、AP テーブルデータをローカルマシンにダウンロードします。

アイテム	説明
[Co-Channel Interference] ダッシュレット	次の 2 つのタブがあります。 • [LATEST]：過去 30 分間に [Low]、[Medium]、[High] の同一チャネル干渉が発生している AP の総数を表示します。 • [TREND]：時間範囲内の AP カウントと選択された時間の割合について、AP の [Low]、[Medium]、[High] の同一チャネル干渉の割合を示します。 グラフの色のセグメントまたは [View Details] リンクをクリックして、[Co-Channel Interference] を開きますスライドインペイン。 **1.** グラフの色のセグメントにカーソルを合わせると、AP の [Low]、[Medium]、[High] の同一チャネル干渉が表示されます。 **2.** グラフの色のセグメントをクリックして、チャートの下に表示される [Access Points] テーブルのデバイスデータを表示します： • AP Name • Slot ID • チャネル • 影響スコア • CCI（dBm） • Duty Cycle （注） [Access Points] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 **3.** [Export] をクリックして、AP テーブルデータをローカルマシンにダウンロードします。

アイテム	説明
[Utilization Per Channel] ダッシュレット	使用率チャートを表示します。 6 GHz 帯域の場合、使用率チャートは、[View by] ドロップダウンリストで選択した UNII レベルに基づきます。UNII レベルは、[PSC]、[UNII 5]、[UNII 6 & 7]、および [UNII 8] です。デフォルトのビューは [PSC] です。 [LATEST] タブには、過去 30 分間に同一チャネル干渉が発生している AP の総数が表示されます。 詳細を表示するには、チャートにカーソルを合わせます。 • チャネル番号（Channel Number） • 使用率 • インターフェイス • 最大使用率 • 最小使用率 [TREND] タブには、時間範囲内の使用率と選択された時間の割合に関するチャネルごとの使用率の詳細が表示されます。 （注） [Select Channel] ドロップダウンリストでは、名前を入力してチャネルを検索するか、リストからチャネルを選択して詳細を表示できます。
[AP and Radar per Channel] ダッシュレット	5 GHz 帯域のチャネルごとの AP およびレーダー情報を表示します。 [LATEST] タブには、過去 30 分間の AP およびチャネルのチャートに、チャネルごとの AP およびレーダーの詳細が表示されます。 チャートにカーソルを合わせると、5-GHz 帯域に関する以下の詳細が表示されます。 • チャネル数 • 無線の数 • チャネルごとのレーダーイベントの数 [Trend] タブには、選択したチャネルの無線およびレーダーイベントの数が表示されます。

アイテム	説明
[AP and Radar per Channel] ダッシュレット	2.4 GHz および 6 GHz 帯域のチャネルごとの AP 情報を表示します。 [LATEST] タブには、チャネル番号とそのチャネル上の無線の数が表示されます。 詳細を表示するには、チャートにカーソルを合わせます。 • チャネルの数 • Tx/Rx の使用率 • Interference [TREND] タブには、選択したチャネルの無線の数が表示されます。

ステップ 9 次の機能のために [RF Coverage] を展開します。

アイテム	説明
[AP Spatial Density] ダッシュレット	

アイテム	説明
	AP の空間密度の値は、インフラストラクチャ内で選択した AP のネイバーである -70 dBm 以上の AP の数を表します。AP の密度は、チャネル、チャネル幅、および Tx 電力の最適な実効値に影響します。 • [LATEST]：インフラストラクチャ内の選択された AP のネイバーである AP の数を、過去 30 分間の無線数の割合、AP ネイバーの密度、およびクライアント数の割合について示します。 以下を表示するには、チャートにカーソルを合わせます。 • AP ネイバー密度 • [Radio Count] • [クライアント カウント（Client Count）] • [TREND]：時間範囲内の AP 数と選択した時間の平均隣接密度数と無線数を表示します。 平均隣接密度範囲は、[<5]、[5-10]、[10-15]、[15-20]、[20-25]、および [>=25] です。 グラフのいずれかの色のセグメントをクリックするか、[View Details] リンクをクリックすると、[AP Spatial Density Details] が開きます。スライドインペイン 1. グラフ内の色のセグメントをクリックして、[Top APs] グラフをネイバー密度の低/高別に表示し、[Access Points] テーブルの次のデバイスデータを表示します。 • AP Name • Slot ID • ネイバー密度メトリック • 合計 Rx ネイバー • チャネルネイバー RSSI で最高 • チャネルネイバーの合計 （注） [Access Points] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 2. [Top APs] エリアで、ドロップダウンリストをクリックして、最も低いネイバー密度または最も高いネイバー密度で上位 AP を選択します。 3. [Top APs] チャートにカーソルを合わせると、AP およびネイバーカウントのチャートに [Min]、[Max]、および [Latest] の AP が表示されます。

アイテム	説明
	4. [Export] をクリックして、AP テーブルデータをローカルマシンにダウンロードします。

アイテム	説明
[Power Distribution] ダッシュレット	

アイテム	説明
	電力分布チャートは、環境内の物理的な Wi-Fi カバレッジエリアを視覚化するのに役立ちます。また、最大および最小の電力レベルで動作している AP を特定することもできます。 [Filter] ドロップダウンリストで選択した [Power Level] または [Power dBm] に基づいてデータを表示できます。 • [LATEST]：過去 30 分間に、さまざまな電力レベルで動作している AP の数と、無線数の割合とネイバー数の割合が表示されます。 • 以下を表示するには、チャートにカーソルを合わせます。 • [Operating Power Level]（電力レベルビュー用） • [Operating Power dBm]（電力 dBm ビュー用） • 無線数 • Neighbor Count • [TREND]：時間範囲内の動作電力レベル、無線数、および選択された時間を表示します。 カーソルを傾向チャートに合わせると、さまざまな電力レベルで動作している無線数の割合が表示されます。 電力レベルは、[Level 1]（最大電力レベル）から [Level 8]（最小電力レベル）まで計算されます。 グラフの色のセグメントをクリックするか、[View Details] リンクをクリックすると、[Power Distribution Details] が開きます。スライドインペイン 1. グラフの色のセグメントをクリックしすると、ネイバー密度の低/高別で表示された [Top APs] グラフと、以下のデバイスデータが [Radios] テーブルに表示されます。 • AP Name • Slot ID • カバレッジホール数 • 送信電力（dBm） • Neighbor Count • ネイバー密度メトリック • デルタ平均ネイバー送信電力（dB） 6 GHz 帯域の場合、[Power dBm] を使用してデータをフィルタリングすると、次のデバイス データが [Radios] テーブルに表示されます。

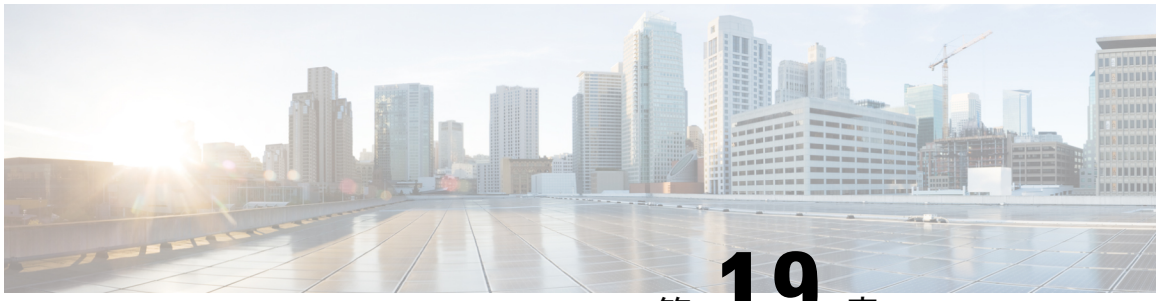
アイテム	説明
	• AP Name • Slot ID • カバレッジホール数 • 送信電力（dBm） • Neighbor Count • ネイバー密度メトリック • デルタ平均ネイバー送信電力（dB） • チャネル幅（MHz） （注） [Access Points] テーブルで、マウスカーソルを [i] アイコンの上に置くと詳細が表示されます。 2. [Export] をクリックして、AP テーブルデータをローカルマシンにダウンロードします。

ステップ 10 [Additional Site Level Information] を展開して、サービスバンドルをダウンロードします。

ステップ 11 [Service Bundle] エリアで、[Request a Latest Service Bundle] リンクをクリックして、選択した建物の過去 1 時間のサービスバンドルをダウンロードします。

ステップ 12 過去 14 日間のサービスバンドルデータをダウンロードするには、[SELECT A PERIOD TO DOWNLOAD] エリアで [Start Date] と [Start Time] および [End Date] と [End Time] を指定し、[Download Service Bundle] をクリックします。

選択した期間に RRM アルゴリズムに使用される構成パラメータと RRM テレメトリを含むサービスバンドルがローカルマシンに保存されます。このサービスバンドルは、Cisco Technical Assistance Center（TAC）でトラブルシューティングに使用することがあります。



第 19 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 （479 ページ）
- インテリジェントキャプチャのサポート対象デバイス （480 ページ）
- インテリジェントキャプチャのベストプラクティス （480 ページ）
- インテリジェントキャプチャの設定方法と使用方法 （481 ページ）
- 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 （518 ページ）

インテリジェントキャプチャについて

Catalyst Center では通常、デバイスとクライアントの正常性に関するすべての情報を シスコ ワイヤレス コントローラから利用できます。インテリジェントキャプチャ（iCAP）は、Catalyst 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 Catalyst Center と直接通信できます。Catalyst 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。Catalyst Center と AP 間の直接通信リンクを利用することで、iCAP は ワイヤレスコントローラからは利用できないデータに AP からアクセスできるようになります。

iCAP 機能が効果的に機能できるようにするには、AP が Catalyst Center への接続を確立する必要があります。AP と Catalyst Center の間にファイアウォールが存在する場合は、次の TCP ポートを開いておきます。

- TCP 443：Catalyst Center の iCAP への HTTPS 接続を開始するために AP によって使用されます。
- TCP 32626：Cisco Catalyst Assurance iCAP 機能に関連する AP/クライアント統計情報およびパケットキャプチャデータの受信用の gRPC チャネルを確立するために使用されます。

（注）
- iCAP は、ローカルモードまたは FlexConnect モードの AP でのみサポートされます。
- iCAP は、SDA 展開ではサポートされていません。

インテリジェントキャプチャのサポート対象デバイス

インテリジェントキャプチャ（iCAP）をサポートする ワイヤレスコントローラ および AP の詳細については、「Feature Matrix for Cisco Wireless Access Points」を参照してください。

インテリジェントキャプチャのベストプラクティス

Catalyst Center でインテリジェントキャプチャ（iCAP）機能を確実に最適化するためのベストプラクティスを以下に示します。

- 新しい ワイヤレスコントローラ デバイスを Catalyst Center に追加したら、すべての iCAP グローバル設定を無効にしてから再度有効にして、新しい ワイヤレスコントローラ に設定されるようにします。
- Catalyst Center から ワイヤレスコントローラ デバイスを削除する前に、すべての iCAP 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 Catalyst Center の再イメージ化を行う前に、すべての iCAP 設定を無効にし、アップグレード完了後に再度有効にします。
- ワイヤレスコントローラをインベントリから削除する場合は、[設定のクリーンアップ（Clean Up Configuration）] オプションを選択します。この操作により、すべての iCAP 設定がコントローラおよびその関連 AP から削除されます。古いデータが原因で、このプロセス中にエラーが発生した場合は、削除を再試行してください。
- AP を廃止するか RMA を実行する前に、[アシュアランス（Assurance）] > [インテリジェントキャプチャの設定（Intelligent Capture Settings）]>[アクセスポイント（Access Point）] の順に選択します。[AP統計情報のキャプチャ（AP Stats Capture）]および[異常キャプチャ（Anomaly Capture）] ウィンドウを確認します。キャプチャモードが [特定：特定のAPを選択（Specific - select specific APs）] に設定されている場合は、削除する特定の AP に対して iCAP を無効にしてください。
- アップグレードを開始する前に、[アシュアランス（Assurance）]>[インテリジェントキャプチャの設定（Intelligent Capture Settings）] > [ワイヤレスパケットキャプチャ（Wireless Packet Capture）] および [OTAスニファキャプチャ（OTA Sniffer Capture）] でキャプチャセッションのステータスを確認します。いずれかのセッション（ICAP フル、オンボーディング、スペクトル、または OTA）が進行中の場合は、アップグレードを続行する前に、これらのセッションが終了するのを待ちます。

インテリジェントキャプチャの設定方法と使用方法

クライアントデバイスのオンボーディング パケット キャプチャ

クライアントデバイスのオンボーディング パケット キャプチャについて

オンボーディングパケットキャプチャセッションは、クライアントデバイスがワイヤレスネットワークに参加するために使用するパケット（802.11 管理フレーム、DHCP、EAP パケットなど）をキャプチャし、クライアントの RF 統計（5 秒のサンプル）を収集します。そのデータは **[Client 360]** > **[Intelligent Capture]** ウィンドウに表示されます。セッションは、すぐに開始することも、後で実行するようにスケジュールすることもできます。セッションのデフォルトの持続時間は 30 分で、最大 8 時間まで設定できます。デフォルトでは、オンボーディング パケット キャプチャは、最後にクライアントに接続した ワイヤレスコントローラ で有効になっています。クライアントローミング シナリオに対応する ワイヤレスコントローラ を 3 つまで選択できます。

（注）

- 「クライアント スケジュール キャプチャ」は「オンボーディング パケット キャプチャ」に名前が変更されました。この名称を合理化する過程で、さまざまな販促アイテムで以前の名前とブランド変更された名前が使用される場合があります。ただし、「クライアント スケジュール キャプチャ」と「オンボーディング パケット キャプチャ」は同じ機能を指します。
- 「ライブキャプチャ」、「スケジュール済みキャプチャ」、および「オンボーディングパケットキャプチャ」はすべて同じ機能を指します。これらの名前は、さまざまな販促アイテムで同じ意味で使用されます。

オンボーディング パケット キャプチャ セッションの制限事項

オンボーディング パケット キャプチャ セッションには次のような制限事項があります。

- 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、各クライアントは最大 3 つのワイヤレスコントローラで有効にできます。

  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、エラーメッセージが表示されます。最大タイムスロット制限に達したときに別のキャプチャセッションをスケジュールするには、実行中のキャプチャセッションを停止するか、キャプチャセッションが完了するまで待機します。その後、新しいキャプチャセッションを開始できます。

（注） 16 個のタイムスロット制限は ワイヤレスコントローラによって適用されます。

キャプチャセッションが Catalyst Center に対して設定されている場合、Catalyst Center が認識していないライブキャプチャセッションやスケジュール済みのキャプチャセッション（ワイヤレスコントローラに対して直接設定された部分的なパケット キャプチャセッションなど）はすべて削除されます。

- 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。
- Catalyst Center に格納するすべてのスケジュール済みオンボーディング パケット ファイルの合計サイズには、3.5 GB の制限があります。制限を超えると、合計サイズが 3.5 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。さらに、合計サイズの制限に達していなくても、14 日間超経過したオンボーディング パケット ファイルは削除されます。

クライアント統計情報について

グローバル設定のオンボーディング パケット キャプチャ セッションを使用すると、サポート対象の AP でクライアント統計情報を 5 秒間隔で収集できます。

クライアント統計情報は、クライアントが接続されている AP で AP 統計が有効になっている場合にも 30 秒間隔で収集されます。

クライアント統計情報が収集されると、**[Client 360]** > **[Intelligent Capture]** ウィンドウの 4 つの RF 統計情報チャートに表示されます。

クライアントデバイスのライブ オンボーディング パケット キャプチャ セッションの実行

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。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

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

ステップ 3 次のいずれかを行うと、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] フィールドに、次のいずれかの要素を入力します。
  - ユーザー ID（Cisco ISE により認証）
  - 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 AP がインテリジェント キャプチャ データを Catalyst Center に送信できない （518 ページ） で詳細を確認してください。

図 *63* : クライアントの *[Intelligent Capture]* ウィンドウ



ステップ 5 タイムラインスライダは次の機能に使用できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。
タイムラインスライダ	タイムラインスライダは、表示されるすべてのデータの時間枠を決定します。ライブキャプチャの結果については、オンボーディングイベントの折れ線グラフが表示されます。緑色はオンボーディングイベント、赤色は異常イベントを示します。 タイムラインを別の時間枠に調整するには、目的の時間枠になるまで [<] ボタンと [>] ボタンをクリックします。 （注） タイムラインには、最長で過去 2 週間のデータを表示できます。 タイムラインの範囲をさらにカスタマイズするには、境界線をクリックしてドラッグします。

ステップ 6 ライブキャプチャセッションを行うには、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 Live Capture] ボタンをクリックします。

c) 実行中のライブキャプチャセッションは、クライアントの [Intelligent Capture Settings] ウィンドウで確認できます。

ステップ 7 ネットワーク接続の確立に関連付けられているイベントを表示するには、[Onboarding Events ダッシュレットを使用します。

[Onboarding Events] ダッシュレット	
アイテム	**説明**
[All] および Anomaly PCAP フィルタ	オンボーディングイベントをフィルタ処理できます。次のオプションがあります。 • [All]：すべてのイベントを表示します。これはデフォルトです。 • Anomaly PCAP：パケットがある異常イベントのみをフィルタ処理します。 （注） クライアントがネットワークに参加する際に問題が発生した場合は、特定のイベントの横に「PCAP」という語が赤色で表示されます。 クライアントが問題なくネットワークに参加できる場合は、特定のイベントの横に「PCAP」という語が灰色で表示されます。

[Onboarding Events] ダッシュレット	
アイテム	説明
Export PCAP	指定されたイベントの範囲のパケットをダウンロードできます。 **1.** [Export PCAP] をクリックします。 **2.** PCAP に含める最初と最後のイベントを指定します。 **3.** ダウンロードを開始するには、[Download PCAP] ボタンをクリックします。 （注） ヒューリスティックを使用してイベントに属するパケットを判断するため、最初のイベントの 1 分前と最後のイベントの 1 分後のパケットがダウンロードに含まれます。これにより、すべての関連するパケットがダウンロードされた PCAP に含まれるようになります。 各エクスポートに含まれるのは、最もタイムスタンプが古いものから 2000 パケットまでに制限されます。
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。イベントは色分けされて以下のことを示しています。 ● : 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） 「PCAP」という単語が横に表示されているイベントは、そのイベントのデータパケットがダウンロードまたは分析のためにキャプチャされていることを示します。 親イベントグループをクリックすると、グループを展開して、そのグループの個々のイベントを表示できます。

[Onboarding Events] ダッシュレット	
アイテム	説明
Event Details	イベントグループまたは個々のイベントをクリックすると、次のセクションでさらに詳細情報を表示できます。 [Client Location]：イベント中のクライアントの場所のマップとクライアントの移動のマップが表示されます。 [Auto Packet Analyzer]：このセクションは、ライブキャプチャ、スケジュールされたキャプチャ、または異常キャプチャセッションがイベントのパケットをキャプチャした場合に表示されます。イベントの横に表示される「PCAP」という単語は、そのイベントがパケットをキャプチャしたことを示します。 [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、フロアマップおよび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。
- カバレッジの強度を色の濃淡で視覚化したヒートマップ
- 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。

  マップ上の次の色でクライアントの正常性が表されています。

  ● : 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。
- マップの下にある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 Catalyst 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 （533 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。

AP クライアント統計情報を表示する 4 つのチャート。詳細については、「クライアント統計情報について（482 ページ）」を参照してください。データは色分けされていて、次の情報が含まれています。

- RSSI および SNR の測定値（デシベル単位）。
- Rx 平均データレート（直近の 5 秒間）および Rx 最新データレート。
- Tx パケットおよび Rx パケット。
- Tx パケットの再試行。

ダッシュレットに表示されるチャートでは、次の操作を行うことができます。

- 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。

クライアントデバイスのオンボーディングパケットキャプチャセッションのスケジュール

クライアントデバイスのオンボーディング パケット キャプチャ セッションをスケジュールできます。

オンボーディング パケットキャプチャ セッションでは次のデータが収集されます。

- オンボーディングイベントのデータパケットおよび [RF Statistics] チャートデータ（5 秒のサンプル）が **[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のライブ オンボーディング パケット キャプチャ セッションの実行 （482 ページ）を参照してください。
- チャートおよびテーブルのデータが **[Device 360]** > **[Intelligent Capture]** ウィンドウに表示されます。AP の RF 統計の表示 （502 ページ）およびAP のスペクトル解析データの表示（511 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

[Onboarding Packet Capture] ウィンドウが表示されます。

ステップ 2 **[+ Schedule Client Capture]** をクリックします。

（注） 既存のオンボーディング パケットキャプチャ タスクが完了していない場合に、同じ ワイヤレスコントローラ で新しいパケットキャプチャ セッションを開始しようとすると、未完了のタスクの競合が原因で失敗します。新しいタスクを開始するには、既存のタスクが完了するまで待つか、既存のタスクを破棄します。

ステップ 3 [Schedule Client Capture] スライドインペイン で、次の手順を実行します。

1. [Select client devices] ドロップダウンリストで、クライアントデバイスを選択します。
2. [Duration] ドロップダウンリストで、オンボーディング パケット キャプチャ セッションの期間を選択します。

   デフォルトの時間は、30 分です。
3. オンボーディング パケット キャプチャを有効にする ワイヤレスコントローラ の横にあるチェックボックスをオンにします。

   ワイヤレスコントローラ を 3 つまで選択できます。
4. [Next] をクリックします。

すべてのオンボーディング パケット キャプチャ セッションが、**Assurance** > **[Intelligent Capture Settings]** ウィンドウの [Onboarding Packet Capture] タブに表示されます。

ステップ 4 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

ステップ 5 [Tasks] ウィンドウで、タスクの展開を監視します。

進行中のクライアントデバイスのオンボーディング パケット キャプチャ セッションの停止

進行中のクライアントデバイスのオンボーディング パケット キャプチャ セッションを停止できます。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

[Onboarding Packet Capture] ウィンドウが表示されます。

ステップ 2 [In-progress Captures] で、オンボーディング パケット キャプチャ セッションの実行を停止する ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 3 [Stop Capture] をクリックします。

クライアントデバイスのフルパケットキャプチャ

クライアントデバイスのフルパケットキャプチャについて

フルパケットキャプチャを使用すると、ネットワークデータをキャプチャし、そのデータを PCAP ファイルとしてダウンロードして、Wireshark で表示できます。詳細については、クライアントデバイスのフル パケット キャプチャ セッションの実行 （490 ページ）を参照してください。

（注） 「クライアント データ パケット キャプチャ」は「フルパケットキャプチャ」に名称変更されました。この名称を合理化する過程で、さまざまな販促アイテムで以前の名前とブランド変更された名前が使用されていることがあります。ただし、「クライアント データ パケット キャプチャ」と「フルパケットキャプチャ」は同じ機能を指しています。

サポートされているアクセスポイントの一覧については、「Feature Matrix for Cisco Wireless Access Points」を参照してください。

フルパケットキャプチャの制限事項

フルパケットキャプチャの制限事項

- 一度に実行できるフル 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、フルパケットキャプチャを機能させるためには、Catalyst Center とシスコ ワイヤレス コントローラの間でクロックを同期させる必要があります。ワイヤレスコントローラが Network Time Protocol（NTP）サーバーに接続されていることを確認します。
- 各フル パケット キャプチャ セッションで最大 1 GB のローリングデータをキャプチャできます。ダウンロードを高速化するために、1 GB のデータが 10 個の 100 MB のファイルに分割されます。

クライアントデバイスのフル パケット キャプチャ セッションの実行

クライアントデバイスでフル パケット キャプチャ セッションを実行できます。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

[Client Health] ウィンドウが表示されます。

ステップ 3 次のいずれかを行うと、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] フィールドに、次のいずれかの要素を入力します。
  - ユーザー ID（Cisco ISE により認証）
  - 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 AP がインテリジェント キャプチャ データを Catalyst Center に送信できない （518 ページ） を参照してください。

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。

- [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。
- [Timeline Slider]：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。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。

（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。

ステップ 6 [Run Packet Capture] をクリックします。

[Run a Data Packet Capture] の スライドインペイン が表示され、デフォルトでは [Onboarding Packet Capture] タブが選択されています。

ステップ 7 **[Run a Data Packet Capture]** スライドインペイン で、**[Full Packet Capture]** タブをクリックします。

（注） 既存のフルパケットキャプチャ タスクが完了していない場合に、同じ ワイヤレスコントローラ で新しいパケットキャプチャ セッションを開始しようとすると、未完了のタスクの競合が原因で失敗します。新しいタスクを開始するには、既存のタスクが完了するまで待つか、既存のタスクを破棄します。

ステップ 8 [Duration] ドロップダウンリストで、パケットキャプチャの期間を選択します。

デフォルトの時間は、30 分です。

ステップ 9 フルパケットキャプチャを有効にする ワイヤレスコントローラ の横にあるチェックボックスをオンにします。

ワイヤレスコントローラ を 3 つまで選択できます。

ステップ 10 [Next] をクリックします。



（注）
- すべてのフル パケット キャプチャ セッションが、**Assurance** > **[Intelligent Capture Settings]** > **[Full Packet Capture]** の下に表示されます。
- パケット キャプチャ セッションが Catalyst Center で設定されている場合、Catalyst Center が認識していないパケット キャプチャ セッションはすべて削除されます（ワイヤレスコントローラ で直接設定されたフル パケット キャプチャ セッションなど）。

ステップ 11 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（79 ページ）を参照してください。

ステップ 12 [Tasks] ウィンドウで、タスクの展開を監視します。



（注） タスクの期間に基づいて、Catalyst Center はフル パケット キャプチャ セッションの有効化タスクと無効化タスクを自動的に実行します。有効化または無効化されたタスクの設定プレビューを表示するには、[Tasks] ウィンドウに移動し、タスクを開き、[View Work Item Details] をクリックします。タスクが完了する前に設定プレビューを表示しない場合、プレビューのオプションは使用できなくなります。

ステップ 13 完了したフルパケットキャプチャおよび OTA パケット キャプチャ セッションから PCAP ファイルをダウンロードするには、**[Intelligent Capture:]** *[Client Device]* ウィンドウで、**[Download]** をクリックします。

AP とクライアント間を移動するパケットの 802.11 ファイルなど、ワイヤレスデータに関する情報を含むファイルをダウンロードできます。



（注） データパケットキャプチャは、個別の 100 MB ファイルに分割されます。Catalyst Center に格納するデータ パケット キャプチャ ファイルの合計サイズには、4 GB の制限があります。制限を超えると、合計サイズが 4 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。さらに、合計サイズの制限に達していなくても、14 日間超経過したデータ パケット キャプチャ ファイルは削除されます。

フルパケットキャプチャ履歴の表示

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のフル パケット キャプチャ セッションの履歴を表示するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

[Onboarding Packet Capture] ウィンドウが表示されます。

ステップ 2 **[Full Packet Capture]** タブをクリックします。

[Full Packet Capture] ウィンドウが表示されます。

ステップ 3 次の情報を表示するには、[Intelligent Capture Settings - Full Packet Capture] ウィンドウを使用します。

オプション	説明
[Identifier]	クライアントのユーザー ID またはホスト名が表示されます。ユーザー ID またはホスト名をクリックすると、[Intelligent Capture: Client Device] ウィンドウが開きます。
[MAC Address]	クライアントデバイスの MAC アドレスが表示されます。
ワイヤレスコントローラ	ワイヤレスコントローラ の名前を表示します。
[First Packet Time]	最初のデータパケットがキャプチャされた時刻が表示されます。
[Last Packet Time]	最後のデータパケットがキャプチャされた時刻が表示されます。
[Total Size]	キャプチャされたデータの合計サイズが表示されます。
[Currently Running]	データパケットキャプチャが実行中かどうかを表示します。
[Type of Packet]	パケットのタイプ（[Wired]、[Wireless] など）が表示されます。
[Duration]	パケットキャプチャの期間を表示します。
[Last Start Time]	パケットキャプチャの前回の開始時刻を表示します。
[Configuration Status]	デバイスの設定ステータスを表示します。

Wi-Fi 帯域およびチャネルの OTA スニファキャプチャ

Wi-Fi 帯域およびチャネルの OTA スニファキャプチャについて

Catalyst Center では、2 つのアクセスポイント（AP）にまたがる最大 4 つの無線で OTA スニファキャプチャを実行できます。選択した無線で無線ロールスニファ機能がサポートされていない場合、Catalyst Center は AP をクライアントサービスモードから専用スニファモードに自動的に切り替えます。それ以外の場合は、無線ロールスニファ機能を使用して、クライアントサービスを中断せずにパケットがキャプチャされます。

（注） ゲートウェイへの静的デフォルトルートが使用できない場合は、静的ルートを 127.0.0.1 に設定します

Wi-Fi 帯域およびチャネルの OTA スニファ キャプチャ セッションの実行

Wi-Fi 帯域およびチャネルの OTA スニファ キャプチャ セッションを実行できます。

Procedure

ステップ 1 メインメニューから次を選択します。**Assurance** > **[Health]**

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client Health] タブをクリックします。

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

ステップ 3 次のいずれかを行うと、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] フィールドに、ユーザー ID（Cisco ISE により認証済み）、IP アドレス、MAC アドレスのいずれかを入力します。

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*] ウィンドウが表示されます。

Attention [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 AP がインテリジェント キャプチャ データを Catalyst Center に送信できない , on page 518 を参照してください。

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。

- [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。[1 hour]（デフォルト）、[3 hours]、[5 hours] のいずれかを選択できます。
- [Timeline Slider]：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。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。

Note 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。

ステップ 6 [Run Packet Capture] をクリックします。

[Client Packet Capture] スライドインペイン が表示され、デフォルトでは [Onboarding Packet Capture] タブが選択されています。

ステップ 7 [Client Packet Capture] スライドインペイン で、[OTA Sniffer] タブをクリックします。

デフォルトではフロアマップビューが表示されます。

ステップ 8 次のいずれかの操作を行って、無線または AP スニッフィングを実行する AP を選択します。

- フロアマップで、AP をクリックします。
- ビュースイッチャのリストアイコンをクリックし、AP の横にあるチェックボックスをオンにします。

Catalyst Center では、OTA スニファでサポートされている無線のみが表示されます。

Note OTA スニファでは、特定の AP 無線の帯域とチャネルで Wi-Fi パケットがキャプチャされます。過去 15 分間以内に OTA に使用されていた場合、同じ AP 無線を OTA に再利用することはできません。同じ AP 無線で OTA を再度有効にするには、その AP 無線の [Device 360] ウィンドウに新しいクライアントサービスデータが表示されるまで待つ必要があります。

ステップ 9 [Next] をクリックします。

ステップ 10 [Radio]、[Band]、[Channel Width]、[Channel] のドロップダウンリストで、それぞれの値を選択します。

Note デュアル無線をサポートする AP の場合は、次のように、プライマリ無線またはセカンダリ無線を使用して OTA スニファ データ パケット キャプチャを実行します。

- AP でデュアル無線モードが無効になっている場合は、プライマリ無線を使用してデータパケットキャプチャを実行します。
- AP でデュアル無線モードが有効になっている場合は、セカンダリ無線を使用してデータパケットキャプチャを実行します。

ステップ 11 [Next] をクリックします。

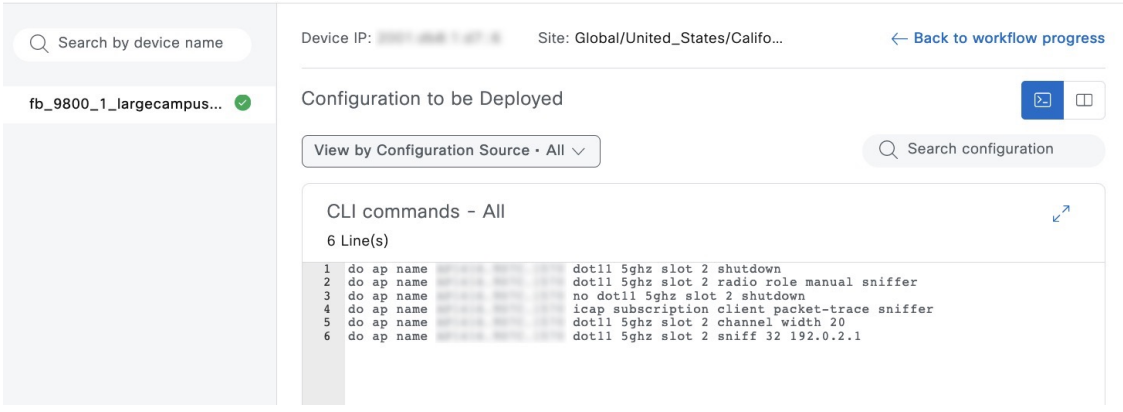
ステップ 12 無線モードの変更とクライアント接続の切断に関する [Warning] ダイアログボックスが表示された場合は、[OK] をクリックして確認し、続行します。

ステップ 13 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する, on page 78を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開, on page 79を参照してください。

Note [Preview Configuration] ウィンドウの [Configuration to be Deployed] でデバイス設定を確認すると、設定されている宛先 IP アドレスはデバイスレベルで無視されます。たとえば、次の図では、宛先 IP アドレスが 192.0.2.1 に設定されています。パケットデータを宛先 IP アドレスに送信する代わりに、Catalyst Center に送信します。



ステップ 14 [Tasks] ウィンドウで、タスクの展開を監視します。

Note

- OTA スニファのキャプチャ期間は 15 分間であるため、Catalyst Center は自動的に有効化タスクと無効化タスクを実行します。有効化または無効化されたタスクの設定プレビューを表示するには、[Tasks] ウィンドウに移動し、タスクを開き、[View Work Item Details] をクリックします。タスクが完了する前に設定プレビューを表示しない場合、プレビューのオプションは使用できなくなります。
- すべての OTA スニファ データ キャプチャ セッションが、**Assurance** > **[Intelligent Capture Settings]** > **[OTA Sniffer]** に表示されます。OTA スニファデータキャプチャは、個別の 500 MB ファイルに分割されます。Catalyst Center に格納する OTA スニファキャプチャファイルの合計サイズには、15 GB の制限があります。制限を超えると、合計サイズが 15 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。さらに、合計サイズの制限に達していなくても、24 時間超経過した OTA スニファキャプチャファイルは削除されます。

完了した OTA スニファキャプチャ セッションからの PCAP ファイルのダウンロード

次のいずれかのウィンドウで、完了した OTA スニファキャプチャ セッションから PCAP ファイルをダウンロードできます。

- [Device 360]：[Device 360] ウィンドウから PCAP ファイルをダウンロードすると、その特定のデバイスの完了した OTA スニファ キャプチャ セッションからのデータのみがダウンロードされます。
- [Client 360]：[Client 360] ウィンドウから PCAP ファイルをダウンロードすると、その特定のクライアントの完了したフル パケット キャプチャ セッションと OTA スニファ キャプチャ セッションの両方からのデータがダウンロードされます。
- [Intelligent Capture Settings]：[Intelligent Capture Settings] ウィンドウの**[OTA Sniffer Capture]** > **[Completed Captures]**タブでは、完了した OTA スニファ キャプチャ セッションから選択した AP のデータのみがダウンロードされます。

[Intelligent Capture Settings] ウィンドウで PCAP ファイルをダウンロードするには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**Assurance** > **[Intelligent Capture Settings]**を選択します。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[OTA Sniffer Capture] タブをクリックします。

[OTA Sniffer Capture] ウィンドウでは、[In-progress Captures] タブがデフォルトで選択されています。

ステップ 3 [Completed Captures] タブをクリックします。

[Completed Captures] テーブルに、完了した OTA スニファ キャプチャ セッションが一覧表示されます。

ステップ 4 [Download] 列で、関連する完了したキャプチャセッションに対応する下矢印アイコンをクリックして、その 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には、AP とクライアント間を移動するパケットの 802.11 ファイルなど、ワイヤレスデータに関する情報が含まれます。



（注） OTA スニファキャプチャのデータパケットファイルは、個別の 500 MB ファイルに分割されます。Catalyst Center に格納されるすべての OTA スニファキャプチャファイルの合計サイズには、15 GB の制限があります。この制限を超えると、合計サイズが 15 GB のしきい値を下回るまで、最も古いパケットファイルが削除されます。さらに、合計サイズの制限に達していなくても、24 時間を超えた OTA スニファキャプチャファイルは自動的に削除されます。

AP およびワイヤレスコントローラの AP 統計情報のキャプチャ

AP およびワイヤレスコントローラの AP 統計情報キャプチャについて

インテリジェントキャプチャ機能を利用すると、特定の AP および対応している ワイヤレスコントローラ で AP 統計情報キャプチャを有効または無効にすることができます。有効になっていると、次のデータがキャプチャされます。

- **[デバイス360（Device 360）]** > **[インテリジェントキャプチャ（Intelligent Capture）]** ウィンドウの [RF統計情報（RF Statistics）] タブに表示される、AP の無線および WLAN の統計情報。
- 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]**ウィンドウの [RF Statistics] 領域に表示される AP クライアント統計情報（サンプリング時間は 30 秒）。

特定の AP での AP 統計キャプチャの有効化または無効化

1 つまたは複数の AP で AP 統計データのキャプチャを有効にして管理できます。キャプチャされるデータには、AP 無線統計、WLAN 統計、AP クライアント統計が含まれます。Catalyst Center は、最大 1000 台の AP の AP 統計キャプチャをサポートできます。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 [Configure AP Enablement] で、[Specific - select specific APs and enable] をクリックしてから、[Get Started] をクリックします。

左側のペインには左側のツリー階層が表示され、右側のペインにはデフォルトのビューが表示されます。これはフロアが選択されていないためです。

ステップ 4 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。

右側のペインでは、[Disabled APs] タブが選択され、選択したフロアで無効になっている AP のリストが表示されます。

（注） ワイヤレスコントローラによって管理されているすべての AP で AP 統計のキャプチャを有効または無効にしようとしていて、[Global - enable or disable capable WLCs] オプションボタンがグレー表示されている場合は、まず [Enabled APs] タブにリストされているすべての有効な AP でこの機能を無効にする必要があります。

ステップ 5 次のいずれか 1 つのタスクを実行します。

- 特定の AP で AP 統計のキャプチャを有効にするには、ステップ 6 （499 ページ）に進みます。
- 特定の AP で AP 統計のキャプチャを無効にするには、[Enabled APs] タブをクリックしてステップ 6 （499 ページ）に進みます。

ステップ 6 AP 統計キャプチャを有効または無効にする AP の横にあるチェックボックスをオンにします。

ステップ 7 選択した AP での AP 統計キャプチャの有効化/無効化

- 選択した AP で AP 統計のキャプチャを有効にするには、[Enable] をクリックします。
- 選択した AP で AP 統計のキャプチャを無効にするには、[Disable] をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

ワイヤレスコントローラでの AP 統計キャプチャの有効化/無効化

対応する ワイヤレスコントローラ で AP 統計のキャプチャを有効または無効にできます。最大 3 つの ワイヤレスコントローラ を有効にできます。この機能を有効にすると、ワイヤレス

コントローラ によって管理されるすべての AP が、AP 無線統計、WLAN 統計、AP クライアント統計などの AP 統計データをキャプチャします。

Catalyst Center は、最大 1000 台の AP の AP 統計キャプチャをサポートできます。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 [Configure AP Enablement] で、[Global - enable or disable capable WLCs] を有効または無効にしてから、[Get Started] をクリックします。

ステップ 4 [Warning] ダイアログボックスで、[Yes] をクリックして続行します。

（注） 特定の AP で AP 統計キャプチャを有効または無効にするときに、[Specific - select specific APs and enable] オプションボタンがグレー表示されている場合は、最初にすべての有効なワイヤレスコントローラ でこの機能を無効にする必要があります。

[AP Stats Capture] タブが選択され、テーブルに対応可能なワイヤレスコントローラが表示されます。ワイヤレスコントローラごとに [Configuration Status] 列に次のいずれかのステータスが表示されます。

- [Success]：Catalyst Center が ワイヤレスコントローラ で AP 統計キャプチャを正常に有効にしました。
- [Not Configured]：Catalyst Center が ワイヤレスコントローラ で AP 統計キャプチャを有効にしていません。
- [In Progress]：Catalyst Center が ワイヤレスコントローラ で AP 統計キャプチャを有効にしています。
- [Failed]：ワイヤレスコントローラ が設定を受け入れなかったため、Catalyst Center が ワイヤレスコントローラ で AP 統計キャプチャを有効にできませんでした。

ヒント [Configuration Status] が [Failed] の場合は、ワイヤレスコントローラ で AP 統計キャプチャを無効にしてから、ワイヤレスコントローラ で再度有効にします。

- [Unknown]：Catalyst Center が ワイヤレスコントローラ で AP 統計キャプチャを有効にしましたが、Catalyst Center がデバイスのステータスを認識していません。

ヒント [Configuration Status] が [Unknown] の場合は、ワイヤレスコントローラで AP 統計キャプチャを無効にしてから、ワイヤレスコントローラ で再度有効にします。

ステップ 5 AP 統計キャプチャを有効または無効にする ワイヤレスコントローラ の横にあるチェックボックスをオンにします。

ステップ 6 ワイヤレスコントローラによって管理されるすべての AP での AP 統計キャプチャを有効または無効にします。

- ワイヤレスコントローラ によって管理されるすべての AP で AP 統計キャプチャを有効にするには、[Enable] をクリックします。
- ワイヤレスコントローラ によって管理されるすべての AP で AP 統計キャプチャを無効にするには、[Disable] をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

AP 統計情報キャプチャに対応していない AP の表示

AP 統計情報キャプチャで互換性のない AP を表示できるのは、AP 有効化のタイプに [Specific - select specific APs and enable] を選択した場合のみです。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 [Configure AP Enablement] で、[Specific - select specific APs and enable] をクリックしてから、[Get Started] をクリックします。

左側のペインには左側のツリー階層が表示され、右側のペインにはデフォルトのビューが表示されます。これはフロアが選択されていないためです。

ステップ 4 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。

右側のペインでは、[Disabled APs] タブが選択され、選択したフロアで無効になっている AP のリストが表示されます。

ステップ 5 [Not-Ready APs] タブをクリックします。

（注） 対応していない 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。インテリジェントキャプチャ（iCAP）をサポートする ワイヤレスコントローラ および AP の詳細については、「Feature Matrix for Cisco Wireless Access Points」を参照してください。

AP の RF 統計の表示

次の手順を使用して、特定の AP の RF 統計を表示できます。

手順

ステップ 1 [Health]メインメニューから次を選択します。**Assurance** > 。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network Health] タブをクリックします。

[Network Health] ウィンドウが表示されます。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名（ハイパーリンクされた識別子）をクリックし、AP の詳細を表示します。
- [Search] フィールド（右上隅にあります）で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

注目 「GRPCリンクの準備ができていません（接続中）（GRPC link is not ready (CONNECTING)）」というメッセージ付きの ⚠ アイコンが AP 名の横に表示される場合は、「クライアントまたはAPがインテリジェントキャプチャデータをCatalyst Centerに送信できない （518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。特定の AP での AP 統計キャプチャの有効化または無効化 （498 ページ）またはワイヤレスコントローラでの AP 統計キャプチャの有効化/無効化 （499 ページ）を参照してください。

ステップ 6 タイムラインを使用すると、指定された時間の RF 統計情報を表示し、データの範囲を指定できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]（デフォルト）、[3 hours]、および [5 hours] 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。

ステップ 7 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の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、サポートされている無線の数に応じて [Radio 0（2.4 GHz or 5 GHz）]、[Radio 1（5 GHz）]、または [Radio 2（6 GHz）] を選択します。

ステップ 8 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、次のタスクを実行できます。

- 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。
[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。

AP およびワイヤレスコントローラの異常キャプチャ

AP およびワイヤレスコントローラの異常キャプチャについて

インテリジェントキャプチャ機能を使用すると、特定の AP またはワイヤレスコントローラで異常キャプチャを有効または無効化にすることができます。有効にすると、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異常オンボーディングイベントをすべてキャプチャし、ダウンロードまたは表示できます。

AP キャプチャの制限事項

Catalyst Center に格納する異常をトリガーしたパケットファイルの合計サイズには、1.05 GB の制限があります。制限を超えると、合計サイズが 1.05 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

特定の AP での異常キャプチャの有効化または無効化

1 つ以上の AP を有効にして管理し、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オンボーディングイベントをキャプチャできます。異常キャプチャを有効にすると、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異常オンボーディングイベントをすべてキャプチャし、ダウンロードして表示できます。異常キャプチャを無効にすると、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異常オンボーディングイベントをすべてキャプチャせず、ダウンロードや表示ができません。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 **[Anomaly Capture]** タブをクリックします。

ステップ 4 **[Configure AP Enablement]** で、**[Specific - select specific APs and enable]** をクリックしてから、**[Get Started]** をクリックします。

左側のペインには左側のツリー階層が表示され、右側のペインにはデフォルトのビューが表示されます。これはフロアが選択されていないためです。

（注） ワイヤレスコントローラによって管理されているすべての AP で異常キャプチャを有効または無効にしようとしていて、**[Global - enable or disable enabled WLCs]** オプションボタンがグレー表示されている場合は、まず **[Enabled APs]** タブにリストされているすべての有効な AP でこの機能を無効にする必要があります。

ステップ 5 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。

右側のペインでは、[Disabled APs] タブが選択され、選択したフロアで無効になっている 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。

ステップ 6 次のいずれか 1 つのタスクを実行します。

- 特定の AP で異常キャプチャを有効にするには、ステップ 7 （506 ページ） に進みます。
- 特定の AP で異常キャプチャを無効にするには、[Enabled APs] タブをクリックして ステップ 7 （506 ページ） に進みます。

ステップ 7 異常キャプチャを有効または無効にする AP の横にあるチェックボックスをオンにします。

ステップ 8 選択した AP での異常キャプチャの有効化または無効化

- 選択した AP で異常キャプチャを有効にするには、**[Enable]** をクリックします。
- 選択した AP で異常キャプチャを無効にするには、**[Disable]** をクリックします。

ステップ 9 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開（79 ページ）を参照してください。

ステップ 10 [Tasks] ウィンドウで、タスクの展開を監視します。

ワイヤレスコントローラ での異常キャプチャの有効化または無効化

対応可能な ワイヤレスコントローラ で異常キャプチャを有効または無効にすることができ、最大3つの ワイヤレスコントローラを有効にできます。異常キャプチャを有効にすると、ワイヤレスコントローラ によって管理される AP に関連付けられているクライアントの異常イベントをすべてキャプチャし、ダウンロードして表示できます。異常キャプチャを無効にすると、ワイヤレスコントローラ によって管理される AP に関連付けられているクライアントの異常オンボーディングイベントをすべてキャプチャせず、ダウンロードや表示ができません。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 **[Anomaly Capture]** タブをクリックします。

ステップ 4 [Configure AP Enablement] で、[Global - enable or disable capable WLCs] を有効または無効にしてから、[Get Started] をクリックします。

ステップ 5 [Warning] ダイアログボックスで、[Yes] をクリックして続行します。

（注） 特定の AP で異常キャプチャを有効または無効にするときに、**[Specific - select specific APs and enable]** オプションボタンがグレー表示になっている場合は、まずすべての有効な ワイヤレスコントローラ でこの機能を無効にする必要があります。

[Anomaly Capture] タブが選択されていて、対応可能な ワイヤレスコントローラ がテーブルに表示されます。ワイヤレスコントローラ ごとに、[Configuration Status] 列に次のいずれかのステータスが表示されます。

- **[Success]**：Catalyst Center が ワイヤレスコントローラ で異常キャプチャを正常に有効にしました。
- **[Not Configured]**：Catalyst Center は ワイヤレスコントローラ で異常キャプチャを有効にしていません。
- **[In Progress]**：Catalyst Center が ワイヤレスコントローラ で異常キャプチャを有効にしています。
- **[Failed]**：ワイヤレスコントローラ が設定を受け入れなかったため、Catalyst Center は ワイヤレスコントローラ で異常キャプチャを有効にできませんでした。

ヒント **[Configuration Status]** が **[Failed]** の場合は、ワイヤレスコントローラ で異常キャプチャを無効にしてから、ワイヤレスコントローラ で再度有効にします。

- **[Unknown]**：Catalyst Center が ワイヤレスコントローラ で異常キャプチャを有効にしましたが、Catalyst Center がデバイスのステータスを認識していません。

ヒント **[Configuration Status]** が **[Unknown]** の場合は、ワイヤレスコントローラ で異常キャプチャを無効にしてから、ワイヤレスコントローラ で再度有効にします。

ステップ 6 異常キャプチャを有効または無効にする ワイヤレスコントローラ の横にあるチェックボックスをオンにします。

ステップ 7 選択した ワイヤレスコントローラ によって管理されるすべての AP で異常キャプチャを有効または無効にします。

- 選択した ワイヤレスコントローラ によって管理されるすべての AP で異常キャプチャを有効にするには、**[Enable]** をクリックします。

  （AP の有効化が完了するまでこれ以上の変更はできないことに関する）**[Warning]** ダイアログボックスが表示された場合は、**[Yes]** をクリックして続行します。

- 選択した ワイヤレスコントローラ によって管理されるすべての AP で異常キャプチャを無効にするには、**[Disable]** をクリックします。

ステップ 8 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

ステップ 9 [Tasks] ウィンドウで、タスクの展開を監視します。

異常キャプチャに対応していない AP とサポートされている AP の表示

異常キャプチャに対応していない AP とサポートされている AP を表示できるのは、AP 有効化のタイプで [Specific - select specific APs and enable] を選択した場合のみです。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [Intelligent Capture Settings] ウィンドウで、[Access Point] タブをクリックします。

[Access Point] ウィンドウでは、[AP Stats Capture] タブがデフォルトで選択されています。

ステップ 3 **[Anomaly Capture]** タブをクリックします。

ステップ 4 **[Configure AP Enablement]** で、**[Specific - select specific APs and enable]** をクリックしてから、**[Get Started]** をクリックします。

左側のペインには左側のツリー階層が表示され、右側のペインにはデフォルトのビューが表示されます。これはフロアが選択されていないためです。

ステップ 5 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。

右側のペインでは、[Disabled APs] タブが選択されていて、選択されているフロアで無効になっている AP のリストが表示されます。

ステップ 6 異常キャプチャの互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。



（注） 対応していない 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。インテリジェントキャプチャ（iCAP）をサポートする ワイヤレスコントローラ および AP の詳細については、「Feature Matrix for Cisco Wireless Access Points」を参照してください。

ステップ 7 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アイコンをクリックします。

AP のスペクトル解析

スペクトル解析時の Cisco AP 機能について

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モードに変更できます。AP の FRA 無線を 5 GHz で動作するように設定している場合、クライアント無線は 2.4 GHz 帯域では動作できません。

サポートされているアクセスポイントの一覧については、『Feature Matrix for Cisco Wireless Access Points』[英語] を参照してください。

2 つの無線スロットを備えた AP	3 つの無線スロットを備えた AP
Aironet 1560 AP Catalyst IW6300 Heavy Duty シリーズ AP Catalyst IW6300 Heavy Duty シリーズ AP	Catalyst 9120 AP Catalyst 9130 AP （注） 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。 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] フィールドは空です。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。

AP でのスペクトル解析セッションの開始

次の手順に従って、特定の AP でスペクトル解析セッションを開始できます。

（注）
- スペクトル解析セッションにかかる時間は 10 分です。
- 同時スペクトル解析セッションの最大数は 10 です。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Health]**の順に選択します。

ステップ 2 [Network Health] タブをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名（ハイパーリンクされた識別子）をクリックし、AP の詳細を表示します。
- [Search] フィールド（右上隅にあります）で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

注目 [GRPC link is not ready (CONNECTING)] というメッセージ付きの ⚠ アイコンが AP 名の横に表示される場合は、「クライアントまたは AP がインテリジェント キャプチャ データを Catalyst Center に送信できない （518 ページ）」を参照してください。

ステップ 5 [Spectrum Analysis] タブをクリックします。

ステップ 6 **[Start Spectrum Analysis]** をクリックします。

ステップ 7 展開のためのタスクのスケジュールを設定します。

[Visibility and Control of Configurations] の設定に応じて、次のいずれかを実行できます

- デバイス設定をすぐに展開するか、後で展開するようにスケジュールを設定します。詳細については、デバイス構成を今すぐまたは後で展開する （78 ページ）を参照してください。
- デバイス設定をプレビューして展開します。詳細については、デバイス設定のプレビューと展開 （79 ページ）を参照してください。

ステップ 8 [Tasks] ウィンドウで、タスクの展開を監視します。

（注） 10 分のスペクトル解析期間に基づいて、Catalyst Center はキャプチャセッションの有効化タスクと無効化タスクを自動的に実行します。有効化および無効化されたタスクの設定プレビューを表示するには、**[Tasks]** ウィンドウに移動し、タスクを開き、**[View Work Item Details]** をクリックします。タスクが完了する前に設定プレビューを表示しない場合、タスクの完了後はプレビューのオプションを使用できなくなります。

AP のスペクトル解析データの表示

次の手順に従って、AP のスペクトル解析データを表示できます。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Health]**の順に選択します。

ステップ 2 [Network Health] タブをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名（ハイパーリンクされた識別子）をクリックし、AP の詳細を表示します。
- [Search] フィールド（右上隅にあります）で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

ステップ 4 [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

注目 「GRPCリンクの準備ができていません（接続中）（GRPC link is not ready (CONNECTING)）」というメッセージ付きの ⚠ アイコンが AP 名の横に表示される場合は、「クライアントまたは AP がインテリジェントキャプチャ データを Catalyst Center に送信できない （518 ページ）」を参照してください。

ステップ 5 [Spectrum Analysis] タブをクリックします。

ステップ 6 タイムラインを使用すると、指定された時間のスペクトル解析データを、データの範囲を指定して表示できます。

タイムラインスライダ	
アイテム	**説明**
[1 hour] ドロップダウンリスト	ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]（デフォルト）、[3 hours]、および [5 hours] 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。

ステップ 7 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のデータをフィルタ処理できます。[2.4 GHz]、[5 GHz]、または [6 GHz] をクリックします。

（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、その AP には選択された帯域を使用している無線がないことを示します。これは、AP に [5 GHz] の無線を出力するクライアントがあるが、無線周波数セレクタが [2.4 GHz] に設定されている場合に発生します。

詳細については、スペクトル解析時の Cisco AP 機能について （509 ページ）を参照してください。

ステップ 8 [Spectrum Analysis] チャートには、次の機能が用意されています。

[Spectrum Analysis] チャート	
アイテム	**説明**
上位チャート（パーシステンス）	このチャートは、RF 環境で検知された各信号の振幅（電力）とチャネル周波数をリアルタイムで提供します。X 軸は振幅を表し、Y 軸はチャネル周波数を表します。 チャート内の色は、選択された 5 分間で同じ振幅およびチャネル周波数で検知される信号の数を表します。 • 青色は、オーバーラップする信号の数が少ない（または信号が同じ振幅と周波数で検知される）ことを示します。 • 赤色は、オーバーラップする信号の数が多いことを示します。 より多くの信号が検知されるにつれ、色の強度が増加します（青色 > 緑色 > 黄色 > オレンジ色 > 赤色）。チャート内の線がオーバーラップし、交差すると、色が変わります。 色の透過性は、信号データの経過時間を表し、古いデータはより透過的になります。 リアルタイムで RF 環境を表示するには、[Real-TimeFFT（Fast Fourier Transform）] をクリックして有効にします。リアルタイム FFT を有効にすると、永続化チャートが制限されて 5 分間のデータストリームのコレクションではなく、「1 つ」の最新データストリームが表示されます。 特定の範囲のチャネルのデータをズームインして表示するには、マウスをクリックしてドラッグし、範囲を選択します。チャートが更新され、選択した特定のチャネルのデータが表示されます。 チャート全体をズームアウトして表示するには、右上隅の虫めがねをクリックします。

[Spectrum Analysis] チャート	
アイテム	説明
ボトムチャート（ウォーターフォール）	このチャートは、データの時間的な解釈を提供します。このチャートは、パーシステンスチャートと同じ情報を提供しますが、フォーマットは異なります。X 軸は時間を表し、Y 軸はチャネル周波数を表します。チャート内の行は、イベントが発生した正確な順序を表します。これにより、問題が発生した場合に根本原因をトラブルシュートすることができます。 チャート内の色は、振幅を表します。青色は低い値（-100 dBm）を示し、赤色は高い値（-20 dBm）を示します。

ステップ 9 [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。

有線クライアントデバイス向けパケットキャプチャ

有線クライアントデバイスの接続またはトラフィックの問題をトラブルシュートするために、Assurance からパケットキャプチャを開始して、関連するスイッチポートからパケットデータを収集できます。

前提条件

有線パケットキャプチャを開始する前に、次のことを確認してください。

- [自動化 - インテリジェントキャプチャ（Automation - Intelligent Capture）] パッケージがインストールされています。
- 有線クライアントが Cisco Catalyst 9200、9300、9400、9500、または 9600 シリーズ スイッチに接続されています。
- スイッチが Cisco IOS XE 17.9 以降を実行しています。
- トラブルシュートする有線クライアントまたはスイッチポートを把握しています。
- 同じデバイスで別の有線パケットキャプチャが現在アクティブではありません。

制限事項

有線クライアントデバイスでパケットキャプチャを実行する場合は、次の制限事項に注意してください。

- デバイスで一度にアクティブにできる有線パケットキャプチャは 1 つだけです。
- キャプチャの保持期間は、一定期間のみに基づいているわけではありません。
- 有線クライアントデバイスのパケットキャプチャは、100 MB のバッファを使用して線形に設定されます。バッファがいっぱいになると、スイッチはパケットキャプチャを停止します。この時点で、次のようになります。
  1. Catalyst Center はキャプチャセッションを停止します。
  2. スイッチのバッファの内容は Catalyst Center に送信されます。
  3. Catalyst Center では、パケットキャプチャが PCAP ファイルに保存され、ダウンロード可能になります。
- ストレージまたはバッファのキャパシティを使い尽くした場合、古いキャプチャファイルが削除される場合があります。

警告 パケットキャプチャファイルを保持する必要がある場合は、速やかにダウンロードしてください。Catalyst Center によって古いファイルが自動的に削除されることがあります。

有線クライアントデバイスでのパケットキャプチャの実行

Catalyst Center によって管理される有線クライアントデバイスでパケットキャプチャを実行するには、次の手順を実行します。

有線デバイスで一度に実行できるパケットキャプチャは 1 つだけです。キャプチャがすでに実行中の場合は、同じデバイスで別のキャプチャを開始する前に、キャプチャを停止する必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[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。

ステップ 2 [Network] タブをクリックします。

[ネットワーク（Network）] 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（Network Devices）] テーブルでハイパーリンクされた識別子をクリックして、特定のデバイスの [デバイス360（Device 360）] ウィンドウを開きます。

デバイスの 360 度ビューが表示されます。

ステップ 4 [ツール（Tools）] セクションで、[インテリジェントパケットキャプチャ（Intelligent Packet Capture）] フィールドの [開始（Start）] をクリックします。

[インテリジェントパケットキャプチャ（Intelligent Packet Capture）] スライドインペインが開きます。

ステップ 5 [場所（Location）] および [接続されたネットワークデバイス（Connected Network Device）] フィールドに値がすでに設定されていることを確認して、ウィザードを完了します。

a) ドロップダウンリストから使用するポートを選択します。

b) パケットキャプチャの期間（1 ～ 60 分）を指定します。

c) （オプション）収集するトラフィックを制限するフィルタを入力します。

詳細については、「パケットキャプチャのフィルタの設定 （516 ページ）」を参照してください。

d) [Next] をクリックします。

（注） [構成の可視化と制御（Visibility and Control of Configurations）] 機能について説明したビデオとドキュメントへのリンクが含まれるウィンドウが開きます。[閉じる（Close）] をクリックして続行します。

e) 展開オプションを選択します。

- [今すぐ（Now）] または [後で（Later）] を選択した場合、デバイス構成を今すぐまたは後で展開する （78 ページ） で説明されている手順を実行します。
- [プレビューと展開（Preview and Deploy）] を選択した場合、デバイス設定のプレビューと展開（79 ページ） で説明されている手順を実行します。

キャプチャが開始されると、Assurance はスイッチに設定を送信し、バックグラウンドでキャプチャを実行します。

パケットキャプチャのフィルタの設定

フィルタを使用して、有線クライアントデバイスのパケットキャプチャ中に Catalyst Center が収集するトラフィックの量を減らし、トラブルシュートしている問題に関連するパケットに焦点を当てることができます。たとえば、フィルタ `ipv4 any host 1.1.1.1` は、宛先 IP アドレス 1.1.1.1 のすべてのパケットをキャプチャします。

有線クライアントデバイス向けパケットキャプチャのフィルタは現在、以下をサポートしています。

- IPv4 トラフィック

- IPv6 トラフィック
- 送信元ベースの一致
- 接続先ベースの一致
- プロトコルベースの一致

フィルタリング機能はインラインフィルタに制限され、ACLベースのフィルタリングはサポートされていません。

実行中のキャプチャの停止

有線クライアントデバイスでアクティブなパケットキャプチャを停止する場合は、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[Intelligent Capture Settings]**。

ステップ 2 [有線パケットキャプチャ（Wired Packet Capture）] をクリックします。

ステップ 3 停止するパケットキャプチャの [停止（Stop）] をクリックします。

完了したパケットキャプチャのダウンロード

有線クライアントデバイスの特定のパケットキャプチャをダウンロードするには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[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。

ステップ 2 [Network] タブをクリックします。

[ネットワーク（Network）] 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（Network Devices）] テーブルでハイパーリンクされた識別子をクリックして、関連するクライアントデバイスの [デバイス360（Device 360）] ウィンドウを開きます。

デバイスの 360 度ビューが表示されます。

ステップ 4 [ツール（Tools）] セクションの [インテリジェントパケットキャプチャ（Intelligent Packet Capture）] フィールドで、[ダウンロード（Download）] をクリックします。

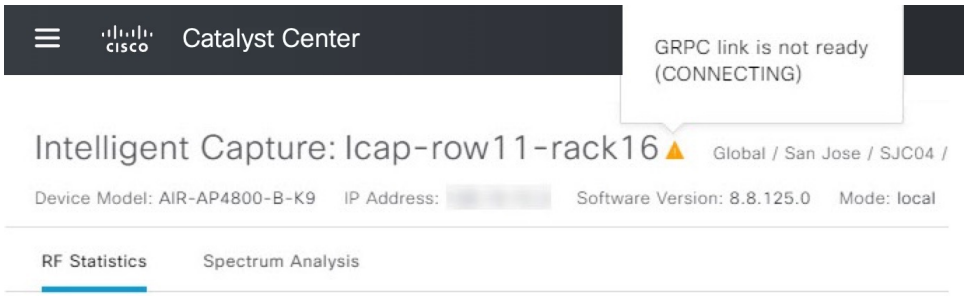
ステップ 5 スイッチで使用可能なキャプチャのリストを確認します。

ステップ 6 ダウンロードするキャプチャを選択し、[ダウンロード（Download）] をクリックします。

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 AP がインテリジェント キャプチャ データを Catalyst Center に送信できない

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 Catalyst 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 Catalyst Center に送信するためには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ または シスコ ワイヤレス コントローラ 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、Catalyst 9800 シリーズ ワイヤレス コントローラ または ワイヤレスコントローラ が Catalyst 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、Catalyst 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。

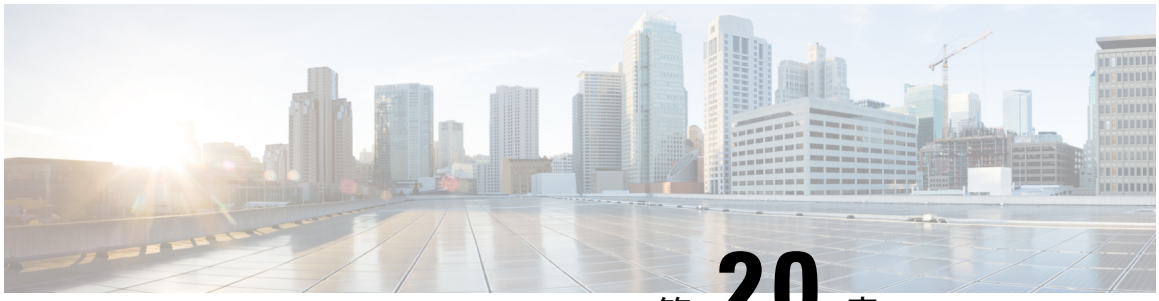
解決策：この問題を解決するには、次の作業を実行します。

1. Catalyst 9800 シリーズ ワイヤレス コントローラ または ワイヤレスコントローラ でインテリジェント キャプチャ サーバーのポート番号が 32626 に設定されていることを確認します。
2. ポート番号が 32626 に設定されていない場合は、手動で設定します。

有線パケットキャプチャの問題のトラブルシューティング

有線パケットキャプチャ機能を使用する際に問題が発生した場合は、次の点を確認してください。

- クライアントデバイスがサポート対象のスイッチであり、サポート対象の Cisco IOS ソフトウェアリリースがあることを確認します。
- 有線クライアントが正しいデバイスとポートに接続されていることを確認します。
- 正しいインターフェイスを選択していることを確認します。
- クライアントデバイスの新しいキャプチャを開始できない場合は、そのデバイスで別の有線キャプチャがすでにアクティブになっているかどうかを確認します。
- 想定されるトラフィックがキャプチャに含まれていない場合は、フィルタ式を確認し、より広範なフィルタを入力します。
- キャプチャがダウンロードできなくなった場合、バッファローテーションによって削除された可能性があります。



第 20 章

SSID モニタリング設定の管理

- SSID モニタリングについて （521 ページ）
- SSID モニタリングの設定 （522 ページ）
- SSID モニタリングのプロビジョニングステータスの表示 （523 ページ）

SSID モニタリングについて

デフォルトでは、Cisco Catalyst Assurance ですべての SSID に関するテレメトリデータをモニターおよび収集します。ただし、ネットワーク内のすべての SSID をモニターする必要がない場合のシナリオもあります。たとえば、ゲストまたはパブリック Wi-Fi サービスを提供する小売、輸送、またはサービス業のユースケースのように、ユーザー数が非常に多くなる可能性があります。このようなシナリオでは、上記の SSID に対するモニタリングをオフにする一方で、同じインフラストラクチャからの企業 SSID に対する豊富なデータは継続して収集することができます。

特定の SSID に対する SSID モニタリングを、その SSID の設定や SSID へのワイヤレス接続に影響を与えることなく有効または無効にすることができます。AP の SSID 機能への影響もありません。ワイヤレスクライアントは、設定に従って、該当する SSID および他のすべての SSID に引き続き接続します。モニタリング対象の SSID のクライアントは、引き続き [Client 360] ウィンドウの詳細データを使用できます。

SSID がモニタリングされていない場合、Cisco Catalyst Assurance はクライアントデータを収集しません。その場合、[Client 360] ウィンドウで、該当するクライアントの詳細データとグラフを使用することはできません。また、クライアントの正常性、クライアント固有の問題、インテリジェントキャプチャなどの他のデータも、これらのクライアントに関しては使用できません。さらに、[Client Health] ウィンドウのダッシュレットには、モニタリング対象ではない SSID のクライアントからのデータは含まれません。

（注） Cisco AireOS ワイヤレスコントローラに関する SSID モニタリングはサポートされていません。Cisco AireOS ワイヤレスコントローラに関して、Catalyst Center は、モニタリングが無効になっている SSID のテレメトリデータをドロップします。

メインメニューから次を選択します。 の **[Assurance]** > **[SSID Monitoring Settings]** を選択すると、[SSID Monitoring] ウィンドウが表示されます。[SSID Monitoring] ウィンドウでは次の操作を行うことができます。

- SSID モニタリング設定を表示する。
- 特定の SSID の SSID モニタリングを有効または無効にする。詳細については、SSID モニタリングの設定 （522 ページ）を参照してください。
- 設定された SSID モニタリングアクションに関するプロビジョニング要求を表示および管理する。詳細については、SSIDモニタリングのプロビジョニングステータスの表示 （523 ページ）を参照してください。

SSID モニタリングの設定

デフォルトでは、すべての SSID がモニタリングされます。ただし、1 つ以上の SSID のモニタリングをいつでも無効にしたり、再度有効にしたりすることができます。SSID モニタリング設定を更新するには、次の手順を使用します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[SSID Monitoring Settings]** の順に選択します。[SSID Monitoring] ウィンドウが開き、自分の SSID が表示されます。

ステップ 2 （任意） SSID のリストを絞り込むには、フィルタアイコン（▼）をクリックし、アクティブなフィールド（[Network Name (SSID)]、[Monitoring Status]、[Action]、または [Controller Config Status]）のいずれかに値を入力します。

フィルタを使用して、表示しない SSID やトラブルシューティングを行わない SSID を除外します。たとえば、テスト用に作成された SSID、社内 IT で使用する SSID、またはゲスト SSID（空港や地下鉄など）は表示する必要がないかもしれません。

ステップ 3 [Action] 列で、SSID に対応する [Disable] または [Enable] オプションをクリックします。

ステップ 4 スライドインペインで次の手順を実行します。

a) SSID モニタリングの変更を今すぐプロビジョニングするか、後でプロビジョニングするようにスケジュールするか、または選択したデバイスに設定を展開するために後で使用できるプレビューを作成するかを選択します。

b) [Task Name] フィールドにタスクの名前を入力します。

c) [Apply] をクリックします。

次のタスク

スケジュールされたSSIDモニタリングタスクのステータスを表示するには、[SSID Monitoring] ウィンドウで [Activity Page] をクリックします。または、メニューアイコンをクリックして次を選択します。 **[Activities]** > **[Tasks]**を選択します。

[Generate Preview] を選択した場合、作業項目のステータスを表示するには、メニューアイコンをクリックして次を選択します。 **[Activities]** > **[Tasks]**を選択します。

SSIDモニタリングのプロビジョニングステータスの表示

SSID モニタリング設定のプロビジョニングステータスを表示するには、次の手順を使用します。

手順

ステップ 1 メインメニューから次を選択します。**[Assurance]** > **[SSID Monitoring Settings]** の順に選択します。[SSID Monitoring] ウィンドウが開きます。

ステップ 2 テーブルで必要な SSID 名をクリックします。
クリックすると、スライドインペインにその SSID に対する SSID モニタリングのプロビジョニング要求のステータスが表示されます。

プロビジョニングステータス	説明
Configuring	ワイヤレスコントローラ で SSID モニタリングアクションの設定が進行中であることを示します。
Not Started	ワイヤレスコントローラに SSID モニタリングアクションがまだ設定されていませんが、設定がまもなく開始されることを示します。
Pending	SSID モニタリングアクションがキューに入れられており、ワイヤレスコントローラ が間もなく設定されることを示します。
成功	ワイヤレスコントローラ で SSID モニタリングアクションがプロビジョニングされたことを示します。
不合格	ワイヤレスコントローラ で SSID モニタリングアクションがプロビジョニングされていないことを示します。
N/A	ワイヤレスコントローラ がテレメトリの無効化をサポートしていないソフトウェアを実行していることを示します。Catalyst CenterはSSIDのテレメトリデータをドロップします。

次のタスク

SSID のプロビジョニングステータスが [Failed] で、再度 ワイヤレスコントローラ のプロビジョニングを試みる場合は、[Retry Failed Configuration] をクリックします。



第 21 章

デバイスのパスをトレース

- パストレースについて （525 ページ）
- パストレースの制限事項 （525 ページ）
- パストレースの実行 （528 ページ）

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行うことができます。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、Catalyst 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、Catalyst 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。

- Catalyst Center のサードパーティ製デバイスからのパストレースはサポートされていません。
- ファブリッククライアントと非ファブリッククライアントの間のパストレースは、サポートされていません。
- 複数の Virtual Routing Forwarding（VRF）仮想ネットワーク（VN）上にある 2 つのファブリッククライアント間のパストレースは、サポートされていません。

- 複数のサイト（ドメイン）上にある 2 つのファブリッククライアント間のパストレースは、サポートされていません。
- いずれかのエッジスイッチがファブリックに含まれていない、同じファブリックの同じサイト内に接続されているクライアントは、サポートされていません。
- ルータのループバック インターフェイスからのパス トレースは、サポートされていません。
- 重複する IP アドレスは、ファブリックの有無にかかわらずサポートされていません。
- パストレースを Locator/ID Separation Protocol（LISP）ファブリックで機能させるには、トラフィックが実行されていて、エッジスイッチでキャッシュを利用できることを確認します。
- Cisco 適応型セキュリティアプライアンス（ASA）は CDP をサポートしていないため、Cisco ASA のパストレースはサポートされていません。Cisco ASA アプライアンスを通るパスを識別することはできません。
- タグなしモードのワイヤレスコントローラの管理インターフェイスでは、パストレースはサポートされていません。
- 集中管理型ワイヤレス モビリティ モードの非対称モビリティ トンネリングに対するパストレースは、サポートされていません。
- 仮想スイッチング システム（VSS）、マルチリンク集約制御プロトコル（MLACP）、または仮想 PortChannel（vPC）のパス トレースはサポートされていません。
- スイッチ仮想インターフェイス（SVI）上の等コスト マルチパス ルーティング（ECMP）のパス トレースは、サポートされていません。
- NAT またはファイアウォールを使用するデバイスでのパストレースはサポートされていません。
- Cisco Performance Routing（PfR）は DMVPN トンネルでサポートされていません。
- VLAN ACL（VACL）が有効になっているパストレースは、サポートされていません。
- 非周期的な更新（NPR）パスシナリオでは、アップグレード後にコントローラでパスは更新されません。また、統計収集が停止します。統計収集を続行するには、新しいパス要求を開始する必要があります。
- Hot Standby Router Protocol（HSRP）VLAN のホストから任意の HSRP ルータに接続されている 非 HSRP VLAN のホストへのパス トレースは、サポートされていません。
- オブジェクト グループは ACL トレースでサポートされていません。
- ポートチャネルの Port Aggregation Protocol（PAgP）モードは、サポートされていません。LACP モードのみがサポートされています。
- インターフェイスに異なるパフォーマンス モニター ポリシーが設定されている場合は、Catalyst Centerを使用したパフォーマンスモニター設定の適用が失敗します。インターフェイスのパフォーマンスモニター設定を削除して、パストレース要求を再送信します。

- パフォーマンスモニター統計情報のパストレースは、Cisco ASR 1000 シリーズルータ（Cisco IOS XE 16.3.1）ではサポートされていません。
- パフォーマンスモニター統計情報のパストレースは、Cisco Catalyst 3850 スイッチ（Cisco IOS XE 16.2.x および 16.3.1）ではサポートされていません。
- Cisco Mobility Express（ME）ワイヤレスコントローラのパストレースはサポートされていません。
- Cisco SD-Access ファブリックで OTT を使用するワイヤレスクライアントのパストレースはサポートされていません。
- レイヤ 2 スイッチからのパストレースはサポートされていません。
- シスコの産業用イーサネット（IE）スイッチは、SD-Access ソリューションの一部として拡張されたノードです。現在、パストレースは拡張ノードを認識していないため、トポロジに拡張ノードが含まれている場合は、エラーメッセージが表示されます。
- デバイス用に IPv4 アドレスと IPv6 アドレスの両方を使用するデュアルスタックはサポートされていません。この状況になると、指定されたアドレスが不明であることを示すエラーメッセージが表示されます。
- Cisco ワイヤレスコントローラは SNMP モビリティの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、Catalyst 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。

- パスをトレースするには、クライアント接続ポートをレイヤ2として設定する必要があります。
- パストレースはスタンバイ WLC をサポートしていません。
- パストレースは、インターフェイスマッピングの制限により、CSRv や C9800-CL などの VM ベースのデバイスをサポートしていません。
- Cisco Mobility Express（ME）や Embedded Wireless Controllers（EWC）のパストレースはサポートされていません。
- パストレースは、IE4000 シリーズなどの拡張ノードをサポートしていません。
- パスのトレースでは、送信元または接続先デバイスとして WLC または AP を使用することはサポートされていません。

- ワイヤレス LISP ファブリックのパストレースでは、AP ではなく、送信元と宛先のエッジ間でのみ VXLAN トンネルが表示されます。
- パストレースは、トランクポート経由で接続されたホストをサポートしていません。
- タグなしモードの WLC 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。
- パストレースは、VSS、M-LACP、または vPC の設定をサポートしていません。
- パストレースは、SVI を介した ECMP をサポートしていません。
- パストレースはポートチャネル PAgP モードをサポートしていません。LACP モードのみがサポートされています。
- パスのトレースは、VLAN ACL（VACL）をサポートしていません。
- NPR（非定期更新）シナリオのパストレースが、システムアップグレード後に自動的に更新されません。統計情報の収集を再開するには、新しいパスリクエストが必要です。
- HSRP VLAN のホストから同じ HSRP/VRRP/GLBP 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。
- 競合するパフォーマンスモニターの設定がインターフェイスに存在すると、パストレースが失敗します。リクエストを送信する前に、この設定を削除する必要があります。
- 定期的なデータベース更新中に基盤となるトレースルート操作がタイムアウトすると、パスのトレースが「データベースは一時的に使用できません（Database is temporarily unavailable）」というエラーを返すことがあります。
- パストレースは L2 ハンドオフをサポートしていません。
- パストレースは、「ファブリックから不明」シナリオをサポートしていません。
- デュアルスタック セットアップのパスのトレースでは、表示される管理 IP が VXLAN トンネルで実際に使用されている IP タイプを示していない場合があり、UI レンダリングに影響を与える可能性があります。

パストレースの実行

パストレース機能は、すべてのデバイスで同様の方法で動作します。[Client 360] または [Device 360] ウィンドウからパストレースを実行できます。

始める前に

- パストレースの既知の制限事項を確認してください。パストレースの制限事項（525 ページ）を参照してください。
- デバイス（ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント）が検出されたことを確認します。IP アドレス範囲または CIDR を使用したネットワークの検

出 （29 ページ）、CDP を使用したネットワークの検出 （26 ページ）、またはLLDP を使用したネットワークの検出 （32 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。

手順

ステップ 1 [Client 360] または [Device 360] ウィンドウの [Path Trace] カテゴリで、[Run New Path Trace] をクリックします。
[Set up Path Trace] スライドインペインが表示されます。

ステップ 2 送信元の IP アドレス、インターフェイス、およびポート番号、宛先の IP アドレス、インターフェイス、およびポート番号を入力します。

フィールド	アクション
[Source IP] フィールド	[送信元IP（Source IP）] フィールドに IP アドレスは事前に入力されていますが、次のいずれかのタスク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IP（Source IP）] ドロップダウンをクリックして、使用可能なオプションからIPアドレスを選択します。送信元IPアドレスのドロップダウンリストは、最大 100 エントリに制限されています。 • [MAC] ドロップダウンをクリックして、利用可能なオプションからMACアドレスを選択するか、新しいMACアドレスを入力し、プラスアイコンをクリックして追加します。
[Interface（optional）] フィールド	ドロップダウンリストからインターフェイスを選択します。 （注） 送信元 IP アドレスがネットワークデバイスの場合は、このフィールドが表示されます。
[Port（optional）] フィールド	トレースを開始するホストのポート番号を入力します。
[Destination] フィールド	• トレースを終了するホストまたはレイヤ 3 転送インターフェイスの IP アドレスを入力します。 • [Destination] フィールドをクリックして、使用可能なオプションから IP アドレスを選択します。宛先 IP アドレスのドロップダウンリストは、最大 100 エントリに制限されています。 • [MAC] ドロップダウンをクリックして、利用可能なオプションからMACアドレスを選択するか、新しいMACアドレスを入力し、プラスアイコンをクリックして追加します。

フィールド	アクション
[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） [Destination] フィールドで選択した IP アドレスがネットワークデバイスの場合、このフィールドが表示されます。
[Port（optional）] フィールド	トレースを終了するホストのポート番号を入力します。

ステップ 3 [Options] エリアで、必要に応じて次のタスクを実行します。

フィールド	アクション
[Protocol] ドロップダウンリスト	（オプション）[tcp] または [udp] を選択します。
[Live Traffic]	[On] に切り替えて有効にすると、選択したデバイスを通過するネットワークパケットを .pcap ファイルとしてリアルタイムでキャプチャできます。 [Max number of packets to capture] ドロップダウンリスト：キャプチャするパケットの最大数を選択します。 （注） [Live Traffic] トグルボタンを有効にすると、[Refresh Every 30sec] トグルボタンが自動的に無効になります。その逆も同様です。
[Refresh Every 30sec]	（オプション）パストレーストポロジを 30 秒ごとに更新するように設定するには、このトグルを [On] に設定します。
[ACL Trace]	（オプション）一致した ACL と特定のトラフィックフローの ACL 結果（許可または拒否）を表示するには、このトグルを [On] に設定します。
[Include Stats] オプション	（オプション）追加の統計を収集するようにパストレースを設定するには、必要に応じて次のチェックボックスをオンにします。 • [Device]：デバイス CPU やメモリ使用率などの情報を収集して表示します。 • [Interface]：デバイスインターフェイスに関する情報を収集して表示します。 • [QoS]：collector-voice-egress、collector-broadcast-video-egress、collector-real-time-interactive-egress などの QoS 情報を収集して表示します。

ステップ 4 [Start] をクリックします。
パス トレース トポロジが表示されます。IP アドレス、プロトコル、およびパス トレースの最終更新日時を示すタイムスタンプが、トポロジの上に表示されます。

ステップ 5 パストレーストポロジでは、次のタスクを実行できます。

a) デバイスにカーソルを合わせると、次の情報が表示されます。

- CPU 使用率
- メモリ使用率
- ACL、トンネリング、およびキューの平均処理遅延
- 転送およびドロップされたパケットの数とドロップの理由を含むパケット転送の決定

[ACL Trace] が [On] に設定されている場合、ACL 名と ACL の結果（許可または拒否など）が表示されます。

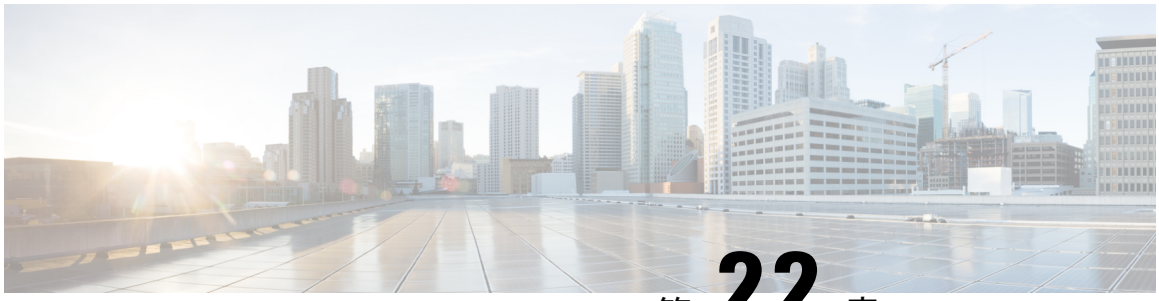
5 タプル値（送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、使用されているプロトコル）が指定されている場合、表示される ACL トレースは 100% 正確です。情報が部分的に指定されている場合、表示される ACL トレースはベストエフォートに基づきます。このような場合、ACL 結果に許可と拒否の両方のステータスが表示される可能性があります。

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 22 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 （533 ページ）
- Cisco CMX API サーバーへのユーザーの追加 （533 ページ）
- Cisco CMX 設定の作成 （534 ページ）
- Cisco CMX のトラブルシューティング （536 ページ）

Cisco Connected Mobile Experiences の統合について

Catalyst Center は、ワイヤレスマップのためのオンプレミス Cisco Connected Mobile Experiences（CMX） の統合をサポートしています。CMX を統合すると、Catalyst Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル（親ノード）で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディングレベルで、大企業の場合はフロアレベルで CMX を割り当てることができます。

（注） セキュリティ上の理由から、CMX は匿名にする必要があります。

Cisco CMX API サーバーへのユーザーの追加

Cisco CMX インスタンスを Catalyst Center ネットワーク設定に追加する前に、Cisco CMX API サーバーにユーザーを追加する必要があります。

手順

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。入力するコマンド

```
ssh -l cmxadmin (cmx-ip-address)
```

ステップ 2 Cisco CMX API サーバーを起動します。入力するコマンド

```
# cmxos apiserver start
```

Example

```
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

ステップ 3 Cisco CMX API サーバーへのユーザーの追加入力するコマンド

```
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

```
[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: Cisco_CMX_web_admin_password
Please re-enter the password for the CMX API Server: Cisco_CMX_web_admin_password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

Cisco CMX 設定の作成

始める前に

- CMX が有効な SSL/TLS 証明書で設定されていることを確認します。CMX 10.5 SSL 証明書のインストール手順 [英語] を参照してください。
- Cisco CMX API ユーザーを追加します。Cisco CMX API サーバーへのユーザーの追加 （533 ページ）を参照してください。

  CMX は Catalyst Center 統合に個別の API リソースを使用するため、CMX で 2 つの同一のユーザーアカウントを設定する必要があります。CLI コマンド **cmxos apiserver user add** を実行し、プロンプトに従ってユーザー名とパスワードを入力して、GUI 管理者ユーザーと一致する CMX API サーバーユーザーを手動で作成する必要があります。CMX では Web GUI パスワード ローテーション ポリシーが適用されるため、管理者 GUI パスワードを変更するたびに、API サーバーユーザーのパスワードも同じ CLI コマンド（**cmxos apiserver user add**）を使用して更新する必要があります。

GUI 管理者ユーザーは /v1 API エンドポイントへの Catalyst Center アクセスを有効にし、API サーバーユーザーは /v3 API エンドポイントへのアクセスを提供します。Catalyst Center の完全な統合には両方が必要です。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。

ステップ 2 [External Services] セクションで、[Cisco Spaces/CMX Servers] をクリックします。

[Cisco Spaces/CMX Servers] ウィンドウが開きます。

ステップ 3 [CMX Servers] テーブルから、[Add] をクリックします。

ステップ 4 [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address]：CMX Web GUI の有効な IP アドレスを入力します。
- [**Username**]：CMX Web GUI の管理者ユーザー名を入力します。

（注） CMX サーバーをサイト、ビルディング、またはフロアに割り当てるには、[Network Hierarchy] に対する書き込み権限が必要です。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Catalyst Center User Role and Permissions」を参照してください。

- [Password]：パスワードログイン情報を入力します。

（注） CMX が到達可能なことを確認します。

ステップ 5 [Add] をクリックします。

接続ステータスは、次の 3 段階で表示されます。

- [Initiating Connection]：サーバーへの接続を確認します。
- [Establishing Trust]：CMX サーバーへの信頼を確立します。CMX サーバーには、信頼を確立するために設定された有効な SSL/TLS 証明書が必要です。証明書が Catalyst Center の信頼できる証明書にまだ保存されていない場合、続行するには証明書を**受け入れる**ように求められます。
- [Connecting CMX Server]：指定されたユーザーログイン情報を検証します。

ステップ 6 CMX サーバーをサイト、建物、またはフロアに割り当てるには、メニューアイコンをクリックし、**[Design]** > **[Network Settings]**の順に選択します。

ステップ 7 [Wireless] タブをクリックします。

ステップ 8 [Global] または必要なエリア、建物、フロアを左側の階層ツリーから、以下を選択します。

ステップ 9 [Cisco Spaces/CMX Servers] をクリックします。

ステップ 10 [**Cisco Spaces/CMX Servers**] セクションで、[**Location Settings**] ドロップダウンリストから CMX サーバーを選択します。

ステップ 11 **[Save]** をクリックします。

[Create CMX Settings] ウィンドウが開きます。

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、Catalyst Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

ステップ 12 フロアマップでは、次のタスクを実行できます。

- 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。[**Info**]、[**Rx Neighbor**]、[**Clients**] タブのあるダイアログボックスが表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアントデバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイドバーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアントトラッキングを実行します。

ステップ 13 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**] ウィンドウで、左側の階層ツリーで変更を加えた建物やフロアの横にある省略記号 ••• にカーソルを合わせ、[**Sync: Cisco Spaces/CMX Servers**] を選択して、変更を手動でプッシュします。

ステップ 14 CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

a) メインメニューから次を選択します。**[System]** > **[Settings]**の順に選択します。
b) [External Services] セクションで、[Cisco Spaces/CMX Servers] をクリックします。
c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
d) 削除する CMX サーバーを選択し、[Delete] をクリックします。
e) [OK] をクリックして削除を実行します。

Cisco CMX のトラブルシューティング

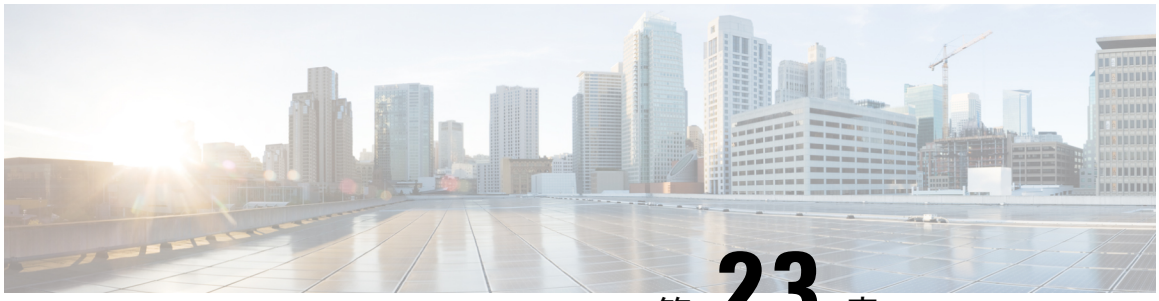
CMX 認証に失敗する場合

- Catalyst 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 ドキュメントリンクを使用して、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 を使用して設定されていて、アクティブになっているかどうかを確認します。
- 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。
- Catalyst 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 23 章

アシュアランス監査ログの表示

• Assurance の監査ログの表示 （539 ページ）

Assurance の監査ログの表示

監査ログは、設定の変更が要求されたとき、設定の変更が実行されたとき、設定中にエラーが発生したかどうかなどの重要なアクティビティを記録するために作成されます。Assurance については、インテリジェントキャプチャ、問題のしきい値、センサー、AI ネットワーク分析の設定が変更されたときに、監査ログが提供されます。

監査ログにアクセスするには、**[アクティビティ]** > **[監査ログ]** の順に選択します。詳細な手順については、*Cisco Catalyst Center Administrator Guide* の「監査ログの表示」を参照してください。

Assurance については、次のデータが監査ログにキャプチャされます。

表 *10* : 監査ログ

アイテム	説明
Date and Time	ログが受信または実行された日時。
Description	監査ログについて簡単な説明。
User	変更を要求または実行したユーザー。

インテリジェントキャプチャの監査ログ

インテリジェントキャプチャについては、次の設定変更をキャプチャするために監査ログが提供されます。

- AP 統計情報のグローバルな有効化/無効化。
- 一連の個々の AP に関する統計情報の有効化/無効化。
- 異常キャプチャのグローバルな有効化/無効化。

- 一連の個々の AP についての異常キャプチャの有効化/無効化。
- スペクトラム解析の有効化。
- スケジュールされたキャプチャの有効化/無効化。
- ライブキャプチャの有効化/無効化。
- データパケットキャプチャの有効化/無効化。

設定中にエラーが発生した場合は、その情報も監査ログに記録されます。

問題のしきい値の監査ログ

問題のしきい値については、次の更新をキャプチャするために監査ログが提供されます。

- サイトの正常性の更新。
- 正常性スコアの更新。
- 問題設定の更新。

センサーの監査ログ

センサーについては、次の設定要求をキャプチャするために監査ログが提供されます。

- テストスイートの追加要求を受信。
- テストスイートの更新要求を受信。
- テストスイートの削除要求を受信。
- 証明書バンドルに関するテストの更新要求を受信。
- テストステータスの追加要求を受信。

AI 分析の監査ログ

AI 分析については、次の AI エージェントの設定変更をキャプチャするために監査ログが提供されます。

- エージェントのオンボード。
- エージェントの復元。
- エージェントの再設定。

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

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

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

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

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