



Cisco DNA アシュアランス リリース 2.3.3 ユーザーガイド

初版：2022年4月26日

最終更新：2023年6月23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)

© 2022–2023 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	新機能および変更された機能に関する情報 1
	Cisco DNA Assurance リリース 2.3.3 の最新情報 1

第 2 章	Cisco DNA アシュアランス の概要 5
	Cisco DNA アシュアランス の概要 5
	アシュアランス のアーキテクチャ 6
	IPv6 アドレスのサポート 7
	ユーザープロファイルの役割および権限 7
	始める アシュアランス 7

第 3 章	Cisco AI Network Analytics の概要 9
	About Cisco AI Network Analytics 9
	Cisco AI ネットワーク分析の利点 11
	Cisco AI Network Analytics のライセンスと導入 12
	Cisco Catalyst 9800 シリーズワイヤレスコントローラでサポートされている Cisco AI Network Analytics の機能 12

第 4 章	アシュアランス を使用するための Cisco DNA Center の設定 15
	アシュアランス の制限事項と制約事項 15
	基本的な設定のワークフロー 15
	デバイスの検出 18
	検出の概要 18
	ディスカバリの前提条件 19
	優先管理 IP アドレス 20

設定のガイドラインと制限事項のディスカバリ	20
CDP を使用したネットワークの検出	21
IP アドレス範囲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	37
ディスカバリ ジョブの管理	44
ディスカバリ ジョブの停止および開始	44
ディスカバリ ジョブの複製	45
ディスカバリ ジョブの削除	45
ディスカバリ ジョブ情報の表示	45
ネットワーク階層の設計	46
ネットワーク階層の概要	46
新しいネットワーク階層の設計	47
既存の Cisco ネットワーク階層の使用	47
マップ内で使用するイメージファイルに関するガイドライン	48
ネットワーク階層のサイトの作成	49
建物の追加	50
建物への基本フロアの追加	50
ネットワーク階層の管理	51
Cisco DNA Center へのサイト階層のインポート	51
ネットワーク階層の検索	52
サイトの編集	53
サイトの削除	53
ビルディングの編集	53
ビルディングの削除	54
フロアの編集	54
2D でのフロアマップのモニタリング	54
2D マップでのフロアマップ要素とオーバーレイの構成	55
フロア ビュー オプション	64
ネットワーク階層マップでのデバイスデータのフィルタ処理	67
インベントリの管理	67
インベントリについて	68

デバイスポーリング間隔の更新	68
インベントリに関する情報の表示	69
ネットワーク デバイスの削除	79
デバイスをサイトに追加する	80
Cisco DNA Center 向けの Cisco ISE の設定について	81
認証サーバとポリシー サーバの設定	82
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	85
Cisco AI Network Analytics データ収集の設定	87
Cisco AI Network Analytics データ収集の無効化	89
機械推論ナレッジベースの更新	90
ローカリゼーションの有効化	91

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 93

企業について	93
企業の全体的な健全性のモニターとトラブルシューティング	93

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 99

ネットワークについて	99
ネットワークの健全性のモニターとトラブルシューティング	99
デバイスの健全性のモニターとトラブルシューティング	109
スイッチおよびルータの重大レベルに満たない選択済み Syslog	124
Cisco StackWise Virtual と制限事項について	125
Cisco StackWise と制限事項について	126
ネットワークデバイスの正常性スコアの設定	127
ファブリック デバイスで SNMP コレクタ メトリックを有効化	128
ネットワークの正常性スコアと KPI メトリックについて	129
ネットワーク ヘルス スコア	130
デバイスカテゴリの正常性スコア	130
個別のデバイス正常性スコア	130
スイッチ ヘルス スコア	131

ルータ ヘルス スコア	133
AP ヘルス スコア	134
ワイヤレス コントローラのヘルス スコア	135
ネットワーク ヘルス 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	136

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	139
クライアントについて	139
すべてのクライアント デバイスの健全性のモニターとトラブルシューティング	139
クライアントデバイスの健全性のモニターとトラブルシューティング	154
有線クライアントのイベントビューアに表示されるメッセージ	161
クライアントの正常性スコアと KPI メトリックについて	161
クライアント ヘルス スコア	162
クライアント オンボーディング スコア	162
クライアント接続スコア	162
個別のクライアント ヘルス スコア	163

第 8 章

アプリケーション健全性のモニター	165
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	165
サポートされるプラットフォーム	166
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	168
アプリケーションの正常性の前提条件	171
アプリケーションテレメトリ設定のプロビジョニング	173
ホストのアプリケーションエクスペリエンスの表示	173
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	175
すべてのアプリケーションの健全性のモニター	176
アプリケーションの健全性のモニター	184
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	189
アプリケーションの正常性スコア設定の設定	193
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	194
全体的なアプリケーション正常性スコア	194
個別アプリケーションの正常性スコア	194

第 9 章	ネットワークサービスの監視	197
	AAA ネットワークサービスの監視	197
	DHCP ネットワークサービスの監視	200

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	205
	SD-Access ファブリック	205
	ファブリックサイトの追加	205
	ファブリックへのデバイスの追加	207
	SD-Access ファブリックの正常性の監視とトラブルシュート	209
	ファブリックサイトの正常性の監視	216
	トランジットおよびピアネットワークの正常性の監視	220
	仮想ネットワークの正常性の監視	225
	仮想ネットワークの正常性スコア	229

第 11 章	問題の表示と管理	231
	問題について	231
	機械推論エンジンについて	232
	VLAN に関連するレイヤ 2 ループの問題について	232
	未解決の問題を表示	233
	AI 駆動型の問題に関与するインスタンスの詳細	237
	レイヤ 2 のループ問題に関与するインスタンスの詳細	241
	PoE の問題に関する問題インスタンスの詳細	244
	MRE を使用した有線クライアントの問題のトラブルシュート	247
	解決済みの問題の表示	250
	無視された問題の表示	252
	問題の解決または無視	254
	無線にアクティビティなしの問題のトリガー	256
	自動問題解決	256
	グローバルな問題の設定の管理	257
	カスタム問題の設定の管理	258

問題の通知の有効化	259
アシュアランス、Cisco AI Network Analytics、および MRE の問題	261
ルータの問題	261
コア層、ディストリビューション層、およびアクセス層に関する問題	263
コントローラの問題	266
アクセスポイントの問題	267
有線クライアントの問題	269
ワイヤレスクライアントの問題	269
AAA 障害の根本原因分析の問題を有効にする	274
アプリケーションの問題	274
センサーの問題	275
AI 駆動型の問題	277
MRE の問題	279
<hr/>	
第 12 章	イベントの表示と管理 281
	イベントダッシュボードの概要 281
	デバイスイベントの表示 281
<hr/>	
第 13 章	センサーの管理とセンサー主導のテスト 285
	センサーとセンサー主導のテストについて 285
	センサーのプロビジョニング 285
	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 285
	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 286
	Cisco Catalyst ワイヤレスコントローラのススコプロビジョニング SSID の有効化 287
	ワイヤレスまたはセンサー デバイスのプロビジョニング 288
	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 291
	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 291
	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 297
	センサーの管理とバックホールの設定 299

ネットワーク内のセンサーの管理	299
バックホールの設定の管理	301
センサデバイスでの永続的なワイヤレスバックホール接続	303
SCEP プロファイルの管理	304
センサー主導テスト	305
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	305
センサー主導テストの管理	310

第 14 章 **Wi-Fi 6E および 6 の対応状況のモニター** 313

Wi-Fi 6E および 6 の対応状況とその利点について	313
Wi-Fi 6E および 6 ネットワークの対応状況の確認	314

第 15 章 **Power over Ethernet の監視** 321

PoE について	321
PoE テレメトリの設定ワークフロー	321
PoE テレメトリに使用するデバイスでの NETCONF の設定	323
PoE テレメトリのテレメトリ設定の更新	325
ネットワーク内の PoE 対応デバイスの監視	326

第 16 章 **不正管理ダッシュボードの監視** 333

ネットワークのセキュリティ脅威の管理	333
--------------------	-----

第 17 章 **Manage Dashboards** 335

ダッシュボードについて	335
カスタムダッシュボードの作成	335
テンプレートからのダッシュボードの作成	336
ダッシュボードの表示	338
ダッシュボードの編集または削除	338
ダッシュボードの複製	339
ダッシュボードをお気に入りにする	339
ダッシュレットの位置の変更	340

第 18 章

ネットワークのトレンドを観察し洞察を得る 341

- ネットワークのトレンドとインサイトについて 341
- ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する 342
- ネットワークトレンドの表示とインサイトの取得 346
- ネットワークヒートマップ内アクセスポイントの比較 351
- KPI 値をネットワーク内のピアと比較 355
- 建物、AP モデルファミリー、およびワイヤレス エンドポイント タイプの比較 357
- 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 360
- 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 363

第 19 章

インテリジェントキャプチャの管理 377

- インテリジェントキャプチャについて 377
- インテリジェントキャプチャ対応デバイス 378
- インテリジェントキャプチャのベストプラクティス 379
- クライアントデバイス向けのライブおよびスケジュール済みキャプチャセッション 380
 - クライアントデバイス向けのキャプチャセッションについて 380
 - クライアント統計情報について 381
 - クライアントデバイスのライブキャプチャセッションの有効化 381
 - クライアントデバイス向けキャプチャセッションのスケジュールと管理 387
- クライアントデバイス向けデータパケットキャプチャ 388
 - クライアントデバイス向けデータパケットキャプチャについて 388
- NAM 統合について 388
 - NAM データポートでの IP アドレス設定 389
 - gRPC コレクタの設定 390
 - クライアントデバイスのデータパケットキャプチャの実行 390
 - クライアントのデータパケットキャプチャ履歴の表示 394
- アクセスポイント向けインテリジェントキャプチャ 395
 - アクセスポイントのインテリジェントキャプチャについて 395
 - アクセスポイントのインテリジェントキャプチャの有効化と管理 396
- RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理 400

	スペクトル解析時の Cisco AP 機能について	405
	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	406
	クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center	406
<hr/>		
第 20 章	デバイスのパスをトレース	409
	パス トレースについて	409
	パス トレースの既知の制限事項	409
	パス トレースの実行	411
<hr/>		
第 21 章	ワイヤレスマップ向け Cisco CMX の統合	415
	Cisco Connected Mobile Experiences の統合について	415
	Cisco CMX API サーバーへのユーザーの追加	415
	Cisco CMX 設定の作成	416
	Cisco CMX のトラブルシューティング	418
<hr/>		
第 22 章	レポート	419
	レポートの概要	419
<hr/>		
第 23 章	アシュアランス監査ログの表示	421
	監査ログの表示 アシュアランス	421
<hr/>		
第 24 章	関連資料	423
	関連資料	423



第 1 章

新機能および変更された機能に関する情報

- [Cisco DNA Assurance リリース 2.3.3 の最新情報 \(1 ページ\)](#)

Cisco DNA Assurance リリース 2.3.3 の最新情報

Cisco DNA Assurance ユーザーガイド、リリース 2.3.3.5 および 2.3.3.0 に記載された新機能と機能変更の概要を次の表に示します。

表 1: Cisco DNA アシュアランス リリース 2.3.3.5 の新機能および機能変更

機能	説明
RF シミュレータ	AI RF シミュレータを使用して、現在の RF プロファイル構成への変更をシミュレートし、[Enhanced RRM] ダッシュボードの拡張 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。 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 (363 ページ) を参照してください。
クライアントダッシュボードのワイヤレスクライアントのトレンドビューの機能強化	クライアントの正常性サマリーでは、ワイヤレスクライアントのトレンドビューが強化されています。放射状棒チャートは、オンボーディングに失敗したクライアントの分布と、オンボーディング失敗の理由を示します。 すべてのクライアント デバイスの健全性のモニターとトラブルシューティング (139 ページ) を参照してください。

表 2: Cisco DNA アシユアランス リリース 2.3.3.0 の新機能および機能変更

機能	説明
Cisco AI Network Analytics : 6 GHz 無線サポート	<p>Cisco AI Network Analytics は、次の機能のために 6 GHz RF をサポートします。</p> <ul style="list-style-type: none"> • ネットワークヒートマップ • AP パフォーマンスアドバイザー • トレンド偏差 (インサイト) • AP RF 統計 • AP スペクトラム解析 <p>ネットワークヒートマップ内アクセスポイントの比較 (351 ページ)、ワイヤレスアクセスポイントのパフォーマンスアドバイザーを表示する (342 ページ)、ネットワークトレンドの表示とインサイトの取得 (346 ページ)、および RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理 (400 ページ) を参照してください。</p>
新しい AP Radio Down の問題	<p>AP の問題に新しい Radio Down の問題が追加されました。Radio Down の問題は、無線がダウンするとトリガーされます。サポートされている無線周波数は、2 GHz、5 GHz、および 6 GHz です。</p> <p>アクセスポイントの問題 (267 ページ) を参照してください。</p>
AP メッシュ : [Device 360] ウィンドウに追加された情報	<p>[Device 360] ウィンドウの [Mesh] タブにメッシュ AP 情報を表示できます。</p> <p>デバイスの健全性のモニターとトラブルシューティング (109 ページ) を参照してください。</p>
新しい AP 無線トラフィック使用率チャート	<p>[AP 360] ウィンドウの [RF] タブの [Detail Information] で、[Traffic Utilization] という新しいグラフを表示できます。このチャートには、受信 (Rx) および送信 (Tx) トラフィック使用率の情報が含まれています。さらに、Rx および Tx トラフィック使用率情報が [Channel Utilization] チャートに追加されました。</p> <p>デバイスの健全性のモニターとトラブルシューティング (109 ページ) を参照してください。</p>
[AP Radio Comparison View] に追加された追加の AP 無線チャンネル使用率メトリック	<p>[デバイス 360] ウィンドウでは、次の追加の KPI によって AP 無線を比較できます。</p> <ul style="list-style-type: none"> • トラフィック使用率 • Tx トラフィック使用率 • Rx トラフィック使用率 <p>デバイスの健全性のモニターとトラブルシューティング (109 ページ) を参照してください。</p>

機能	説明
パストレースの拡張機能	<p>パストレースの結果には、ACL、トンネリング、およびキューの平均処理遅延、およびパケットドロップ決定の理由が含まれます。</p> <p>パストレースの実行 (411 ページ) を参照してください。</p>
Cisco SD-Access : ランジットネットワークとピアネットワーク	<p>SD-Access 健全性ダッシュボードで、トランジットネットワークとピアネットワークの健全性を監視できます。</p> <p>トランジットおよびピアネットワークの正常性の監視 (220 ページ) を参照してください。</p>
Cisco AI Network Analytics : ネットワークヒートマップのローミング KPI	<p>ネットワークヒートマップは、次のローミング KPI をサポートしています。</p> <ul style="list-style-type: none"> • 正常な着信ローミングイベント • 正常な発信ローミングイベント • 着信ローミングイベントの合計 <p>ネットワークヒートマップ内アクセスポイントの比較 (351 ページ) を参照してください。</p>
Cisco AI Network Analytics : ピア比較 KPI	<p>ピア比較では、次の KPI がサポートされています。</p> <ul style="list-style-type: none"> • オンボーディングエラーソース : ネットワーク内のオンボーディングエラーソースをピアのオンボーディングエラーソースと比較します • ローミングエラーソース : ネットワークのローミングエラーソースをピアのローミングエラーソースと比較します <p>KPI 値をネットワーク内のピアと比較 (355 ページ) を参照してください。</p>
Intel 分析のサポート	<p>[Client 360] ウィンドウの [Detail Information] に、[Intel Connectivity Analytics] タブが新たに追加されました。このタブは、Intel ワイヤレスアダプターでサポートされているデバイスでのみ使用できます。</p> <p>クライアントデバイスの健全性のモニターとトラブルシューティング (154 ページ) を参照してください。</p>
クライアントダッシュボードの強化	<p>アシュアランス [Client] ダッシュボードの [Client Devices] ダッシュレットには、クライアントを追跡し、ネットワークで検出されたときにクライアントに通知できる [Tracked Client] が含まれています。</p> <p>すべてのクライアントデバイスの健全性のモニターとトラブルシューティング (139 ページ) を参照してください。</p>

機能	説明
Cisco SD-Access : LISP と Pub/Sub セッション	<p>[SD-Access Health] で、ファブリックサイトにおける [LISP] と [Pub/Sub] のセッションの監視がサポートされます。これらの KPI は、ファブリックサイト、SD-Access トランジット、トランジットコントロールプレーン、およびデバイスの正常性の計算に含まれています。</p> <p>ファブリックサイトの正常性の監視 (216 ページ)、仮想ネットワークの正常性の監視 (225 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 (220 ページ)、および デバイスの健全性のモニターとトラブルシューティング (109 ページ) を参照してください。</p>
デバイスのイベント	<p>このリリース以前は、イベントは [Device] ウィンドウにのみ表示されていました。現在、[Events] ダッシュボードは、デバイスイベントのよりコンテキストに応じた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、アシュアランスがこれらの詳細を提供します。</p> <p>イベントの表示と管理 (281 ページ) を参照してください。</p>



第 2 章

Cisco DNA アシュアランスの概要

- [Cisco DNA アシュアランスの概要 \(5 ページ\)](#)
- [アシュアランスのアーキテクチャ \(6 ページ\)](#)
- [IPv6 アドレスのサポート \(7 ページ\)](#)
- [ユーザープロファイルの役割および権限 \(7 ページ\)](#)
- [始めるアシュアランス \(7 ページ\)](#)

Cisco DNA アシュアランスの概要

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

アシュアランスには、次のような利点があります。

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

アシユアランスのアーキテクチャ

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

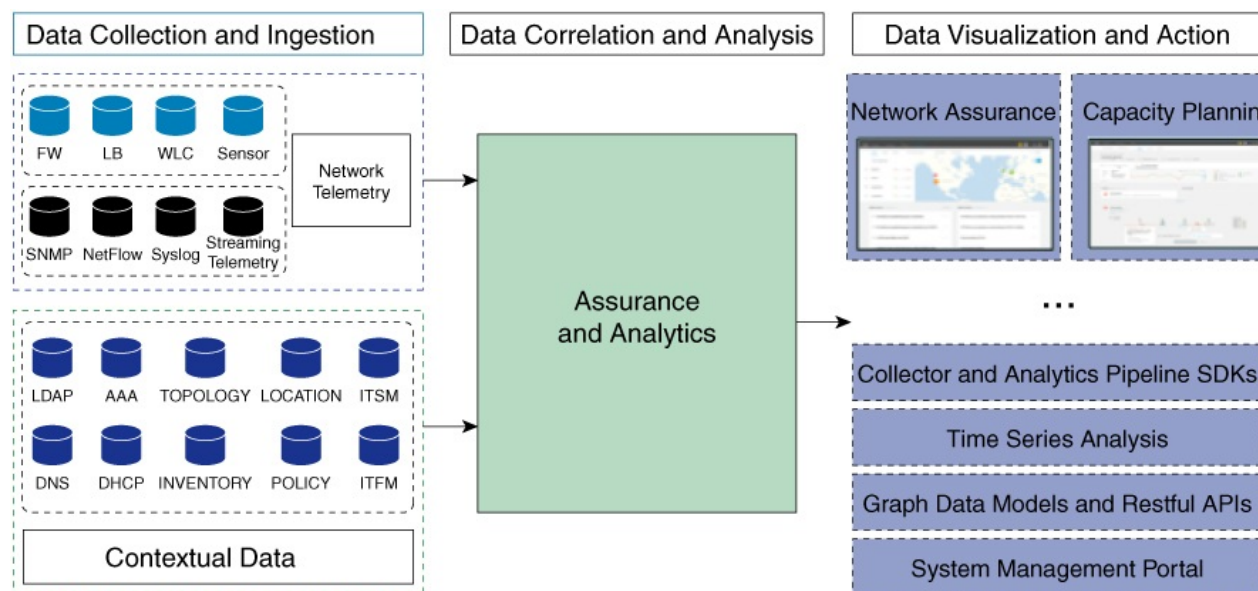
アシユアランスは多目的でリアルタイムのネットワークデータの収集および分析エンジンであり、これによりネットワークデータのビジネスにおける可能性を大幅に向上させることができます。

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

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

次の図とその後の情報で、アシユアランスアーキテクチャについて説明します。

図 1: アシユアランスアーキテクチャ



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

- **データの可視化とアクション**：データはデータベースに保存され、API を介してアシユアランス 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。アシユアランス は、以下を提供するオープンシステムです。

- コレクタと分析パイプライン SDK
- 時系列分析
- グラフデータモデルと RESTful API
- システム管理ポータル

IPv6 アドレスのサポート

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

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

ユーザープロファイルの役割および権限

Cisco DNA 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。ユーザープロファイルに割り当てられたロールは、ユーザーが実行する権限を持つ機能を定義します。Cisco DNA Center には、SUPER-ADMIN-ROLE、NETWORK-ADMIN-ROLE、および OBSERVER-ROLE 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 は、ユーザーに幅広い機能を提供し、カスタムロールの作成やユーザープロファイルへの割り当てなど、Cisco DNA Center GUI ですべてのアクションを実行できるようにします。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Cisco DNA Center GUI での機能が制限されます。

Cisco DNA Center でアクションを実行できない場合、それを許可しないロールがユーザープロファイルに割り当てられていることが原因である可能性があります。詳細については、システム管理者に確認するか、または [Cisco DNA Center 管理者ガイド](#) を参照してください。

始める アシユアランス

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

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

- 既存のインフラストラクチャ：既存のインフラストラクチャ（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 \(15 ページ\)](#) を参照してください。
- 新規または存在しないインフラストラクチャ：既存のインフラストラクチャがなく、ゼロから開始（新規導入）する場合は、ネットワーク階層を設計します。ネットワーク階層の設計については、[Cisco DNA Center ユーザガイド](#) を参照してください。



第 3 章

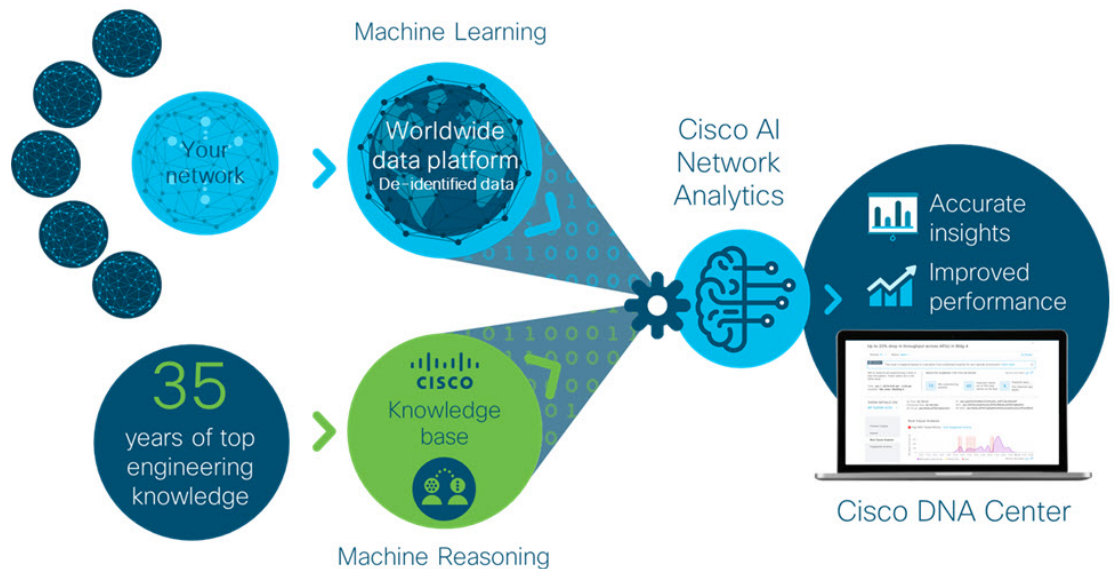
Cisco AI Network Analytics の概要

- [About Cisco AI Network Analytics](#) (9 ページ)
- [Cisco AI ネットワーク分析の利点](#) (11 ページ)
- [Cisco AI Network Analytics のライセンスと導入](#) (12 ページ)
- [Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポートされている Cisco AI Network Analytics の機能](#) (12 ページ)

About Cisco AI Network Analytics

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

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



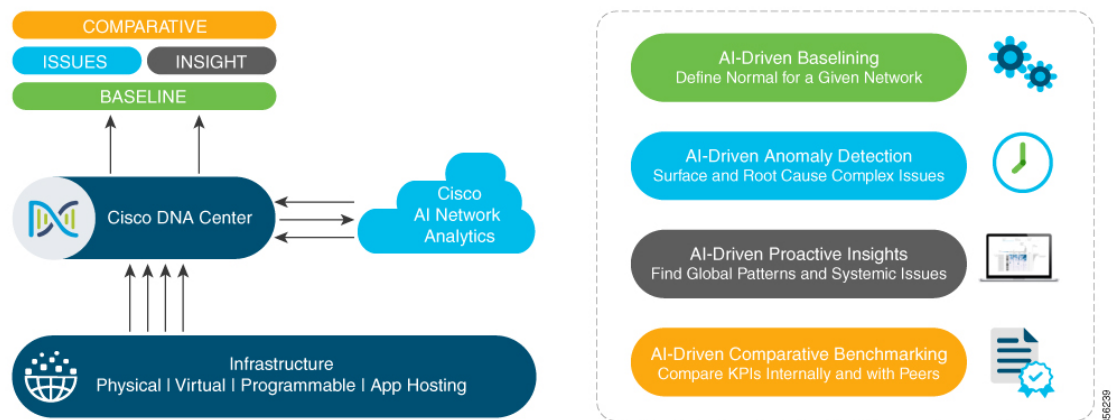
Cisco AI Network Analytics 構成は次のとおりです。

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

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 DNA アシユアランス と完全に統合された Cisco DNA Center のシンプルかつ直感的で強力なユーザーインターフェイスを駆使して、こうした価値を提供します。

図 3: Cisco AI Network Analytics 機能



Cisco AI Network Analytics は、次のとおりです。

- **クラウドベースのインフラストラクチャ**：ネットワークイベント情報が Cisco DNA Center で非識別化され、セキュアな暗号化チャネルを介して Cisco AI Network Analytics クラウドベースのインフラストラクチャに送信されます。Cisco AI Network Analytics クラウドは、このような非識別化されたネットワークイベントデータに対して機械学習モデルを実行し、問題点と包括的なインサイトを Cisco DNA Center に返します。
- [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 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**（イ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 駆動型 AP 比較**：ヒートマップ内の特定の月について、ネットワーク内のすべての AP を比較してトレンドを把握し、洞察を得ます。
 - **AI 駆動型のピア比較**：選択した主要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。
 - [AI-Driven Network Comparisons]：選択した 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 ネットワーク分析の利点

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

- [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ベースラインを作成します。これらの基準は、ネットワーク環境の変化に応じて、デバイス数、ユーザー数、およびアプリケーション数が増加するのに伴い、学習し適応します。

- **インサイトの向上** : Cisco AI Network Analytics では、機械学習を使用して、ネットワークからの膨大な量のデータを個別のネットワーク基準値に関連付け、ネットワークに重大な影響をもたらす問題を明らかにします。これにより、問題の関連性が絞り込まれます。Cisco AI Network Analytics は、ネットワーク動作の傾向とパターンを検出し、具体的な問題が派生する前に問題を特定できるようにします。
- **[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、Cisco DNA Center の Cisco DNA Advantage ソフトウェアライセンスの一部で、アシュアランスのユーザーインターフェイスとシームレスに統合される、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り生成されたインサイトと問題が提供され、機械学習エンジンで発生した問題の分析、トラブルシューティング、および対応に必要な可視化ツールも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）Cisco DNA Center の実行インスタンスと、Cisco AI Network Analytics クラウドへの HTTPS 接続が必要です。HTTPS 接続は、プロキシサーバーを介してもサポートされます。HTTPS 接続にプロキシサーバーを使用する場合、設定は Cisco DNA Center グローバル設定から継承されます。ネットワークイベントデータは、クラウドに送信される前に非特定化されます。結果とインサイトは Cisco AI Network Analytics クラウドサービスによって返され、復号された後、アシュアランス ユーザーインターフェイスに直接表示されます。詳細については、「[Cisco AI Network Analytics Privacy Data Sheet](#)」を参照してください。

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

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

Cisco DNA Center リリース	サポートされる機能	Cisco IOS-XE の最小ソフトウェアバージョン
2.3.3	<ul style="list-style-type: none">• 接続の問題の特定 : Cisco AI Network Analytics は、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、スループットの問題などのオンボーディングの問題を特定できます。• 傾向の特定と洞察	16.12.1s



第 4 章

アシュアランス を使用するための Cisco DNA Center の設定

- [アシュアランス の制限事項と制約事項 \(15 ページ\)](#)
- [基本的な設定のワークフロー \(15 ページ\)](#)
- [デバイスの検出 \(18 ページ\)](#)
- [ネットワーク階層の設計 \(46 ページ\)](#)
- [インベントリの管理 \(67 ページ\)](#)
- [デバイスをサイトに追加する \(80 ページ\)](#)
- [Cisco DNA Center 向けの Cisco ISE の設定について \(81 ページ\)](#)
- [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 \(85 ページ\)](#)
- [Cisco AI Network Analytics データ収集の設定 \(87 ページ\)](#)
- [機械推論ナレッジベースの更新 \(90 ページ\)](#)
- [ローカリゼーションの有効化 \(91 ページ\)](#)

アシュアランス の制限事項と制約事項

アシュアランス 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。

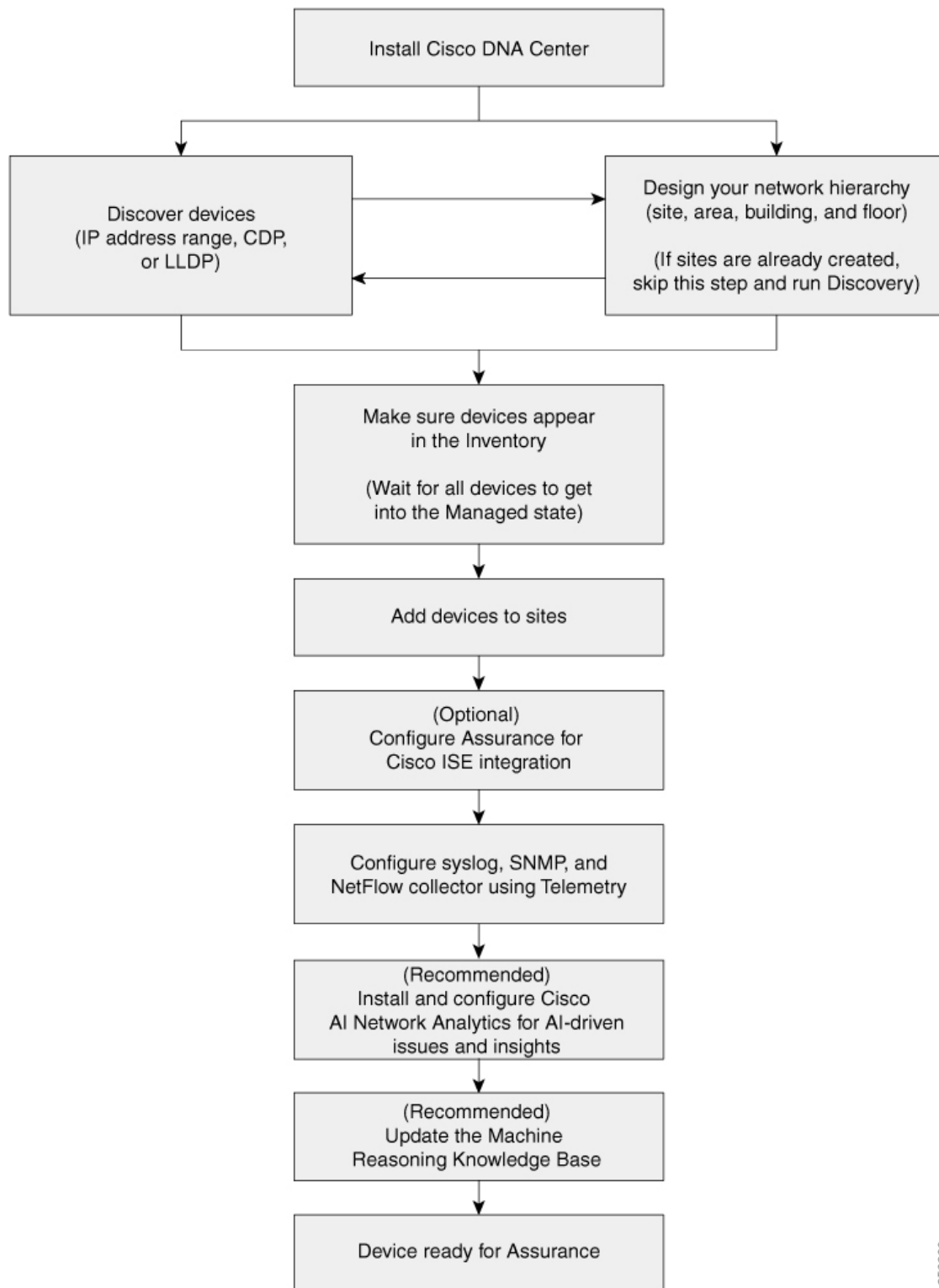
基本的な設定のワークフロー

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

ここでは、アシュアランスを設定するために実行する必要がある基本タスクについて説明します。この章は、[Cisco DNA Center ユーザーガイド](#) と併用してください。

基本的なワークフローを理解するために、次の図と次の手順を参照してください。

図 4: アシュアランスを使用するための Cisco DNA Center の設定の基本的なワークフロー



356269

始める前に

アシュアランスの制限事項と制約事項 (15 ページ) を参照してください。

ステップ 1 Cisco DNA Center をインストールします。

[Cisco DNA Center 設置ガイド](#)を参照してください。

ステップ 2 任意の順序で次の操作を行います。

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

[IP アドレス範囲を使用したネットワークの検出 \(29 ページ\)](#)、[CDP を使用したネットワークの検出 \(21 ページ\)](#)、および[LLDP を使用したネットワークの検出 \(37 ページ\)](#) を参照してください。

(注) 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。

[新しいネットワーク階層の設計 \(47 ページ\)](#) または [既存の Cisco ネットワーク階層の使用 \(47 ページ\)](#) を参照してください。

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

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

[インベントリに関する情報の表示 \(69 ページ\)](#) を参照してください。

(注) 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

[デバイスをサイトに追加する \(80 ページ\)](#) 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。

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、アシュアランスを設定して Cisco ISE を統合できます。統合することで、アシュアランスのユーザー名やオペレーティングシステムなど、有線クライアントの詳細な情報を参照できます。

[Cisco DNA Center 向けの Cisco ISE の設定について \(81 ページ\)](#) 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 \(85 ページ\)](#) を参照してください。

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

[Cisco AI Network Analytics データ収集の設定 \(87 ページ\)](#) 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 \(90 ページ\)](#) を参照してください。

ステップ 10 アシュアランス アプリケーションの使用を開始します。

デバイスの検出

Cisco DNA 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

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

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

デバイスは次の 3 つの方法で検出できます。

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

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

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



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

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



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

ディスカバリの前提条件

ディスカバリを実行する前に、次の最小要件を満たしてください。

- 『[Cisco DNA Center Compatibility Matrix](#)』を参照して、Cisco DNA Center によって検出されるデバイスを把握してください。
- Cisco DNA Center とデバイス間の望ましいネットワーク遅延は 100 ミリ秒のラウンドトリップ時間 (RTT) であることに注意してください（最大遅延は 200 ミリ秒 RTT です）。
- Cisco DNA Center が使用できるように 1 つ以上の SNMP クレデンシャルがデバイス上で設定されていることを確認してください。少なくとも、これには SNMPv2C 読み取りクレデンシャルを使用できます。
- Cisco DNA Center に検出させ、管理委させるデバイスの SSH クレデンシャルを設定します。以下の基準のうち、少なくとも 1 つが満たされる場合、Cisco DNA Center はデバイスを検出し、そのインベントリに追加します。
 - デバイスへの SSH アクセスのために Cisco DNA Center が使用するアカウントが、特権 EXEC モード（レベル 15）である。
 - ディスカバリ ジョブで設定される CLI クレデンシャルの一部としてデバイスのイネーブルパスワードを設定している。詳細については、[設定のガイドラインと制限事項のディスカバリ](#)（20 ページ）を参照してください。

優先管理 IP アドレス

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

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

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

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

設定のガイドラインと制限事項のディスカバリ

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

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

- 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。

CDP を使用したネットワークの検出

Cisco Discovery Protocol (CDP) IP アドレス範囲、または LLDP を使用してデバイスを検出できます。この手順では、CDP を使用してデバイスとホストを検出する方法を示します。



- (注)
- ディスカバリ機能では、正しい SNMP 読み取り専用コミュニティストリングが必要です。SNMP 読み取り専用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 読み取り専用コミュニティストリングである public を使用します。
 - 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 \(19 ページ\)](#) 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 IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 メニューアイコン (☰) をクリックして、[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 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

- [Discovery Type] : [CDP] オプションボタンをクリックして CDP を有効にします。
- [IP Address] : シード IP アドレスを入力し、Cisco DNA Center でディスカバリスキャンを開始します。
- [Subnet Filter] : ディスカバリスキャンから IP アドレスまたはサブネットを除外します。IP アドレスを除外するには、個々の IP アドレス (x.x.x.x) を入力します。サブネットを除外するには、Classless Inter-Domain Routing (CIDR) アドレス (x.x.x.x/y) を入力します。ここで、x.x.x.x は IP アドレス、y はサブネットマスクです。サブネットマスクは、0 ~ 32 の値です。

IP アドレスとサブネットをさらに除外するには、追加アイコン (+) をクリックします。

- [CDP Level] : 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。
- [Preferred Management IP Address] : 次のいずれかのオプションボタンをクリックします。
 - [None] : デバイスが任意の IP アドレスを使用できるようにします。
 - [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、Cisco DNA Centerは**優先管理 IP アドレス (20 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。
 - (注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、CDP ネイバーの IP アドレスが Cisco DNA Center から到達可能であることを確認します。

ステップ 5 [Credentials] エリアを展開し、使用するログイン情報を選択します。
すでに作成されているグローバルクレデンシャルのいずれかを選択するか、独自のディスカバリクレデンシャルを設定します。

ステップ 6 既存のログイン情報を使用するには、使用するグローバルログイン情報を選択し、ステップ 14に進みます。そのクレデンシャルを使用しない場合は、選択解除します。

ステップ 7 新しいログイン情報を設定するには、[Add Credentials] をクリックします。
(注) 自身のログイン情報を設定する場合は、[Save as global settings] チェックボックスをオンにして、将来の検出ジョブのためにそれらを保存できます。

ステップ 8 CLI クレデンシャルの場合は、次の手順を実行します。

- a) 次のフィールドを設定します。

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。
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	<p>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が必要な場合にのみ、このパスワードを設定します。</p> <p>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。</p> <p>(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。</p>

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 9 SNMP v2c ログイン情報の場合は、[SNMP v2c] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 4: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 10 (任意) SNMP v3 ログイン情報の場合は、[SNMP v3] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 5: SNMPv3 のクレデンシャル

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

フィールド	説明
Privacy Type	<p>プライバシータイプ。 ([Mode] として [AuthPriv] を選択した場合に有効になります)。 次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 検出機能とインベントリ機能は、 CISCOAES192 プライバシータイプと CISCOAES256 プライバシータイプのみをサポートします。 • Cisco DNA アシュアランスは、 これらのプライバシータイプをサポートしていません。
Privacy Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコ ワイヤレス コントローラでは、 パスワード (あるいはパスフレーズ) は少なくとも 12 文字以上である必要があります。 ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。 パスワードに必要な最低限の文字数が守られないと、 デバイスではCisco DNA Centerによる検出、 監視、 管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、 この設定では表示されません。

- b) これらのログイン情報を後で使用するために保存する場合は、 [Save as global settings] 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しなかった場合、 ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 11 (任意) SNMP プロパティを設定するには、 [SNMP PROPERTIES] をクリックし、 次の手順を実行します。

- a) 次のフィールドを設定します。

表 6: SNMP のプロパティ

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

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 12 (任意) HTTP ログイン情報を設定するには、[HTTP (S)] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 7: 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、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

- b) (任意) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 13 (任意) NETCONF が有効になっているネットワークデバイスがあり、Cisco DNA Center で NETCONF を使用してそれらのデバイスの構成をインストール、操作、および削除する場合は、[NETCONF] をクリックして次の手順を実行します。

- a) [Port] フィールドに、ポート番号を入力します。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
 - Cisco DNA 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のみ、カスタムポートを使用できます詳細については、[Cisco DNA Center 管理者ガイド](#)の「Device Controllability」の項を参照してください)

(注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。

(注) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にする必要があります。

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 14 (任意) デバイスとの接続に使用されるプロトコルを設定するには、[Advanced] エリアを展開し、次の手順を実行します。

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

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

- b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

(注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。

ステップ 15 [Discover] をクリックします。

ステップ 16 今すぐ検出を実行するには、[Discover Devices] スライドインペインで [Now] オプションボタンをクリックし、[Start] をクリックします。それ以外の場合は、次のステップに進みます。

新しいデバイスのみを検出する場合は、[Discover only new devices] トグルボタンをクリックします。

ステップ 17 後で検出するようにスケジュールを設定するには、次の手順を実行します。

1. [Later] ラジオボタンをクリックします。
2. 開始日時を定義します。
3. [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
4. [Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。
 - [None] : 検出は繰り返されません。
 - [Daily] : [Run at Interval (Days)] フィールドに間隔を日単位で入力します。
 - [Weekly]:[Run at Interval (Weeks)] フィールドに間隔を週単位で入力します。
5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。

(注) 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。
6. [End Date] または [End After] をクリックします。
 - [End Date] : 繰り返しを終了する月、日付、年を入力します。
 - [End After] : 繰り返しを終了するまでの回数を入力します。

7. [Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出を表示します。検出を開始する前に、[Edit] をクリックして編集するか、または [Cancel] をクリックしてキャンセルできます。

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

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

IP アドレス範囲を使用したネットワークの検出

IP アドレス範囲、CDP、または LLDP を使用してデバイスを検出できます。この手順では、IP アドレス範囲を使用してデバイスとホストを検出する方法を示します。

始める前に

[ディスカバリの前提条件 \(19 ページ\)](#) で説明されているように、デバイスには必須のデバイス設定が存在する必要があります。

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

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 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

- [Discovery Type] : [IP Address/Range] オプションボタンをクリックし、IP アドレスまたはアドレス範囲を使用してデバイスを検出します。
- [From] および [To] フィールド : [From] フィールドに開始 IP アドレスを入力し、[To] フィールドに終了 IP アドレスを入力します。

IP アドレス範囲を追加するには、追加アイコン ([+]) をクリックします。

(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 のウィンドウでは、データが表示されません。

- [Subnet Filter] : ディスカバリスキャンから IP アドレスまたはサブネットを除外します。IP アドレスを除外するには、個々の IP アドレス (x.x.x.x) を入力します。サブネットを除外するには、Classless Inter-Domain Routing (CIDR) アドレス (x.x.x.x/y) を入力します。ここで、x.x.x.x は IP アドレス、y はサブネットマスクです。サブネット マスクは、0 ~ 32 の値です。

IP アドレスとサブネットをさらに除外するには、追加アイコン (+) をクリックします。

- [Preferred Management IP Address] : 次のいずれかのオプションボタンをクリックします。

- [None] : デバイスが任意の IP アドレスを使用できるようにします。
- [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、Cisco DNA Centerは**優先管理 IP アドレス (20 ページ)** で説明されているロジックを使用して、管理 IP アドレスを選択します。

- ステップ 5** [Credentials] エリアを展開し、使用するログイン情報を選択します。
 すでに作成されているグローバルクレデンシャルのいずれかを選択するか、独自のディスカバリクレデンシャルを設定します。
- ステップ 6** 既存のログイン情報を使用するには、使用するグローバルログイン情報を選択し、ステップ 14に進みます。そのクレデンシャルを使用しない場合は、選択解除します。
- ステップ 7** 新しいログイン情報を設定するには、[Add Credentials] をクリックします。
 (注) 自身のログイン情報を設定する場合は、[Save as global settings] チェックボックスをオンにして、将来の検出ジョブのためにそれらを保存できます。
- ステップ 8** CLI クレデンシャルの場合は、次の手順を実行します。
 a) 次のフィールドを設定します。

表 8: CLI クレデンシャル

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

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。

- c) [Save] をクリックします。

ステップ 9 SNMP v2c ログイン情報の場合は、[SNMP v2c] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 9: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 10 (任意) SNMP v3 ログイン情報の場合は、[SNMP v3] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 10: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。

フィールド	説明
Auth Type	<p>使用する認証タイプ（[Mode] として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5] : HMAC-MD5 に基づく認証。
Auth Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシータイプ。（[Mode] として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 検出機能とインベントリ機能は、CISCOAES192 プライバシータイプと CISCOAES256 プライバシータイプのみをサポートします。 • Cisco DNA アシュアランスは、これらのプライバシータイプをサポートしていません。

フィールド	説明
Privacy Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 11 (任意) SNMP プロパティを設定するには、[SNMP PROPERTIES] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 11: SNMP のプロパティ

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

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 12 (任意) HTTP ログイン情報を設定するには、[HTTP (S)] をクリックし、次の手順を実行します。

- a) 次のフィールドを設定します。

表 12: 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、[読み取り (Read)] または [書き込み (Write)] です。
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

- b) (任意) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 13 (任意) NETCONF が有効になっているネットワークデバイスがあり、Cisco DNA Center で NETCONF を使用してそれらのデバイスの構成をインストール、操作、および削除する場合は、[NETCONF] をクリックして次の手順を実行します。

- a) [Port] フィールドに、ポート番号を入力します。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
 - Cisco DNA 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のみ、カスタムポートを使用できます詳細については、[Cisco DNA Center 管理者ガイド](#)の「Device Controllability」の項を参照してください)

(注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。

(注) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスを検出するには、NETCONF を有効にする必要があります。

- b) これらのログイン情報を後で使用するために保存する場合は、[Save as global settings] 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しなかった場合、ログイン情報を使用できるのは現在の検出ジョブに対してのみです。
- c) [Save] をクリックします。

ステップ 14 (任意) デバイスとの接続に使用されるプロトコルを設定するには、[Advanced] エリアを展開し、次の手順を実行します。

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

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

- b) 使用する順序でプロトコルをドラッグ アンド ドロップします。

(注) [Add Discovery] ウィンドウの [Advanced] エリアで [Telnet] プロトコルを選択すると、NETCONF は無効になります。

ステップ 15 [Discover] をクリックします。

ステップ 16 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。それ以外の場合は、次のステップに進みます。

新しいデバイスのみを検出する場合は、[Discover only new devices] トグルボタンをクリックします。

ステップ 17 後で検出するようにスケジュールを設定するには、次の手順を実行します。

1. [Later] ラジオボタンをクリックします。
2. 開始日時を定義します。
3. [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
4. [Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。
 - [None] : 検出は繰り返されません。
 - [Daily] : [Run at Interval (Days)] フィールドに間隔を日単位で入力します。
 - [Weekly]:[Run at Interval (Weeks)] フィールドに間隔を週単位で入力します。
5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。

(注) 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。
6. [End Date] または [End After] をクリックします。
 - [End Date] : 繰り返しを終了する月、日付、年を入力します。
 - [End After] : 繰り返しを終了するまでの回数を入力します。

7. [Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出を表示します。検出を開始する前に、[Edit] をクリックして編集するか、または [Cancel] をクリックしてキャンセルできます。

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

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

LLDP を使用したネットワークの検出

Link Layer Discovery Protocol (LLDP)、CDP、または IP アドレス範囲を使用してデバイスを検出できます。この手順では、LLDP を使用してデバイスとホストを検出する方法を示します。



- (注)
- 検出には、SNMP 読み取り専用コミュニティストリングが必要です。SNMP 読み取り専用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、検出ではデフォルトの SNMP 読み取り専用コミュニティストリングである **public** が使用されます。
 - CLI ログイン情報はホストの検出には必要ありません。ホストは接続されているネットワークデバイスを介して検出されます。

始める前に

- ネットワークデバイスで LLDP を有効にします。
- [ディスカバリの前提条件 \(19 ページ\)](#) で説明されているように、ネットワークデバイスを設定します。
- クライアント IP アドレスとしてネットワークデバイスのホストの IP アドレスを設定します。(A host is an end-user device, such as a laptop computer or mobile device.)

ステップ 1 メニューアイコン (☰) をクリックして、[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 [New Discovery] ウィンドウの [Discovery Name] フィールドに、名前を入力します。

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

- [Discovery Type] : [LLDP] オプションボタンをクリックして LLDP を有効にします。
- [IP Address] : シード IP アドレスを入力し、Cisco DNA Center でディスカバリスキャンを開始します。

- [Subnet Filter] : ディスカバリスキャンから IP アドレスまたはサブネットを除外します。IP アドレスを除外するには、個々の IP アドレス (x.x.x.x) を入力します。サブネットを除外するには、Classless Inter-Domain Routing (CIDR) アドレス (x.x.x.x/y) を入力します。ここで、x.x.x.x は IP アドレス、y はサブネットマスクです。サブネット マスクは、0 ~ 32 の値です。

IP アドレスとサブネットをさらに除外するには、追加アイコン (+) をクリックします。

- [LLDP Level] : 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。

- [Preferred Management IP Address] : 次のいずれかのオプションボタンをクリックします。

- [None] : デバイスが任意の IP アドレスを使用できるようにします。
- [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、Cisco DNA Center は [優先管理 IP アドレス \(20 ページ\)](#) で説明されているロジックを使用して、管理 IP アドレスを選択します。
(注) ループバック インターフェイスの IP アドレスを優先管理 IP アドレスとして使用するには、LLDP ネイバーの IP アドレスが Cisco DNA Center から到達可能であることを確認します。

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

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

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

表 13: CLI クレデンシャル

フィールド	説明
Name/Description	CLI クレデンシャルを説明する名前または語句。
Username	ネットワーク内のデバイスの CLI にログインするために使用する名前。
Password	ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。 セキュリティ上の理由から、確認のためにパスワードを再入力します。 (注) パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Enable Password	<p>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。</p> <p>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。</p> <p>(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。</p>

d) [SNMP v2c] をクリックして、次のフィールドを設定します。

表 14: SNMPv2c のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

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

表 15: SNMPv3 のクレデンシャル

フィールド	説明
Name/Description	追加した SNMPv3 設定の名前または説明。
Username	SNMPv3 設定に関連付けられている名前。
Mode	<p>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。</p> <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。

フィールド	説明
Auth Type	<p>使用する認証タイプ（[Mode]として [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。</p> <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5] : HMAC-MD5 に基づく認証。
Auth Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 一部のシスコワイヤレスコントローラでは、パスワード（あるいはパスフレーズ）は少なくとも12文字以上である必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
Privacy Type	<p>プライバシータイプ。（[Mode]として [AuthPriv] を選択した場合に有効になります）。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 検出機能とインベントリ機能は、CISCOAES192プライバシータイプとCISCOAES256プライバシータイプのみをサポートします。 • Cisco DNA アシュアランスは、これらのプライバシータイプをサポートしていません。

フィールド	説明
Privacy Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

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

表 16: SNMP のプロパティ

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

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

表 17: 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、[読み取り (Read)] または [書き込み (Write)] です。

フィールド	説明
Read	<p>最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

フィールド	説明
Write	<p>最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。</p> <ul style="list-style-type: none"> • [Name/Description] : 追加している HTTPS ログイン情報の名前または説明。 • [Username] : HTTPS 接続の認証に使用される名前です。 • [Password] : HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 • [Port] : HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443 (HTTPS の既知のポート) です。 <p>パスワードは 7 ~ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。</p> <ul style="list-style-type: none"> • 小文字の英字 (a ~ z) • 大文字の英字 (A ~ Z) • 数字 (0 ~ 9) • 特殊文字 (: # _ * ?) - <p>パスワードにスペースや山カッコ (<>) は使用できません。一部の Cisco IOS XE デバイスでは、疑問符 (?) を使用できないので注意してください。</p>

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

- a) 使用するプロトコルの名前をクリックします。緑のチェックマークはプロトコルが選択されていることを示します。有効なプロトコルは、[SSH] (デフォルト) および [Telnet] です。
- b) 使用する順序でプロトコルをドラッグアンドドロップします。

ステップ 7 [Discover] をクリックします。

[Discover Devices] スライドインペインが表示されます。

ステップ 8 今すぐ検出を実行するには、[Now] ラジオボタンをクリックし、[Start] をクリックします。

新しいデバイスのみを検出する場合は、[Discover only new devices] トグルボタンをクリックします。

ステップ 9 後で検出するようにスケジュールを設定するには、次の手順を実行します。

1. [Later] ラジオボタンをクリックします。
2. 開始日時を定義します。
3. [Time Zone] ドロップダウンリストから、タイムゾーンを選択します。
4. [Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。

- [None] : 検出は繰り返されません。
 - [Daily] : [Run at Interval (Days)] フィールドに間隔を日単位で入力します。
 - [Weekly]:[Run at Interval (Weeks)] フィールドに間隔を週単位で入力します。
5. 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End] チェックボックスをオンにして終了日時を定義します。
- (注) 繰り返しでは、新しいデバイスのみを検出できます。上部に表示される [Discover only new devices] トグルボタンは、デフォルトで有効になっています。
6. [End Date] または [End After] をクリックします。
- [End Date] : 繰り返しを終了する月、日付、年を入力します。
 - [End After] : 繰り返しを終了するまでの回数を入力します。
7. [Start] をクリックします。

通知アイコンをクリックして、スケジュールされた検出を表示します。検出を開始する前に、[Edit] をクリックして編集するか、または [Cancel] をクリックしてキャンセルできます。

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

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

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

- ステップ 1** メニューアイコン (☰) をクリックして、[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** アクティブなディスカバリ ジョブを停止するには、次の手順を実行します。
- a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
 - b) 下部ペインの右側で、[Stop] をクリックします。
- ステップ 4** 非アクティブなディスカバリ ジョブを再起動するには、次の手順を実行します。
- a) 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。
 - b) 下部ペインの右側で、[Re-discover] をクリックします。

ディスカバリ ジョブの複製

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

始める前に

少なくとも1つのディスカバリ ジョブを実行する必要があります。

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

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 左側の [Discoveries] ペインで、ディスカバリジョブをクリックします。

ステップ 4 下部ペインの右側で、[Copy & Edit] をクリックします。

Cisco DNA 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ず。

ステップ 5 (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 6 新しいディスカバリ ジョブのパラメータを定義または更新します。

ディスカバリ ジョブの削除

アクティブまたは非アクティブに関係なく、検出ジョブを削除できます。

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

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 左側の [Discoveries] ペインで、削除するディスカバリジョブをクリックします。

ステップ 4 下部ペインの右側で、[Delete] をクリックします。

ステップ 5 [OK] をクリックして確定します。

ディスカバリ ジョブ情報の表示

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

始める前に

少なくとも1つのディスカバリジョブを実行します。

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

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 詳細については、次の領域のひとつの隣にある下矢印をクリックします。

- [Discovery Details] : ディスカバリジョブを実行するために使用されたパラメータが表示されます。パラメータには、CDP または LLDP レベル、IP アドレス範囲、およびプロトコルの順序などの属性が含まれます。
- [Credentials] : 使用されたログイン情報の名前が提供されます。
- [History] : 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。

ネットワーク階層の設計

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

ネットワーク階層の概要

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。この階層構造により、デザインの設定や構成を特定の階層要素に簡単に適用できます。たとえば、デザインの設定をエリア全体に適用したり、床のみに適用したりすることができます。

デザインの設定を適用する場所を後で識別できるように、階層要素に名前を付けることができます。

作成できる階層要素には、その階層要素をどの要素に配置できるか、またどの要素をその階層要素に配置できるかを指定するルールがあります。

- [Global] : 他のすべての階層要素がその中に存在するデフォルトの要素。[Global] の直下に配置することが可能な要素は、エリアおよびサイトのみです。
- [Areas] と [Sites] : エリア (Area) とサイト (Site) は、[Global] または他のエリアやサイトに存在します。エリアとサイトには物理アドレスがありません。最大の要素として、地理的地域を識別します。エリアとサイトにより、エリアおよびサイトのグループ化が可能になります。

- [Buildings] : 建物 (Building) は、エリアまたはサイトに存在します。建物を作成する場合、物理アドレスまたは緯度と経度の座標を指定する必要があります。建物にエリアを含めることはできません。ただし、フロアを含めることはできます。
- [Floors] : フロア (Floor) は建物に存在します。壁や窓など、建物のさまざまなコンポーネントを含むマップの有無にかかわらず、建物にフロアを追加できます。フロア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 を含むファイルタイプ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フロアマップに配置して、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。

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。ただし、既存のフロアを別の建物に移動できないことに注意してください。

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。

- 新しいネットワーク階層を作成する。詳細については、「[新しいネットワーク階層の設計 \(47 ページ\)](#)」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、[Cisco DNA Center ユーザガイド](#)の を参照してください。

新しいネットワーク階層の設計

[Design]領域では、ネットワーク全体のデバイスに適用可能な物理トポロジ、ネットワーク設定、デバイスのタイプやプロファイルなど、ネットワークの構造とフレームワークを作成します。既存のインフラストラクチャがない場合は、設計ワークフローを使用します。既存のインフラストラクチャがある場合は、[ディスカバリ機能](#)を使用します。詳細については、「[検出の概要 \(18 ページ\)](#)」を参照してください。

これらのタスクは、[Design] 領域で実行します。

ステップ 1 ネットワーク階層を作成します。

ステップ 2 グローバル ネットワーク設定を定義します。

ステップ 3 ネットワーク プロファイルを定義します。

既存の Cisco ネットワーク階層の使用

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 Cisco DNA 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**：既存のサイト階層を CSV ファイル形式でダウンロードします。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**：マップ情報を 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します。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。

マップアーカイブの基礎をグローバル階層に置くか、次のように単一のサイト、建物、またはフロアの階層に置くかを選択できます。

- [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) Cisco DNA 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、Cisco DNA 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次の影響を与えます。

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 DNA Center ユーザガイド](#)を参照してください。

マップ内で使用するイメージファイルに関するガイドライン

マップイメージファイルを使用するには、次のガイドラインに従ってください。

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

ネットワーク階層のサイトの作成

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

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

世界地図が右側のペインに表示されます。

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

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

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

[Area Name] フィールドには、次の制限があります。

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

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

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

ステップ 5 [Add] をクリックします。

左側ペインの親ノードにサイトが作成されます。

建物の追加

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

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

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

ステップ 3 **[Add Building]** ダイアログボックスで建物の詳細を追加します。

a) **[Building Name]** フィールドに建物の名前を入力します。

[Building Name] フィールドには、次の制限があります。

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

b) **[Parent]** ドロップダウンリストから、親ノードを選択します。**[Global]** がデフォルトの親ノードです。

c) **[Address]** フィールドにアドレスを入力します。

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

ステップ 4 **[Add]** をクリックします。

左側ペインの親サイトに建物が作成され、表示されます。

建物への基本フロアの追加

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。

CAD、非 CAD、または Ekahau ファイルのフロアマップを含むフロアを追加するには、[Cisco DNA Center ユーザガイド](#)を参照してください。:

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

ステップ 2 左側のペインで、建物の横にある省略記号 **...** の上にカーソルを置き、**[Add Floor]** を選択します。

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

[Floor Name] フィールドには、次の制限があります。

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

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

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

ステップ 5 [Add] をクリックします。

ネットワーク階層の管理

Cisco DNA 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 DNA Center ユーザガイド](#)を参照してください。

始める前に

- Cisco DNA 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 Cisco DNA 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 Cisco DNA Center から削除する必要があります。

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

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、次のいずれかのオプションボタンをクリックします。

- [Merge with Existing Sites] : ダウンロードしたサイト情報を既存のサイト情報と結合します。
- [Overwrite Existing Sites] : Cisco DNA 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ダウンロード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、[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。

(注) CSV ファイルがない場合は、[Download 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。

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、それらを Cisco DNA Center にインポートできます。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。

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

[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 次のオプションの少なくとも 1 つを選択します。

- [Map Information] : [On] ボタンをクリックして、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] ボタンをクリックして、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ことを選択した場合は、次のように、選択したマップの情報を含めるか、すべての情報を含めるかを指定する必要があります。

- [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。

ネットワーク階層の検索

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

ステップ 1 階層を検索するには、左側のペインの [Search Hierarchy] 検索フィールドで、検索するサイト、建物、フロア名の名称の一部または正式名称のどちらかを入力します。

階層は、検索フィールドに入力したテキストに基づきフィルタリングされます。

ステップ 2 [Site Name] と [Site Type] のフィルタ基準で階層を検索するには、[Search Hierarchy] 検索フィールドのフィルタアイコンをクリックし、次の手順を実行します。

1. [Site Name] 名前フィールドに、検索するサイトの名前を入力します。
2. 検索結果にすべての建物の住所を含めるには、[Include Address for all Building] チェックボックスをオンにします。
3. [Site Type] 領域で、フィルタ条件に含める [Area]、[Outdoor Area]、[Building]、または [Floor] の横にあるチェックボックスをオンにします。
4. [Search] をクリックします。

フィルタ基準に基づいて、階層がフィルタリングされます。

5. 左側のペインの検索条件を除外するには、それぞれの条件の横にある X マークをクリックします。

サイトの編集

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

ステップ 2 左側のペインで、サイトの横にある省略記号 ... にカーソルを合わせて、[Edit Area] を選択します。

ステップ 3 [Edit Area] ダイアログボックスで、必要な編集を行います。

ステップ 4 [Update] をクリックして変更を保存します。

サイトの削除

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

ステップ 2 左側のペインで、サイトの横にある省略記号 ... にカーソルを合わせて、[Delete Area] を選択します。

ステップ 3 ダイアログボックスで [OK] をクリックして、削除を確定します。

ビルディングの編集

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

ステップ 2 左側のペインで、ビルディングの横にある省略記号 ... にカーソルを合わせて、[Edit Building] を選択します。

ステップ 3 [Edit Building] ダイアログボックスで、必要な編集を行います。

ステップ4 [Update] をクリックして変更を保存します。

ビルディングの削除

ビルディングを削除すると、そのテナントマップもすべて削除されます。削除されたマップ内の AP は、未割り当ての状態に移行します。

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

ステップ2 左側のペインで、ビルディングの横にある省略記号 ... にカーソルを合わせて、[Delete Building] を選択します。

ステップ3 ダイアログボックスで [OK] をクリックして、削除を確定します。

フロアの編集

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

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

ステップ2 左側のペインで、そのフロアの横にある省略記号 ... にカーソルを合わせて、[Edit Floor] を選択します。




ステップ3 [Edit Floor] ポップアップで、必要な変更を行います。

ステップ4 [Update] をクリックして変更を保存します。

2D でのフロアマップのモニタリング

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

- フロアマップウィンドウの右上隅にある [Find] 機能を使用して、AP、センサー、クライアントなど特定のフロア要素を検索します。検索基準に一致する要素は、右側のペインでテーブルとともにフロアマップに表示されます。マウスをテーブルの上に置くと、フロアマップ上の検索要素が接続線で示されます。
- フロアマップウィンドウの右上隅にある ⓘ アイコンをクリックして、次の作業を行います。
 - フロアプランを PDF としてエクスポートします。
 - フロアマップで距離を測定します。
 - スケールを設定してフロア面積を変更します。

- フロアマップウィンドウの右下隅にある  アイコンをクリックして、場所をズームインします。ズームレベルは画像の解像度によって異なります。高解像度画像では、より高いズームレベルを使用できます。各ズームレベルはさまざまなスケールで表示される各種スタイルマップで構成されていて、対応する詳細が表示されます。マップの中にはスケールを小さくしても大きくしても同じ状態のマップもあります。
-  アイコンをクリックすると、広範囲のマップが表示されます。
-  アイコンをクリックすると、マップアイコンの凡例が表示されます。

2D マップでのフロアマップ要素とオーバーレイの構成

2D マップを表示しているときに、マップツールバーの [Add/Edit] をクリックして編集モードに入ります。編集モードでは、次のことができます。

- 次のデバイスを追加、配置、および削除します。
 - アクセスポイント (AP) と計画されたアクセスポイント (PAP)
 - Sensor
- 次のオーバーレイ オブジェクトを追加、編集、および削除します。
 - カバレッジエリア
 - ロケーションリージョン
 - 壁
 - 柵ユニット
 - マーカー
 - \[GPS Markers\]
 - ポイントの位置合わせ

フロアマップでの AP の操作

Cisco DNA Center Cisco DNA Center によって、カバレッジエリアの無線周波数 (RF) 信号の相対強度を表示する全体マップのヒートマップが計算されます。2D ワイヤレスマップの場合、このヒートマップは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値に過ぎません。

フロアマップに AP を配置する際は、次の注意事項を考慮してください。

- 部屋や建物の屋外の近くにデバイスが置かれるように、カバレッジ領域の境界に沿って AP を設置します。このようなカバレッジ領域の中心に設置された AP からは、場合によっては他の全 AP から等距離に見えてしまうデバイスに関して有益なデータが得られません。

AP の追加、配置、編集、および削除

- AP 全体の密度を高め、AP をカバレッジエリアの周辺部に近づけることにより、位置精度を向上させることができます。
- 細長いカバレッジ領域では、直線的に AP を配置しないようにします。各 AP でデバイスロケーションのスナップショットが他と異なるように、それらを交互にずらします。
- 設計では高帯域幅アプリケーションにも十分に対応できる AP 密度が提供されますが、位置に関しては、単一デバイスの各 AP ビューが似ているという弱点があります。そのことが位置の判別を困難にしています。AP をカバレッジ領域の周辺に移動して、それらを交互にずらします。それぞれにおいてデバイスの見え方が明確に異なる可能性が高くなり、結果としてより位置精度が高まります。
- フロアマップでのヒートマップの表示を最適化するには、AP の高さを約 10 フィート (3 m) 以下に設定します。

AP の追加、配置、編集、および削除

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

始める前に

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

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

ステップ 2 左側のペインで、サイトをクリックしてからビル名をクリックし、最後に関心のあるフロアをクリックします。

ステップ 3 マップツールバーで **[AP]** トグルボタンが有効になっていることを確認します。

ステップ 4 マップツールバーから、**[Add/Edit]** をクリックします。

ステップ 5 マップから、AP を追加、編集、配置、再配置、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	<ol style="list-style-type: none"> 1. マップの左側のペインで、[Add APs] をクリックします。 2. [Add APs] スライドインペインでは、次のいずれかの操作を実行できます。 <ul style="list-style-type: none"> • 単一の AP を追加するには：追加する AP の横にある [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。 <p>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。</p> 3. [Save] をクリックします。
AP の配置	<ol style="list-style-type: none"> 1. マップの左ペインの [Unpositioned] カテゴリから、AP をクリックします。 2. AP を配置するフロアマップ上の場所をクリックします。 3. [Save] をクリックします。
AP の位置変更	<ol style="list-style-type: none"> 1. マップで、AP をクリックして選択します。 2. AP を新しい位置にドラッグアンドドロップします。 3. [Save] をクリックします。
AP の編集	<ol style="list-style-type: none"> 1. マップで、AP をクリックします。 2. [Edit AP] スライドインペインから、必要に応じて AP 設定を構成します。 3. [Save] をクリックします。

アクション	手順
<p>複数の AP の編集</p> <p>(注) 複数の AP を編集する場合、属性値は、値が同じであれば表示されます。そうでない場合は空白です。アンテナの値は、選択した AP のモデル番号と無線（無線の数と動作帯域）が同じである場合にのみ編集できます。計画された AP のモデル番号は変更できますが、追加された AP は変更できません。</p>	<ol style="list-style-type: none"> 1. 次のいずれかの方法を使用して、AP を選択します。 <ul style="list-style-type: none"> • 最初のデバイスをクリックし、Shift キーを押しながら残りのデバイスをクリックします。 • マップ ナビゲーション ツールバーで、[Select by rectangle] をクリックします。次に、マップの領域をクリックし、強調表示された長方形をドラッグして、連続した領域内の AP を選択します。長方形内で強調表示されているすべての AP が選択されています。 2. [Edit AP] スライドインペインから、必要に応じて AP 設定を構成します。 3. [Apply] をクリックします。 4. [Save] をクリックします。
<p>AP の削除</p>	<ol style="list-style-type: none"> 1. AP または計画された AP をクリックします。 2. マップの左側のペインで、[Remove APs] をクリックします。 3. [Save] をクリックします。

AP のクイック ビュー

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

- [Info] をクリックすると、次の AP の詳細が表示されます。
 - [Associated] : AP が関連付けられているかどうかを示します。
 - [Name] : AP 名。
 - [MAC Address] : AP の MAC アドレス。
 - [Model] : AP モデル番号。
 - [Admin/Mode] : AP モードの管理ステータス。
 - [Type] : 無線タイプ。
 - [OP/Admin] : 動作ステータスおよび AP モード。
 - [Channel] : AP のチャンネル番号。
 - [Antenna] : アンテナ名。

- [Azimuth] : アンテナの方向。
- [Rx Neighbors] ラジオ ボタンをオンにすると、マップ上に選択した AP に隣接する Rx ネットワークが接続回線とともに表示されます。また、フロアマップには AP が関連付けられているかどうか AP 名とともに表示されます。
- [Device 360] をクリックすると、特定のネットワーク要素（ルータ、スイッチ、AP、またはシスコ ワイヤレス コントローラ）の 360 度ビューが表示されます。



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

マップへのセンサーの追加



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

センサーデバイスは AP 1800s センサー専用です。Cisco Aironet 1800s アクティブセンサーは、PnP を使用してブートストラップされます。アシュアランスサーバーに到達可能かどうかの詳細情報を取得してからアシュアランスサーバーと直接通信します。センサーテストに関する情報を含む詳細については、『[Cisco DNA アシュアランス User Guide](#)』を参照してください。

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

ステップ 2 フロアを左側の階層ツリーで、次を選択します。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 [Add Sensors] スライドインペインから、追加するセンサーのチェックボックスをオンにします。またはセンサー行の横にある [Add] をクリックします。

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

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

ステップ 5 完了したら、[Save] をクリックします。

カバレッジエリアの追加、編集、および削除

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

長方形以外の建物がある場合、またはフロア内で長方形以外の領域をマークする場合には、マップ描画ツールを使用してカバレッジエリアまたは多角形の領域を作成できます。

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

ステップ 2 フロアを左側の階層ツリーで、次を選択します。します。

ステップ 3 マップツールバーから、**[2D] > [Add/Edit] > [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。

- [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。
- [Add Coverage]** をクリックします。
- 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。
- 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。

- 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。
- マップツールバーの **[Save]** をクリックします。

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。

- マップツールバーから、**[Add/Edit] > [Coverage Areas]** をクリックします。
- 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。
- 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。
- 完了したら、マップツールバーの **[Save]** をクリックします。

ステップ 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。

- マップツールバーから、**[Add/Edit] > [Coverage Areas]** をクリックします。
- カバレッジエリアを右クリックし、**[Delete]** を選択します。
- カバレッジエリアが削除されたら、マップツールバーから **[Save]** をクリックします。

障害物の作成

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

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

ステップ 2 左ペインで、フロアを選択します。

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

- ステップ 4** [Obstacles] の横にある [Overlays] パネルで、[Add] をクリックします。
- ステップ 5** [Obstacle Creation] ダイアログ ボックスで、[Obstacle Type] ドロップダウン リストから障害のタイプを選択します。作成可能な障害のタイプは、[Thick Wall]、[Light Wall]、[Heavy Door]、[Light Door]、[Cubicle]、および [Glass] です。
選択した障害のタイプの予測信号損失が自動的に取り込まれます。信号損失は、これらのオブジェクトの周辺の RF 信号強度を計算するために使用されます。
- ステップ 6** [Add Obstacle] をクリックします。
- ステップ 7** 障害物を作成する領域に描画ツールを移動します。
- ステップ 8** 描画ツールをクリックして、描線を開始および停止します。
- ステップ 9** エリアの輪郭を描画したら、そのエリアをダブルクリックして強調表示します。
- ステップ 10** [Obstacle Creation] ウィンドウで [Done] をクリックします。
- ステップ 11** [Save] をクリックして、障害をフロア マップに保存します。
- ステップ 12** 障害を編集するには、[Obstacles] の隣にある [Overlays] パネルで、[Edit] をクリックします。
すべての使用可能な障害物がマップ上で強調表示されます。
- ステップ 13** 変更が完了したら、[Save] をクリックします。
- ステップ 14** 障害を削除するには、[Obstacles] の隣にある [Overlays] パネルで、[Delete] をクリックします。
すべての使用可能な障害物がマップ上で強調表示されます。
- ステップ 15** 障害にマウス カーソルを合わせ、クリックして削除します。
- ステップ 16** [Save] をクリックします。

ロケーションリージョンの追加、編集、および削除

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

マップ上での包含および除外領域を定義するには、次のガイドラインを使用します。

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。
- フロア上の包含リージョンを 1 つだけ定義できます。デフォルトでは、各フロア領域が作成されるたびに、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。
- 1 つのフロア領域に複数の除外領域を定義することができます。

マップ上での包含および除外領域の定義

マップ上での包含および除外領域を定義するには、次のガイドラインを使用します。

- 包含領域と除外領域は多角形領域で表され、最低 3 点で構成される必要があります。

包含リージョンの追加、編集、および削除

- 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たびに、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。
- 1つのフロア領域に複数の除外領域を定義することができます。

包含リージョンの追加、編集、および削除

-
- ステップ1** メニューアイコン (☰) をクリックして、**[Design] > [Network Hierarchy]**。
- ステップ2** フロアを左側の階層ツリーで、次を選択します。します。
- ステップ3** マップツールバーから、**[2D] > [Add/Edit] > [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、**[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 **[Delete]** を選択します。
- ステップ8** マップツールバーの **[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

フロアの計算の精度を高めるため、計算から除外するリージョン（除外リージョン）を定義できます。たとえば、建物内のアトリウムや階段の吹き抜けなどのリージョンを除外できます。原則として、除外リージョンは包含リージョンの境界内に定義されます。

-
- ステップ1** メニューアイコン (☰) をクリックして、**[Design] > [Network Hierarchy]**。
- ステップ2** フロアを左側の階層ツリーで、次を選択します。します。
- ステップ3** マップツールバーから、**[2D] > [Add/Edit] > [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 [Delete] を選択します。

ステップ 8 マップツールバーの [Save] をクリックします。

ロケーションリージョンの編集

ステップ 1 [Overlays] パネルで、[Location Regions] の横にある [Edit] をクリックします。

使用可能なロケーションリージョンがマップ上で強調表示されます。

ステップ 2 必要な変更を行って、[Save] をクリックします。

ロケーションリージョンの削除

ステップ 1 [Overlays] パネルで、[Location Regions] の横にある [Delete] をクリックします。

使用可能なロケーションリージョンがマップ上で強調表示されます。

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

ステップ 3 [Save] をクリックします。

レールの作成

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

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

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

ステップ 2 左ペインで、フロアを選択します。

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

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

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

描画アイコンが表示されます。

■ マーカーの追加、編集、および削除

- ステップ 6** レールラインの開始ポイントで描画アイコンをクリックします。ラインの描画を停止するときやラインの方向を変える際は、再びクリックします。
- ステップ 7** フロアマップ上にレールラインを描画したら、描画アイコンを2回クリックします。レールラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。
- ステップ 8** [Save] をクリックします。
- ステップ 9** [Overlays] パネルで、[Rails] の横にある [Edit] をクリックします。
使用可能なレールがマップ上で強調表示されます。
- ステップ 10** 変更を加えて、[Save] をクリックします。
- ステップ 11** [Overlays] パネルで、[Rails] の横にある [Delete] をクリックします。
使用可能なすべてのレールラインがマップ上で強調表示されます。
- ステップ 12** 削除するレールラインの上にマウスのカーソルを合わせ、[Delete] をクリックします。
- ステップ 13** [Save] をクリックします。

■ マーカーの追加、編集、および削除

- ステップ 1** メニューアイコン (☰) をクリックして、[Design] > [Network Hierarchy]。
- ステップ 2** フロアを左側の階層ツリーで、次を選択します。します。
- ステップ 3** マップツールバーから、[2D] > [Add/Edit] > [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から、[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 Marker] 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 [Delete] を選択します。
- ステップ 10** マップツールバーの [Save] をクリックします。

■ フロアビューオプション

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

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

アクセス ポイントの表示オプション

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

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

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

- [Dual-Band Radios] : Cisco Aironet 2800 および 3800 シリーズ アクセスポイント上の XOR デュアルバンド無線を識別してマークします。
- [Health Score] : AP の正常性スコア。
- **Issue Count**
- [Coverage Issues]
- [AP Down Issues]

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

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

センサーオプションの表示

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

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

オーバーレイ オブジェクトの表示オプション

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

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

マップ プロパティの設定

[Map Properties] パネルを展開して、以下を構成します。

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

グローバルマッププロパティの設定

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

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

ネットワーク階層マップでのデバイスデータのフィルタ処理

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

インベントリの管理

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

インベントリについて

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

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

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery（このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF） デバイスのリストについては、[ディスカバリの前提条件（19 ページ）](#) を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 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（68 ページ）](#) を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

デバイスポーリング間隔の更新

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

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

始める前に

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

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

ステップ 2 更新するデバイスを選択します。

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

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


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

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

ステップ 6 [更新 (Update)] をクリックします。

インベントリに関する情報の表示

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

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

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


[Focus] ドロップダウンリストから [Default] ビューを選択した場合、[Inventory] テーブルには、リストされたデバイスの [Device Name]、[IP Address]、[Device Family]、および [MAC Address] のみが表示されます。

デフォルトでは、[Inventory] テーブルに 25 のエントリが表示されます。追加のエントリを表示するには、[Show More] をクリックします。[Inventory] テーブルには最大 500 のエントリを表示できます。

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

始める前に

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

メニューアイコン () をクリックして、[Provision] > [Network Devices] > [Inventory] の順に選択します。[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。次の表に、使用できる情報を記載します。

■ インベントリに関する情報の表示

表 18: インベントリ

カラム	説明
Device Name	

カラム	説明
	<p>デバイスの名前。</p> <p>デバイス名をクリックすると、デバイスの次の詳細が表示されます。</p> <p>[Details] : デバイス名、到達可能性ステータス、管理性ステータス、IP アドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。</p> <ul style="list-style-type: none"> • [View Assurance 360] : [Assurance 360] ウィンドウが表示されます。ウィンドウを開くには、アシュアランス アプリケーションをインストールしておく必要があります。 • インターフェイス <ul style="list-style-type: none"> • [Ethernet Ports] (すべてのデバイスが対象) : イーサネットポートの動作ステータスと管理ステータスが表示されます。 <p>トグルボタン () を使用して、[Ports] ビューと [Ports] テーブルを切り替えます。[Ports] ビューでポートをクリックするか、[Ports] テーブルでポート名をクリックして、ポートの詳細を表示します。</p> <p>Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチと Cisco ASR 1000 シリーズ アグリゲーション サービス ルータの場合、[Ports] ビューにはラインカードとスーパーバイザカードの詳細が表示されます (使用可能な場合)。</p> <p>ラインカードの詳細には、プラットフォーム、アドレス、シリアル番号、ロール、およびスタックメンバー番号に関する情報が含まれます。スーパーバイザカードの詳細には、部品番号、シリアル番号、スイッチ番号、およびスロット番号に関する情報が含まれます。</p> <p>[Ports] テーブルには、動作ステータス、管理ステータス、タイプ、ネイティブ VLAN、音声 VLAN、MAC アドレス、PoE ステータス、速度、MTU およびポートの説明が表示されます。</p> <p>Cisco Catalyst 2000、3000、および 9000 シリーズ スイッチの場合、[Ports] ビューでポートをクリックするか、[Ports] テーブルのポート名をクリックして、ポートの最大割り当て電力、および消費電力の詳細を表示します。</p> <ul style="list-style-type: none"> • [Neighbor Details] : <ul style="list-style-type: none"> [Ports] ビューでポートをクリックするか、[Ports] テーブルでポート名をクリックして、ポートの詳細を表示します。[Port Details] ウィンドウには、ポートに接続されているデバイスの詳細が表示されます。[Neighbor Details] エリアには、デバイス名、デバイスが接続されているポートの名前、およびデバイスの機能が表示されます。 ポートには、CDP ネイバーの詳細が表示されます。CDP が存在しない場合、LLDP ネイバーの詳細が表示されます。CDP と LLDP ネイバーの両方が存在しない場合、[Port Details] ウィンドウに [Neighbor Details] が表示されません。 • [ColorCode] : このドロップダウンリストには、次のビューが用意されています。

カラム	説明
	<ul style="list-style-type: none"> • [Status] : イーサネットポートのデフォルトビューを表示します。 • [VLANs] : 特定のポートに割り当てられている VLAN を表示します。 [VLANs] ビューでは、最大 5 つの VLAN を選択し、ポートに関連付けられている VLAN のみを一覧表示できます。 [VLANs] ビューには、VLAN ポートマッピングの [Selected]、[Not Configured]、[Default]、および [VLAN] カラーコードが表示されます。 • [Port Channels] : デバイスで設定されている上位 5 つのポートチャンネルを表示します。 [Port Channels] ビューには、デバイスで設定されているポートチャンネルの [Selected] および [Port-channel] カラーコードが表示されます。 • [Port Actions] : <ul style="list-style-type: none"> • [Clear Mac Address] : ポートの MAC アドレスをクリアできます。 [Ports] ビューでポートをクリックし、 [Port Actions] ドロップダウンリストから [Clear Mac Address] を選択します。 • [Port Shut] : ポートをシャットダウンできます。 [Ports] ビューでポートをクリックし、 [Port Actions] ドロップダウンリストから [Port Shut] を選択します。 [Okay] をクリックして確定します。 ポートの管理ステータスが [Down] に変わります。 ポートの管理ステータスを [Up] に変更するには、 [Port Actions] ドロップダウンリストから [Port No Shut] を選択し、 [Okay] をクリックします。 <p>error-disabled ポートは黄色で表示されます。 [Ports] ビューで error-disabled ポートをクリックして、エラーの理由を表示します。 error-disabled ポートをアクティブにするには、MAC アドレスをクリアして、ポートをシャットダウンします。</p> • [Port Description] : [PORT DESCRIPTION] の横にある [Edit] アイコンをクリックし、説明を入力して [Save] をクリックし、 [Okay] をクリックしてポートに説明を追加します。説明を削除するには、 [Delete] アイコンをクリックします。

カラム	説明
	<ul style="list-style-type: none"> • [Update Native VLAN] : [Native VLAN] の横にある [Edit] アイコンをクリックし、[Edit Native VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。2つの VLAN が事前設定されているポートの VLAN を更新することはできません。 <ul style="list-style-type: none"> • VLAN の更新、ポートの説明の追加、MAC アドレスのクリア、およびポートのシャットダウンを行うには、デバイスソフトウェアタイプが Cisco IOS または Cisco IOS-XE である必要があります。 • ワイヤレスコントローラでは、VLAN の更新、MAC アドレスのクリア、およびポートのシャットダウンはサポートされていません。 • VLAN の更新、MAC アドレスのクリア、およびポートのシャットダウンは、アクセスポートでのみサポートされます。 • ポートをシャットダウンすると、ポートのトラフィックが中断されます。 • [Update Voice VLAN] : [Voice VLAN] の横にある [Edit] アイコンをクリックし、[Edit Voice VLAN] ドロップダウンリストから VLAN を選択し、[Save] をクリックして VLAN を更新します。 • [Native VLAN] (スイッチとハブのみが対象) : 動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。 <ul style="list-style-type: none"> • 製造時提供のデフォルト VLAN の VLAN ID • 設定されたデフォルト VLAN の VLAN ID • 設定された VLAN の VLAN ID <p>[Search] または [Filter] をクリックして、VLAN の詳細を表示できます。</p> • [Virtual Ports] (ワイヤレスデバイス、コントローラ、ルータのみが対象) : 動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] または [Filter] をクリックして、ポートの詳細を表示できます。 • [Hardware and Software] : デバイスのハードウェアとソフトウェアの詳細が表示されます。 • [Configuration] : show running-config コマンドの出力で表示される内容に似た詳細な構成情報が表示されます。 <p>この機能は、AP とワイヤレスコントローラにはサポートされていません。したがって、これらのデバイスタイプの場合は設定データは返されません。</p>


カラム	説明
	<ul style="list-style-type: none"> • [Power] : デバイスに割り当てられている電力、消費電力、および残りの電力に関する詳細が表示されます。 [Power Supplies] テーブルに、動作ステータス、シリアル番号、およびベンダー機器タイプの詳細が表示されます。 • [Fans] : ファンの動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。 • [SFP Modules] : プラットフォーム、シリアル番号、製造元、および Small Form-Factor Pluggable (SFP) モジュールの接続先ポートの詳細を表示します。 [Search] または [Filter] をクリックして、ポートの詳細を表示できます。 • [User Defined Fields] : デバイスに関連付けられているユーザー定義フィールドが表示されます。 • [Config Drift] : 構成の変更を表示し、同じデバイスの任意の 2 つのバージョンを選択して、各バージョンの実行中の構成データを比較できます。 (注) 実行中の構成データは、ワイヤレスコントローラやレガシーコントローラなどのデバイスではサポートされません。 • [Wireless Info] : プライマリとセカンダリの管理対象ロケーションが表示されます。 • [Mobility] : モビリティグループ名、RF グループ名、仮想 IP、およびモビリティ MAC アドレスが表示されます。 (注) 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30分を超える期間にわたってその情報を更新していないことを意味しています。
IP Address	デバイスの IP アドレス。

カラム	説明
<p>Support Type</p>	<p>デバイスのサポートレベルが表示されます。</p> <ul style="list-style-type: none"> • [Supported] : Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。 • [Limited] : レガシーデバイス用のデバイスパックは、Cisco DNA Center の次の機能についてのみテストされています。 <ul style="list-style-type: none"> • 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 : デバイス名、IPアドレス、サポートタイプ、デバイスファミリ、サイト、到達可能性、MACアドレス、デバイスロール、イメージバージョン、稼働時間、最終同期ステータス、最終更新日、シリアル番号、デバイスシリーズ、プラットフォームなどのデバイス詳細について、サポートが提供されます。 • 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。 <p>詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。</p> <ul style="list-style-type: none"> • [Unsupported] : Cisco DNA Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合、サービスリクエストまたはバグを発生させることは求められていません。 • [Third Party] : デバイスパックは、お客様またはビジネスパートナーによって構築され、認定プロセスを経ています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡する必要があります。

カラム	説明
Reachability	<p>以下は、さまざまなステータスのリストです。</p> <ul style="list-style-type: none"> • [Reachable] : Cisco DNA Center から SNMP、HTTP (S)、および NETCONF ポーリングを使用してデバイスに到達できます。 • [Ping Reachable] : Cisco DNA Center から ICMP ポーリングを使用してデバイスに到達できます。SNMP、HTTP (S)、および NETCONF ポーリングでは到達できません。 • [Unreachable] : SNMP、HTTP (S)、NETCONF、ICMP のいずれのポーリングでもデバイスに到達できません。
[EoX Status]	<p>EoX スキャンのステータスが表示されます。</p> <ul style="list-style-type: none"> • [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] : Cisco DNA 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] : Cisco DNA 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。 <p>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ず (ある場合)。</p> <p>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。</p> <p>slide-in pane 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。</p>
Manageability	<p>デバイスのステータスが示されます。</p> <ul style="list-style-type: none"> • [Managed] と緑色のチェックアイコン : デバイスに到達可能で、完全に管理されています。 • [Managed] とオレンジ色のエラーアイコン : デバイスは管理されていますが、到達不能、認証失敗、NETCONF ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。 • [Unmanaged] : デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。
MAC Address	デバイスの MAC アドレス。
Image Version	デバイスで現在実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。

カラム	説明
Serial Number	シスコ デバイスのシリアル番号。
Uptime	デバイスが起動してから、稼働している時間。
Device Role	<p>スキャンプロセス中に、検出された各デバイスに割り当てられているロール。デバイスロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。</p> <p>(注) デバイス ロールを手動で変更すると、割り当ては静的のままになります。Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。</p> <p>必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。</p> <ul style="list-style-type: none"> • Unknown • Access • Core • Distribution • Border Router
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、 ネットワーク階層の概要 (46 ページ) を参照してください。
Last Updated	Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。
Device Family	ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。
Device Series	デバイスのシリーズ番号 (Cisco Catalyst 4500 シリーズ スイッチなど)。
Resync Interval	デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、 Cisco DNA Center 管理者ガイド を参照してください。

カラム	説明
Last Sync Status	<p>デバイス最終検出のスキャン状態。</p> <ul style="list-style-type: none"> • [Managed] : デバイスは完全に管理された状態です。 • [Partial Collection Failure] : デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information] (i) アイコンにマウスを合わせます。 • [Unreachable] : デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。 • [Wrong Credentials] : デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。 • [In Progress] : インベントリ収集が実行されています。
プロビジョニングステータス	<p>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。</p> <ul style="list-style-type: none"> • [Success] : デバイスでの最近の操作が成功しました。 • [Success with a warning icon] : デバイスでの最近の操作が成功しました。ただし、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。

カラム	説明
Credential Status	<p>デバイスのクレデンシャルステータスが示されます。</p> <ul style="list-style-type: none"> • [Not Applied] : デバイスのクレデンシャル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。 <p>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。</p> <p>[Credential Status] slide-in pane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。</p> <p>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。</p> <ul style="list-style-type: none"> • [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 Ethernet Mac Address	AP イーサネット MAC アドレスに関する詳細を表示します。
AP CDP Neighbors	インベントリリストページの AP に接続されているスイッチとポートに関する詳細を表示します。インベントリリストページには、接続されたアクセススイッチが Cisco DNA 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せん。


ネットワーク デバイスの削除

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

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

始める前に

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

- ステップ 1** メニューアイコン () をクリックして、[Provision]>[Network Devices]>[Inventory] の順に選択します。[Inventory] ウィンドウには、ディスクバリプロセス中に収集されたデバイス情報が表示されます。
- ステップ 2** 削除するデバイスの横にあるチェックボックスをオンにします。

■ デバイスをサイトに追加する

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


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

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

ステップ 5 [OK] をクリックして、アクションを確認します。

デバイスをサイトに追加する

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

- ステップ 1 メニューアイコン (☰) をクリックして、[Provision] > [Network Devices] > [Inventory] の順に選択します。
[Inventory] ウィンドウには、ディスクバリプロセス中に収集されたデバイス情報が表示されます。
- ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。
- ステップ 3 [Actions] メニューから、[Provision] > [Assign Device to Site] を選択します。
- ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの  アイコンの横にあるリンクをクリックします。
- ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。
- ステップ 6 [Save] をクリックします。
- ステップ 7 (任意) 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。
- ステップ 8 [Next] をクリックします。
- ステップ 9 [Task Name] フィールドに、任意のタスク名を入力します。
- ステップ 10 即座にデバイスをサイトに割り当てるには、[Now] オプションボタンをクリックし、[Assign] をクリックします。
- ステップ 11 将来の日付と時刻でデバイスのサイトへの割り当てをスケジュールするには、[Later] オプションボタンをクリックして展開する日時を定義し、[Assign] をクリックします。
- ステップ 12 CLI 構成をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックして、次の手順を実行します。
- [Task Name] フィールドに任意のタスク名を入力し、[Preview] をクリックします。
後で、作成した構成のプレビューを使用して、選択したデバイスに展開できます。
 - [Task Submitted] メッセージで、[Work Items] リンクをクリックします。

(注) [Task Submitted] メッセージが表示されなかった場合は、メニューアイコンをクリックし、**[Activities] > [Work Items]**の順に選択します。

- **[Work Items]** ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。
- CLI 設定の詳細を表示し、**[Deploy]** をクリックします。
- 即座にデバイスを展開するには、**[Now]** オプションボタンをクリックし、**[Apply]** をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、**[Later]** オプションボタンをクリックし、展開する日時を定義します。
- 確認ウィンドウで **[Yes]** をクリックします。

(注) CLI タスクは、**[Work Items]** ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 13 サイトにデバイスを割り当てるときにデバイスの可制御性が有効になっていると、ワークフローが自動的にトリガーされ、サイトからデバイスにデバイス設定がプッシュされます。**[Focus]** ドロップダウンリストから **[Provision]** を選択し、**[Provision Status]** 列の **[See Details]** をクリックします。デバイスの可制御性を有効にしている場合、デバイスにプッシュされる設定が別のウィンドウに表示されます。

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

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

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

1. メニューアイコン (☰) をクリックして、**[System] > [Settings] > [External Services] > [Authentication and Policy Servers]** の順に選択して、Cisco ISE サーバーの詳細を入力します。
2. Cisco ISE サーバーが正常に追加されると、NCP は NDP (ネットワーク データ プラットフォーム) との接続を確立し、pxGrid ノード、キーストア、およびトラストストアファイルの詳細を送信します。
3. NDP は、NCP から受信した設定に基づき、pxGrid セッションを確立します。
4. NCP が pxGrid ノードのフェールオーバーを自動的に検出すると、ペルソナが稼働し、NDP に通信します。

5. ISE 環境に変化があると、NDP は新しい pxGrid アクティブノードと新しい pxGrid セッションを開始します。

認証サーバとポリシーサーバの設定

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

始める前に

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



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

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



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

- 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、[Work Centers] > [Trustsec] > [Trustsec Servers] > [Trustsec AAA Servers] でも定義する必要があります。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。
- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名 (SAN) のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の SAN フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。



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

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

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

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

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

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

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

- [Server IP Address] : ISE サーバーの IP アドレス。
- [Shared Secret] : デバイス認証のキー。
- [Username] : Cisco ISE CLI にログインするために使用するユーザー名。
(注) このユーザーにはスーパーユーザーの管理権限が必要です。
- [Password] : Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN] : Cisco ISE サーバーの完全修飾ドメイン名 (FQDN) 。
(注)
 - Cisco ISE ([Administration] > [Deployment] > [Deployment Nodes] > [List]) で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
 - 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名 (CN) または Subject Alternative Name (SAN) と一致する必要があります。

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

hostname.domainname.com

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

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

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

- [Connect to pxGrid] : pxGrid 接続を有効にするには、このチェックボックスをオンにします。
Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Cisco DNA Center システムを認証するために Cisco ISE に送信) 、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。
このオプションを有効にする場合は、次のことを確認してください。
 - Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局 (CA) によって生成されていること (そうでない場合、pxGrid 認証は失敗します) 。
 - [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。
- [Protocol] : [TACACS] と [RADIUS] (デフォルト) 。両方のプロトコルを選択できます。

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

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

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

Cisco ISE サーバー登録フェーズ :

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

pxGrid サブスクリプション登録フェーズ :

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

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

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

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

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

始める前に

サイトを作成し、サイトにデバイスを割り当てます。『[ネットワーク階層のサイトの作成 \(49 ページ\)](#)』を参照してください。

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

ステップ 2 [SNMP Traps] エリアで、次のいずれかを実行します。

- [Use Cisco DNA 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] エリアで、次のいずれかを実行します。

- [Use Cisco DNA 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 [NetFlow] エリアで、次のいずれかを実行します。

- [Use Cisco DNA Center as NetFlow collector server] 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 Cisco DNA Center が宛先として設定されている必要があります。Cisco DNA 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 Client Data Collection] エリアで、[Enable Cisco DNA Center IPDT on all devices] 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] オプションボタン (デフォルト) をクリックします。

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

ステップ 6 [Wireless Controller, Access Point and Wireless Clients Health] 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。

ステップ 7 [Save] をクリックします。

Cisco AI Network Analytics データ収集の設定

Cisco AI Network Analytics が、ネットワークデバイスおよびサイト階層から Cisco DNA Center にネットワークイベントデータをエクスポートできるようにするには、次の手順を実行します。

始める前に

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

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

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

AI Network Analytics

Using AI and Machine Learning, AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Configure

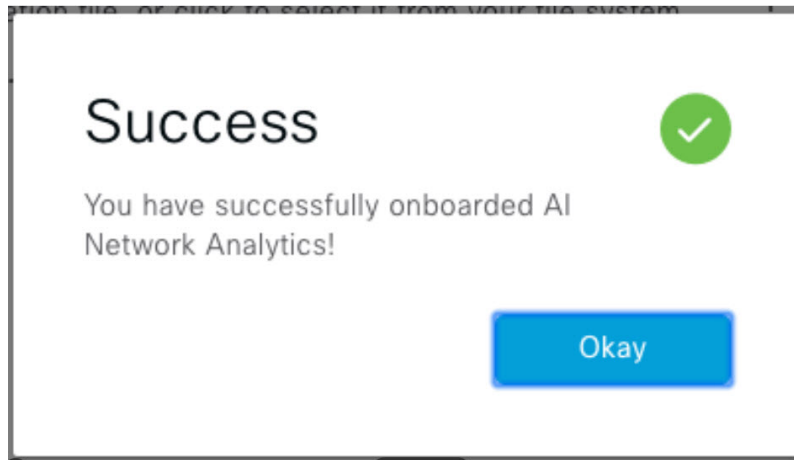
Recover from a config file ⓘ

ステップ 3 次のいずれかを実行します。

- アプライアンスに以前のバージョンの Cisco AI Network Analytics がインストールされている場合は、次の手順を実行します。
 1. [Recover from a config file] をクリックします。
[Restore AI ネットワーク分析] ウィンドウが表示されます。

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

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



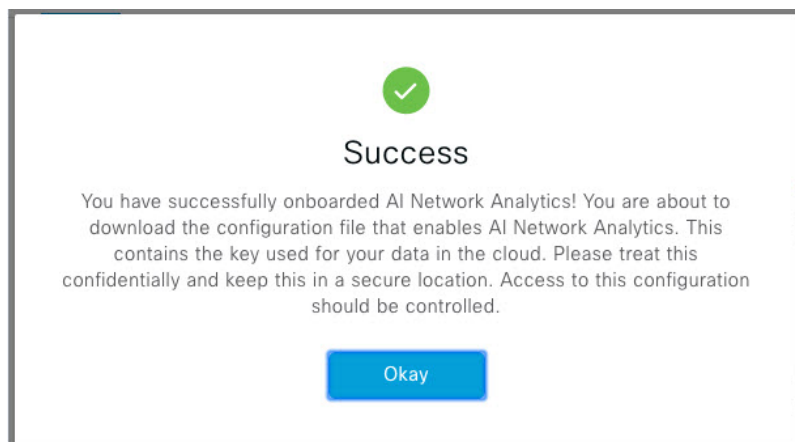
- Cisco AI Network Analytics を初めて設定する場合は、次の手順を実行します。

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

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

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

Cisco AI Network Analytics が有効になるまでに数分かかる場合があります、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 データ収集の無効化

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

ステップ 1 メニューアイコン (☰) をクリックして、[System] > [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 (オプション) 以前の設定が間違っていて配置されている場合は、[Download configuration file] をクリックします。

機械推論ナレッジベースの更新

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

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

ステップ 2 **[External Services]** まで下にスクロールし、**[Machine Reasoning Knowledge Base]**を選択します。

[Machine Reasoning Knowledge Base] ウィンドウには、次の情報が表示されます。

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

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

- **[AUTO UPDATE]** : 機械推論ナレッジベースが Cisco DNA Center で自動的に毎日更新されます。
- **[CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY]** : 自動構成を実行できる CX Cloud と Cisco DNA Center を統合します。この統合により、Cisco DNA Center のセキュリティアドバイザリ ツールからデバイスの強化された脆弱性検出が直接提供されます。

ステップ 3 （推奨） **[AUTO UPDATE]** チェックボックスをオンにして、機械推論ナレッジベースを自動的に更新します。

[Next Attempt] 領域に、次の更新の日付と時刻が表示されます。

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

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

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

1. **[Download]** をクリックします。

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

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

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

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


デフォルトの言語を変更するには、次のタスクを実行します。

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

• Google Chrome から、次の手順を実行します。

1. 右上隅にある  アイコンをクリックし、[Settings] を選択します。
2. 下にスクロールして [Advanced] をクリックします。
3. [Languages] > [Language] ドロップダウンリストから、[Add languages] を選択します。
[Add languages] ポップアップウィンドウが表示されます。
4. [Chinese]、[Japanese]、または [Korean] を選択して、[Add] をクリックします。

• Mozilla Firefox から、次の手順を実行します。

1. 右上隅にある  アイコンをクリックし、[Options] を選択します。
2. [Language and Appearance] > [Language] エリアから、[Search for more languages] を選択します。
[Firefox Language Settings] ポップアップウィンドウが表示されます。
3. [Select a language to add] ドロップダウンリストから、[Chinese]、[Japanese]、または [Korean] を選択します。
4. [OK] をクリックします。

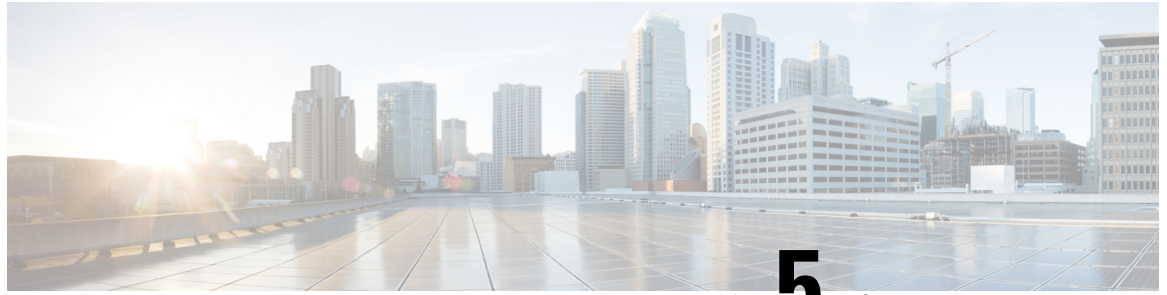
ステップ 2 Cisco DNA Center にログインします。

GUI 画面は、選択した言語で表示されます。

図 5: ローカライズされたログイン画面の例



The image shows a localized login page for Cisco DNA Center. At the top center is the Cisco logo, consisting of a stylized signal icon above the word "CISCO". Below the logo, the text "Cisco DNA Center" is displayed in a large blue font. Underneath that, the tagline "ネットワークの設計、自動化、保証" (Network design, automation, assurance) is written in a smaller black font. The login form includes two input fields: "ユーザ名*" (Username*) and "パスワード*" (Password*), each with a horizontal line below it. A blue button with the text "ログイン" (Login) is positioned below the password field. A thick horizontal line is located at the bottom of the page content area.



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

- [企業について](#) (93 ページ)
- [企業の全体的な健全性のモニターとトラブルシューティング](#) (93 ページ)

企業について

企業全体の健全性のモニターとトラブルシューティングに、アシュアランスを使用できます。企業はネットワークデバイスとクライアントで構成されています。

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

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

企業の全体的な健全性のモニターとトラブルシューティング

この手順を使用して、ネットワークデバイスやクライアントを含む企業の健全性の概要を把握し、対処する必要がある潜在的な問題があるかどうかを判断します。

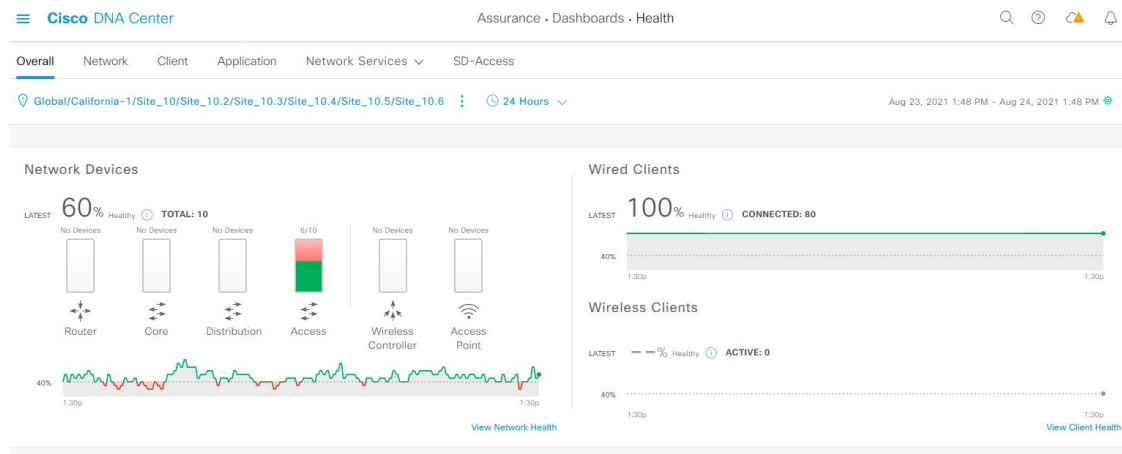
始める前に

アシュアランスを設定します。「[基本的な設定のワークフロー](#) (15 ページ)」を参照してください。


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

[Overall health] ダッシュボードが表示されます。

図 6: [Overall Health] ダッシュボード



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

[Overall] 正常性ダッシュボードの上部のメニューバー	
アイテム	説明
 Global [Location] ペイン	<ul style="list-style-type: none">  をクリックして、サイト階層からサイト、建物、またはフロアを選択します。  ロケーションアイコンの横にある  をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。  Hide Sites をクリックして [Sites] テーブルを非表示にします。   : このトグルボタンをクリックして、ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。テーブルには、特定のロケーションの正常なクライアントとネットワークデバイスの割合が選択に基づいて表示されます。   : このトグルボタンをクリックすると、企業のすべてのサイトの正常性が、地理的ロケーションに基づいた正常性マップで表示されます。デフォルトでは、提示されるサイトは問題の重大度に従って色分けされています。 ヘルス スコアの色は、その重大度を示します。正常性は 1 ~ 10 のスケールで測定され、10 が最高スコアになります。スコア 0 は、データを取得できなかったことを示します。  [Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Overall] ダッシュボードに表示されます。
時間範囲	過去 3 時間、24 時間、または 7 日間のデータを表示できます。
[Actions] ドロップダウン リスト	<p>[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。</p> <p>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 (340 ページ) および カスタムダッシュボードの作成 (335 ページ) を参照してください。</p>

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

[Overall Health Summary] ダッシュレット	
アイテム	説明
[Network Devices]	<p>Network Score : 企業全体での正常 (良好) なデバイス (ルータ、スイッチ、ワイヤレスコントローラ、アクセスポイント) の割合。 ネットワークヘルススコア (130ページ) を参照してください。</p> <p>Device Category Health Score : デバイスカテゴリ ([Router]、[Core]、[Distribution]、[Access]、[Controller]、[Access Point]) で正常 (良好) なネットワークデバイスの割合。</p> <p>(注) SD-Access ファブリックを選択すると、このエリアには [Fabric Edge]、[Fabric Border]、および [Fabric Control Plane] のカテゴリで正常なネットワークデバイスの割合が表示されます。</p> <p>[View Network Health] をクリックして、[Network Health] ダッシュボードを開きます。 ネットワークの健全性のモニターとトラブルシューティング (99 ページ) を参照してください。</p>
[Wired Clients] と [Wireless Clients]	<p>有線クライアントとワイヤレスクライアントの間のスコア分布を示します。 [Wired] スコアまたは [Wireless] スコアは、企業全体の正常 (良好) な有線またはワイヤレスのクライアントデバイスの割合です。 クライアントヘルススコア (162ページ) を参照してください。</p> <p>[View Client Health] をクリックすると、[Client Health] ダッシュボードが開きます。 すべてのクライアントデバイスの健全性のモニターとトラブルシューティング (139ページ) を参照してください。</p>

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	<p>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。</p> <p>[View AAA Dashboard] をクリックして、[Network Services AAA] ダッシュボードを開きます。 AAA ネットワークサービスの監視 (197 ページ) を参照してください。</p>
[DHCP]	<p>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。</p> <p>[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 (200 ページ) を参照してください。</p>

ステップ 5 次の機能には、[Top 10 Issue Type] ダッシュレットを使用します。

[Top 10 Issues] ダッシュレット

対処する必要がある上位 10 件の問題を表示します（存在する場合）。問題は色分けされ、事前割り当てされた P1 から始まる優先度レベルで並び替えられます。

問題をクリックすると、スライドインペインが開き、問題のタイプに関する追加の詳細が表示されます。スライドインペインで問題のインスタンスをクリックします。必要に応じて、次の操作を実行できます。

- 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。
- 問題のインスタンスを無視するには、次の手順を実行します。
 1. [Status] ドロップダウンリストから、[Ignore] を選択します。
 2. スライダーで問題を無視する時間数を設定します。
 3. [Confirm] をクリックします。

[View All Issues] をクリックすると、[Open Issues] ウィンドウが開きます。

問題の詳細については、[未解決の問題を表示（233 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

- ネットワークについて (99 ページ)
- ネットワークの健全性のモニターとトラブルシューティング (99 ページ)
- デバイスの健全性のモニターとトラブルシューティング (109 ページ)
- ネットワークデバイスの正常性スコアの設定 (127 ページ)
- ファブリック デバイスで SNMP コレクタ メトリックを有効化 (128 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 (129 ページ)

ネットワークについて

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

ネットワークの健全性のモニターとトラブルシューティング

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

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



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

始める前に

アシユアランスを設定します。「[基本的な設定のワークフロー（15 ページ）](#)」を参照してください。

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

[Overall health] ダッシュボードが表示されます。


ステップ 2 [Network] タブをクリックします。

[Network health] ダッシュボードが表示されます。

図 7: [Network Health] ダッシュボード



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

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

ロケーションペインには、次の機能があります。

ロケーションオプション	
アイテム	説明
 トグルボタン [List View]	このトグルボタンをクリックすると、ネットワークのサイトとビルディングがリスト形式で表示されます。 ドロップダウンリストをクリックして、次のオプションを選択できます。 <ul style="list-style-type: none"> • [Hierarchical Site View] : リストをサイトレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。 • [Building View] : リストをビルディングレベルで並べ替えます。[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。
 トグルボタン [Map View]	このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、ネットワークサイトは問題の重大度に従って色分けされています。
 Hide Sites	[Hide Sites] アイコンをクリックして、サイトテーブルを非表示にします。
 トポロジツール	このアイコンをクリックすると、次のビューがある [Topology] ウィンドウが開きます。 <ul style="list-style-type: none"> • [Geographical View] : このトグルボタンをクリックすると、ネットワークが地理的マップで表示されます。  ロケーションにカーソルを合わせると、正常なデバイスの割合が表示されます。 <ul style="list-style-type: none"> •  [Topology View] : このトグルボタンをクリックすると、ネットワークにおけるコンポーネントの接続状況を示すトポロジが表示されます。 デバイスにカーソルを重ねると、デバイスロール、IP アドレス、ソフトウェアバージョンなどのデバイス情報が表示されます。デバイスの 360 度ビューを取得するには、[View Details 360] をクリックします。

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

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

c) [Apply] をクリックします。

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

- [Export Dashboard] : ネットワークダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- [Edit Dashboard] : ダッシュボードの表示をカスタマイズできます。ダッシュレットの位置の変更 (340 ページ) およびカスタムダッシュボードの作成 (335 ページ) を参照してください。

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

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

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

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

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

しきい値を変更するには、次の手順を実行します。

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

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

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

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

[Network Device Health Summary] ダッシュレット	
アイテム	説明
	<p>次のタブが含まれます。</p> <ul style="list-style-type: none"> • [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。 <ul style="list-style-type: none"> • ネットワーク正常性概要スコア : ネットワークの正常性の概要スコアは、ネットワーク全体または選択したサイトにおける正常（良好）なデバイスの割合です。ネットワークヘルススコア（130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。 <p>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。</p> <p>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。</p> <p>ハイパーリンク付きのデバイスカテゴリ（[Access]、[Core]、[Distribution]、[Router]、[Wireless Controller]、[Access Point]）をクリックして、スライドインペインに追加の詳細情報を表示できます。</p> • 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。 <p>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。</p> <ul style="list-style-type: none"> ● : 不良なネットワークデバイス。ヘルススコアの範囲は1～3です。 ● : 中程度のネットワークデバイス。ヘルススコアの範囲は4～7です。 ● : 良好なネットワークデバイス。ヘルススコアの範囲は8～10で

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

ステップ 9 [AP] ダッシュレットを使用して、次の情報を確認できます。




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

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

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

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

[Networks Devices] ダッシュレット	
アイテム	説明
[Type]	<p>[All]、[Access]、[Core]、[Distribution]、[Router]、[WLC]、および [AP] の各オプションを使用して、デバイスタイプに基づいてテーブルをフィルタリングします。</p> <p>(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。</p> <p>SDA ファブリックドメインの場合、オプション ([All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric WLC]、[Fabric AP]、[Extended Node]) を使用して、ファブリックタイプに基づいてテーブルをフィルタ処理します。</p>
全体的な正常性	<p>次のオプションを使用して、デバイスの全体的な正常性スコアに基づいてテーブルをフィルタリングします。</p> <ul style="list-style-type: none"> • [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	<p>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。</p> <p>(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。</p> <p>[Overall Health Score] 列で、正常性スコアの上にマウスカーソルを合わせます。デバイスの正常性スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。デバイスの正常性は、KPI メトリックの最小サブスコアです (デバイスのタイプに基づく)。ルータおよびスイッチの場合、次の KPI メトリックがあります。システムリソース (メモリ使用率と CPU 使用率)、データプレーン (アップリンクの可用性とリンクエラー)、ファブリック (コントロールプレーン到達可能性)。[Fabric Domain Name]、[Fabric Name]、および [Fabric Role] 列には、ファブリックドメイン名、ファブリック名、およびファブリックロール (エッジ、ボーダー、マップサーバーなど) が表示されます。</p> <p>[Reachability] 列には、デバイスのステータス (到達可能、アップ、到達不能、再起動など) が表示されます。</p>
デバイス 360	<p>[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。</p> <p>[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。</p>
 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。
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none">  をクリックします。 オプションのリストが表示されます。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。

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

[Network Devices Reachability] ダッシュレット

色分けされたチャートには、ルータ、スイッチ、およびワイヤレスコントローラの到達可能性ステータスが表示されます。

- Reachable
- Unreachable

[Latest] タブには、5 分間のスナップショットビューが表示されます。

[Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインで、タイムラインスライダにカーソルを合わせると、一定期間の到達可能性ステータスを表示できます。ロールとロケーションに基づく上位デバイスの到達可能性ステータス数が、水平バーグラフとしてタイムラインスライダの下に表示されます。

水平バーとして表示されるデータを選択し、[All]、[Access]、[Core]、[Distribution]、[Router]、[WLC] の各オプションを指定すると、到達可能性ステータス、デバイスタイプ、およびロケーションに基づいてテーブルをフィルタ処理できます。

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

[WAN Link Utilization] ダッシュレット

棒グラフには、使用可能な WAN リンクの WAN リンク使用率のみのステータスが表示されます。

(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。『Cisco DNA 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して、次の情報を確認できます。

[WAN Link Availability] ダッシュレット

色分けされたチャートには、ネットワークで使用可能な WAN リンクの情報が表示されます。

[Latest] タブには、使用されている WAN リンクの割合が表示されます。

[Trend] タブには、時間範囲の設定で選択した時間範囲のトレンドビューが表示されます。たとえば、時間範囲を過去 3 時間に設定すると、[Trend] タブには 3 時間のデータが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの要素を選択して、より詳細なデータを表示できます。

タイムラインスライダの下に水平バーとして表示されるデータを選択して、上位の場所（リンク数）とデバイスタイプ（リンク数）に基づいてテーブルをフィルタ処理できます。

デバイスの健全性のモニターとトラブルシューティング

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

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

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Network] タブをクリックします。

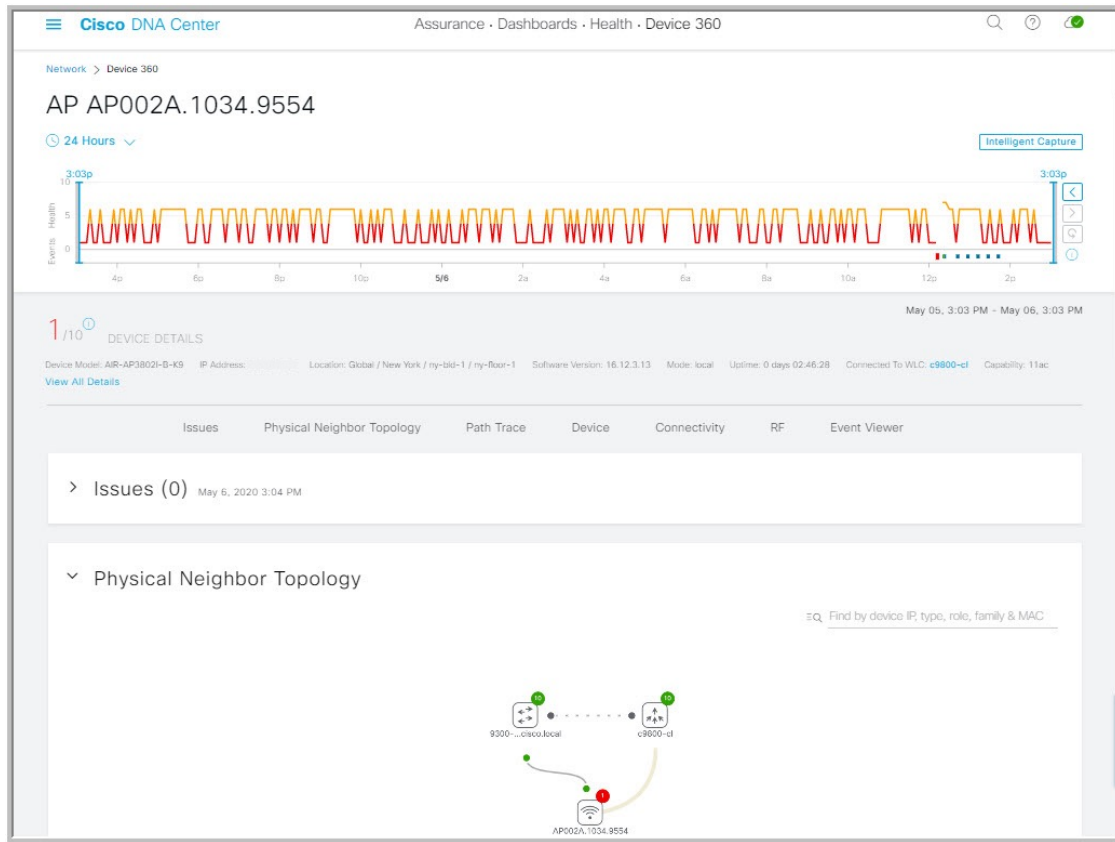
ステップ 3 [Network] 正常性ダッシュボードで、次のいずれかを実行します。

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

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

(注) デフォルトでは [Map View] が表示されます。

図 8: [Device 360] ウィンドウ



- ステップ 4** 時間範囲設定 (🕒 24 Hours) をクリックして、ウィンドウに表示されるデータの時間範囲を指定します。
- 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。
 - 開始日付と時刻、終了日付と時刻を指定します。
 - [Apply] をクリックします。

- ステップ 5** [Intelligent Capture] をクリックすると、特定のネットワークデバイスのキャプチャされたオンボーディングおよびデータパケットを表示、モニターリング、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理 (400 ページ) を参照してください。

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

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

(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。

タイムラインスライダには、次の機能があります。

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

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

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

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

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

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

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

- (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が含まれます。詳細については、「[スイッチヘルススコア \(131 ページ\)](#)」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 \(125 ページ\)](#) 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 \(126 ページ\)](#) を参照してください。

- **[Router]** : ルータの正常性スコアは、次のパラメータの最小サブスコアです。メモリ使用率、CPU 使用率、リンクエラー、リンク破棄、アップリンクの可用性、コントロールパネルへの到達可能性。詳細については、「[ルータヘルススコア \(133 ページ\)](#)」を参照してください。

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

- **[AP]** : AP の正常性スコアは次のパラメータの最小サブスコアです。メモリ使用率、CPU 使用率、リンクエラー、無線使用率、干渉、ノイズ、電波品質。詳細については、「[APヘルススコア \(134 ページ\)](#)」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ヘルススコア \(135 ページ\)](#) 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]** の場合、**[Fabric Role]**、**[Fabric Domain]**、**[Fabric Site]**、**[System Resources]**、**[Data Plane]**、**[Virtual Network]**、および **[Events]** の各要素がデバイス詳細エリアに表示されます。

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

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

[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]** の各要素がデバイス詳細エリアに表示されます。

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

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

スライドインペインでは、次の操作を実行できます。

- この問題を解決するには、次の手順を実行します。

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

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

次を実行できます。

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

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

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

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

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

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

- [For APs] : シナリオと、各シナリオにつながる一連のサブイベントが表示されます。これにより、どのサブイベントの間に問題が発生したのかを特定できます。送信電力の変更、RF チャンネル変更、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。
- [For switches and routers] : クリティカル以上の重大度 (致命的およびアラート) を示すすべての syslog、アップ/ダウンしているあらゆるリンクのイベント、到達可能デバイスまたは非到達可能デバイスのイベントが表示されます。また、クリティカルレベルより重大度が低い syslog (エラー、注意、通知、および情報) も表示されます。詳細については、[スイッチおよびルータの重大レベルに満たない選択済み Syslog \(124 ページ\)](#) を参照してください。
- [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。

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

[パストレースの実行 \(411 ページ\)](#) 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 \(165 ページ\)](#) 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 \(173 ページ\)](#) を参照してください。

(注) このカテゴリは、ルータのみに表示されます。

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

次の各タブをクリックすると、対応する詳細が表示されます。

[Device Info] タブ

デバイスの CPU、メモリ、稼働時間、温度などに関する情報を表示します。

(注) 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。

(注) 帯域外で設定されたネットワークデバイスの場合、稼働時間のチャートは正常性スコアやその他のデータと正しく関連しません。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～午後 2 時 00 分の 3 時間ウィンドウを選択（タイムラインスライダを使用）しても、ダウンタイムが表示されません。この問題は、Cisco DNA Center がデバイスからシステム稼働時間情報を受信できないために発生します。この問題を回避するには、デバイスと Cisco DNA Center の間で構成を同期させます。

[Connectivity] タブ

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

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

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

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

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

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

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

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

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

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

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

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

[Fabric Site] タブ

このタブは、SD-Access ファブリックで使用できます。

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

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

[Interfaces] タブ

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

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

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

(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。

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

[PoE] タブ

このタブは、PoE 対応スイッチおよび AP で使用できます。

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

スイッチ

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


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

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

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

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

このテーブルは次の方法でカスタマイズできます。

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

AP

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

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

[StackWise] タブ

このタブは、Cisco StackWise に対して表示されます。

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

[StackWise Virtual] タブ

このタブは、Cisco StackWise Virtual に対して表示されます。

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

[RF] タブ

このタブは、AP とワイヤレスクライアントに対して表示されます。

- [RF] タブには、[Radio 0]、[Radio 1]、[Radio 2] のように、無線固有の KPI に対応するタブがあります。それぞれの無線のタブをクリックすると、その無線のチャンネル使用率、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、チャンネル情報などのチャートが表示されます。

(注) [RF] タブの制限

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

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

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

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

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

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

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

[Virtual Network] タブ

このタブは、SD-Access ファブリックで使用できます。

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

[Transits and Peers Network] タブ

このタブは、SD-Access ファブリックで使用できます。

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

[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ンネル、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、無線固有の次の 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。

- 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** [View Floor] ドロップダウンリストから、AP 無線を比較するフロアを選択します。
- フロアマップ上の AP アイコンにカーソルを合わせると、AP 無線のデバイスの詳細 ([MAC Address]、[Model]、[Mode]、[Issue Count] など) が表示されます。
- ステップ 18** [Compare AP Radios] をクリックしてフロアマップ上の AP 無線を比較します。
- [Map View] がデフォルトで表示され、最後の 5 分間の AP 無線データが表示されます。
- ステップ 19** フロアマップ上の AP アイコンをクリックします。
- 比較する無線を選択または選択解除するためのダイアログボックスが表示されます。
- ステップ 20** フロアで比較する無線のリストの横にあるチェックボックスをオンにします。

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

ステップ 21 [AP Radio Compatibility] を使用して、比較のために選択された AP 無線のリストを表示します。
[Radio]、[IP Address]、[Model]、[Uptime]、[Connected to WLC]、[Floor] を比較できます。

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

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

- チャンネル情報
- 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
- チャンネルの使用率
- 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。

スイッチおよびルータの重大レベルに満たない選択済み Syslog

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

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

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

Cisco StackWise Virtual と制限事項について

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

StackWise Virtual 対応デバイス

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

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

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

StackWise Virtual の制限事項

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

- Cisco StackWise Virtual を設定した後も、2 番目のスイッチはインベントリに表示されたままになります。独自の IP アドレスがないため、応答を停止します。回避策として、次が可能です。
 1. インベントリから 両方のスイッチを削除します。 [ネットワーク デバイスの削除 \(79 ページ\)](#) を参照してください。
 2. StackWise Virtual を設定します (2つのスイッチを1つの仮想スイッチに設定します)。
 3. デバイスを検出します。 [IP アドレス範囲を使用したネットワークの検出 \(29 ページ\)](#)、[CDP を使用したネットワークの検出 \(21 ページ\)](#)、または [LLDP を使用したネットワークの検出 \(37 ページ\)](#) を参照してください。



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

- Cisco StackWise Virtual を削除すると、2つのスイッチは独立します。両方が同じ IP アドレスを持ち、デュアルアクティブ検出 (DAD) 状態で動作します。回避策として、次が可能です。
 1. 2 番目のスイッチで別の IP アドレスを設定します。
 2. デバイスをもう一度検出します。 [IP アドレス範囲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 \(21 ページ\)](#)、または [LLDP を使用したネットワークの検出 \(37 ページ\)](#) を参照してください。

Cisco StackWise と制限事項について

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

Cisco StackWise 対応デバイス

Cisco StackWise をサポートするデバイスを次に示します。

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

StackWise の制限事項

Cisco StackWise には、次の既知の制限事項があります。

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

ネットワークデバイスの正常性スコアの設定

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

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

[Health Score] ウィンドウが表示されます。

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

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

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

KPI のスライドインペインが表示されます。

ステップ 4 KPI の正常性スコアを次のように設定します。

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

(注) ネットワークデバイスの正常性スコアは、含まれるすべての KPI の中で最も低いスコアです。

制約事項 正常性スコアの計算には、少なくとも 1 つの KPI を含める必要があります。

注目 ネットワークデバイスの KPI 正常性スコアを表示する際、除外された KPI には正常性スコアの代わりに「NA」と表示されます。

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

ステップ 5 [Apply] をクリックします。

確認のダイアログボックスが表示されます。

ファブリック デバイスで SNMP コレクタ メトリックを有効化

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

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

ステップ 2 [Collectors] をクリックします。

コレクタのリストが表示されます。

ステップ 3 [COLLECTOR-SNMP] をクリックします。

[COLLECTOR-SNMP] ウィンドウが開きます。

ステップ 4 [+ Add] をクリックします。

[SNMP Configuration] ダイアログ ボックスが開きます。

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

図 9: SNMP の設定

SNMP Configuration

Configuration for SNMP collector Configuration

List of metrics to be enabled*

- CPU
- Memory
- Interface
- Environment Temperature
- Interface Availability
- Device Availability
- QOS
- RTTMON
- LISP
- CLISP

Polling Interval

10.00

Collector Information

Satellite ID

satellite0

Site ID

site0

Configuration Name*

SNMP_Config

Keep the name unique for this configuration

Keep the name unique for this configuration

Save Configuration

367645

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

ステップ 7 [Save Configuration] をクリックします。

ネットワークの正常性スコアと KPI メトリックについて

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

ネットワークヘルススコア

ネットワークの正常性スコアは、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。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） \div 100 （ネットワークデバイスの総数）

デバイスカテゴリの正常性スコア

デバイスカテゴリの正常性スコア（アクセス、コア、ディストリビューション、ルータ、ワイヤレス）は、ターゲットカテゴリ内の正常なネットワークデバイスの数（正常性スコアが8～10）をそのカテゴリのネットワークデバイスの総数で割ったパーセンテージです。スコアは5分ごとに計算されます。

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8～10のネットワークデバイス） \div 100 （そのカテゴリのネットワークデバイス）

個別のデバイス正常性スコア

個別のデバイスの正常性スコアは、KPIメトリック正常値スコア（システムの正常性、データプレーンの接続性、コントロールプレーンの接続性）の内の最小スコアになります。KPIメトリックスコアは、KPIごとに定義されるしきい値に基づきます。

デバイス正常性スコア = MIN（システムの正常性、データプレーンの接続性、コントロールプレーンの接続性）

デバイスのタイプに応じて、メトリックは変わります。

システムの正常性	
デバイスタイプ	説明
スイッチ（アクセスおよび配信）	CPU使用率やメモリ使用率などのシステムモニターリングメトリックが含まれます。
ワイヤレス	次のシステムモニターリングメトリックが含まれます。 <ul style="list-style-type: none"> ワイヤレスコントローラの場合、メモリ使用率、空きタイマー、空き Mbufが含まれます。 APの場合、CPU使用率とメモリ使用率が含まれます。
ルータ	CPU使用率やメモリ使用率などのシステムモニターリングメトリックが含まれます。

システムの正常性	
デバイスタイプ	説明
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）	<p>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。</p> <p>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。</p>
ワイヤレス	<p>次のシステムモニターリングメトリックが含まれます。</p> <ul style="list-style-type: none"> ワイヤレスコントローラの場合、WQE プール、パケットプール、リンクエラーなどのメトリックが含まれます。 AP の場合、インターフェイス、ノイズ、電波品質、無線利用率などの RF メトリックが含まれます。
ルータ	リンクエラーなどのメトリックが含まれます。

コントロールプレーンの接続性	
デバイスタイプ	説明
ワイヤレス	<p>次の KPI が含まれます。</p> <ul style="list-style-type: none"> ワイヤレスコントローラの場合、コントロールプレーンノードサーバーへの接続性が含まれます。 ファブリックデバイスの場合、コントロールプレーンノードへの接続性などのメトリックが含まれます。

スイッチヘルススコア

スイッチヘルススコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	<ul style="list-style-type: none"> CPU 使用率が 95 パーセント以下の場合、スコアは 10 です。 CPU 使用率が 95 パーセント以上の場合、スコアは 1 です。

パラメータ	スコアの計算
メモリ使用率	<ul style="list-style-type: none"> 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)	<p>リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス (スイッチ、ルータ、ワイヤレスコントローラ、AP など) 間のトポロジリンクを指します。</p> <p>物理インフラストラクチャインターフェイスにエラーがある場合のスコアは 8、すべてのリンクがダウンしている場合は 1、それ以外の場合は 10 です。</p>
リンク破棄	<p>リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス (スイッチ、ルータ、ワイヤレスコントローラ、AP など) 間のトポロジリンクを指します。</p> <p>物理インフラリンクにパケットドロップ (廃棄) がある場合、すべてのリンクで廃棄が発生した場合のスコアは 8、それ以外の場合は 10 です。</p>
リンクステータス	<p>リンクステータスのアップ/ダウンについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス (スイッチ、ルータ、ワイヤレスコントローラ、AP など) 間のトポロジリンクを指します。</p> <p>物理インフラストラクチャインターフェイスがダウンしている場合のスコアは 8、すべてのインターフェイスがダウンしている場合は 1、それ以外の場合は 10 です。</p>

パラメータ	スコアの計算
コントロールプレーンノードへの接続 - ファブリックデバイスのみ (エッジおよびポーター)	<ul style="list-style-type: none"> 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。 <p>(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。</p> <p>(注) ヘルススコアをファブリックデバイス向けに正しく入力するには、SNMP コレクタ メトリックを有効にします。ファブリックデバイスでSNMP コレクタ メトリックを有効化 (128 ページ) を参照してください。</p>

ルータ ヘルス スコア

ルータ ヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> メモリ使用率が95パーセント以下の場合、スコアは10です。 メモリ使用率が95パーセント以上の場合、スコアは1です。
WAN 接続	<ul style="list-style-type: none"> 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	<p>リンクエラーについては、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス (スイッチ、ルータ、ワイヤレスコントローラ、APなど) 間のトポジリンクを指します。</p> <p>物理インフラストラクチャ インターフェイスにエラーがある場合のスコアは8、すべてのリンクがダウンしている場合は1、それ以外の場合は10です。</p>

パラメータ	スコアの計算
リンク破棄	<p>リンク破棄については、インフラストラクチャリンクだけが考慮されます。インフラストラクチャリンクとは、ネットワークデバイス（スイッチ、ルータ、ワイヤレスコントローラ、AP など）間のトポロジリンクを指します。</p> <p>物理インフラリンクにパケットドロップ（廃棄）がある場合、すべてのリンクで廃棄が発生した場合のスコアは8、それ以外の場合は10です。</p>

AP ヘルス スコア

AP ヘルス スコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
CPU 使用率	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<p>スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。</p> <ul style="list-style-type: none"> • 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	<p>スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。</p> <p>2.4 GHz 無線の場合：</p> <ul style="list-style-type: none"> • 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。 <p>5 GHz 無線の場合：</p> <ul style="list-style-type: none"> • 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	<p>スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。</p> <p>2.4 GHz 無線の場合：</p> <ul style="list-style-type: none"> 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。 <p>5 GHz 無線の場合：</p> <ul style="list-style-type: none"> 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	<p>スコアは無線ごとに個別に計算されて、平均無線スコアが確定します。</p> <p>2.4 GHz 無線の場合：</p> <ul style="list-style-type: none"> 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。 <p>5 GHz 無線の場合：</p> <ul style="list-style-type: none"> 電波品質が 75 パーセント以上の場合、スコアは 10 です。 電波品質が 75 パーセント未満の場合、スコアは 1 です。

ワイヤレスコントローラのヘルススコア

ワイヤレスコントローラのヘルススコアは、次のパラメータの最小サブスコアです。

パラメータ	スコアの計算
メモリ使用率	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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。

パラメータ	スコアの計算
空きメモリバッファ (MBufs)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。 <p>(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。</p>

ネットワークヘルススコアと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。Cisco DNA 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

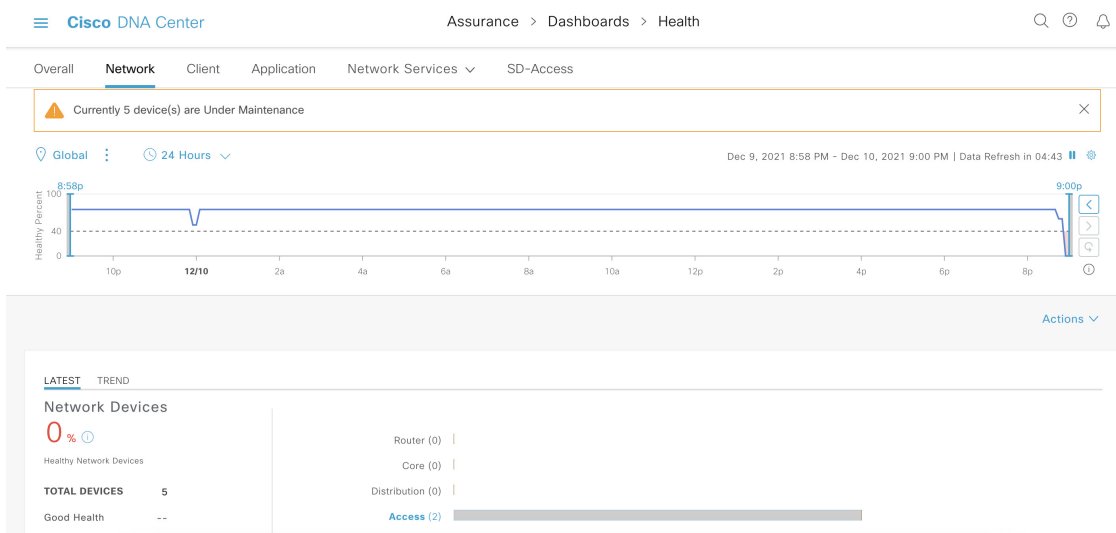
ンスモードになったかに関係なく、メンテナンスモードのすべてのデバイスを同じように扱います。

ネットワークデバイスがメンテナンスモードの間は、Cisco DNA Center はデバイスに対して次のタスクを実行しないため、ネットワーク正常性スコアとKPIメトリックには、メンテナンスモードのネットワークデバイスは含まれません。

- 正常性データを収集します。
- インターフェイス統計を収集します。
- トリガーの問題。
- サイトの正常性スコアなどの正常性スコアの計算にデバイスを含まず。

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、Cisco DNA Center では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、メンテナンスウィンドウの開始時刻と終了時刻が [device 360] ページに表示され、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 10: メンテナンスバナー付きの [Device 360] ページ



Cisco DNA Center は、メンテナンスモードのデバイスに対して次のタスク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。
- アシユ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。



第 7 章

クライアント正常性のモニターとトラブルシューティング

- [クライアントについて](#) (139 ページ)
- [すべてのクライアントデバイスの健全性のモニターとトラブルシューティング](#) (139 ページ)
- [クライアントデバイスの健全性のモニターとトラブルシューティング](#) (154 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](#) (161 ページ)

クライアントについて

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

すべてのクライアントデバイスの健全性のモニターとトラブルシューティング

クライアントが、ネットワークデバイス（アクセスポイントやスイッチ）に接続されているエンドデバイス（コンピュータ、電話など）であること。Cisco DNA Center は、有線クライアントとワイヤレスクライアントの両方をサポートしています。

この手順を使用して、すべての有線およびワイヤレスのクライアントの正常性の概要を把握し、対処する必要がある潜在的な問題があるかどうかを判断します。

アシュアランス 機械学習（ML）アルゴリズムを使用してネットワーク内の動作パターンを抽出し、トレンドを予測します。これらのトレンドは、[Client Onboarding Time] ダッシュレットおよび [Client Count Per SSID] ダッシュレットに基準として表示されます。



(注) HA フェールオーバーが発生した場合、クライアントの正常性データの表示に 1 時間かかることがあります。

始める前に

アシュアランスを設定します。「[基本的な設定のワークフロー \(15 ページ\)](#)」を参照してください。

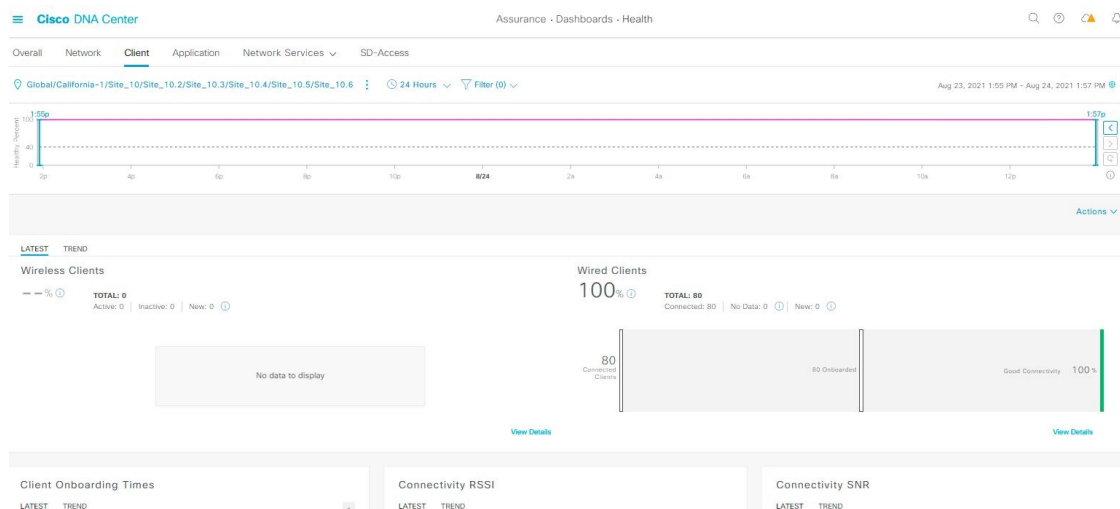
ステップ 1 [Health]メニューアイコン (☰) をクリックして、**アシュアランス** >。

[Overall health] ダッシュボードが表示されます。


ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

図 11: クライアントの正常性ダッシュボード



ステップ 3 次の機能には、[Client] 正常性ダッシュボードの上部メニューバーを使用します。

[Client] 正常性ダッシュボードの上部メニューバー	
アイテム	説明
 Global [Location] ペイン	<p>クリックすると、次のアイコンが表示されます。</p> <ul style="list-style-type: none">  Global  をクリックして、左側の階層ツリー ペインから、エリア、建物、またはフロアを選択します。 ロケーションアイコンの横にある  をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。  Hide Sites をクリックして [Sites] テーブルを非表示にします。   : このトグルボタンをクリックすると、ドロップダウンリストを使用して、サイトまたは建物ごとの正常なクライアントの割合をテーブル形式で表示できます。ロケーションに対して [Apply] をクリックすると、[Client Health] ダッシュボードにはそのロケーションのクライアント情報のみが表示されます。   : このトグルボタンをクリックすると、すべてのクライアントサイトの正常性が、地理的ロケーションに基づいたクライアント正常性マップで表示されます。デフォルトでは、クライアントサイトは問題の重大度に従って色分けされています。 <p>ヘルス スコアの色は、その重大度を示します。正常性は 1 ~ 10 のスケールで測定され、10が最高スコアになります。スコア 0は、クライアントが非アクティブであることを示します。</p> <p>[Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Client Health] ダッシュボードに表示されます。</p>
 時間範囲の設定	<p>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。</p> <ol style="list-style-type: none"> ドロップダウンメニューで範囲の長さ ([3 Hours]、[24 Hours]、または[7 days]) を選択します。 [開始日付 (Start Date)]と時刻、[終了日付 (End Date)]と時刻を指定します。 [Apply] をクリックします。

[Client] 正常性ダッシュボードの上部メニューバー	
アイテム	説明
[Filter] アイコン	<p>[SSID] および [Band] オプションが含まれます。ドロップダウンリストから SSID と帯域周波数の隣にあるチェックボックスをオンにして選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。</p> <p>(注) 複数の SSID を選択できます。たとえば、クラス 1 およびクラス 2 の SSID を選択した場合、ダッシュボードには、クラス 1 SSID とクラス 2 SSID に接続されているクライアントの情報が表示されます。</p>
[Actions] ドロップダウン リスト	<p>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。</p> <p>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 (340 ページ) および カスタムダッシュボードの作成 (335 ページ) を参照してください。</p>

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。

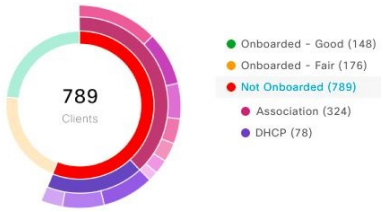
しきい値を変更するには、次の手順を実行します。

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

(注) [Client Summary] の [Health Score] が赤色で表示される場合、カスタムしきい値の変更に影響が出ます。カスタムしきい値によって、正常または異常なデバイスの数が変わることはありません。

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

[Client Health Summary] ダッシュレット	
アイテム	説明
[Client Health Summary] エリア	<p>次のタブが含まれます。</p> <ul style="list-style-type: none"> • [Latest] : デフォルトで表示されます。主要な構成は以下のとおりです。 <ul style="list-style-type: none"> • [Wireless Clients] と [Wired Clients Health Summary Score] : ワイヤレスおよび有線クライアントの正常性スコアは、正常にオンボードされ接続性が良好なクライアントの割合です。 クライアントヘルススコア (162 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。 <p>(注) 新しいクライアントは、健全性スコア計算ウィンドウの開始5分後に、オンボードを試行するクライアントです。これらのクライアントの正常性スコアは、次の5分間の計算ウィンドウに含まれます。</p> • [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。 <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> ● : 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]	<p>[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。</p> <p>放射状棒チャートは、オンボーディングに失敗したクライアントの分布と、オンボーディング失敗の理由を示します。各セグメントをクリックして、失敗の理由を表示できます。</p>  <ul style="list-style-type: none"> • そのセグメントのクライアント数別のデータタイプカテゴリ。 • そのセグメント内のクライアントの詳細データが格納されたテーブル。

ステップ 6 ネットワーク内のクライアントの特定の KPI とメトリックを表示するには、KPI ダッシュレットを使用します。次の表では、KPI ダッシュレットについて説明します。

(注) チャートデータは 5 分ごとに更新されます。

[Client Onboarding Times] ダッシュレット	
アイテム	説明
[Client Onboarding Times] チャート	<p>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。</p> <p>チャートには、次の2種類があります。</p> <ul style="list-style-type: none"> • [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。 <p>(注) [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析の機能については、AI ネットワーク分析を有効にする必要があります。 Cisco AI Network Analytics データ収集の設定 (87 ページ) および Cisco AI Network Analytics の概要 (9 ページ) を参照してください。</p> <p>重要 基準チャートを表示するには、[Filter] オプションからサイトと SSID を選択する必要があります。</p> <p>基準チャートの詳細は、異なる色で表示されます。</p> <ul style="list-style-type: none"> • 緑色のバンド : 予測基準値。 • 青色の実線 : 実際の値。 <p>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。</p>

[Client Onboarding Times] ダッシュレット	
アイテム	説明
[View Details]	<p>[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。</p> <ul style="list-style-type: none"> 左側のペインには、[Overall]、[Association]、[Authentication]、[DHCP] タブが表示されます。タブをクリックすると、右側のペインにチャートが表示されます。 右側のペインに表示される [Charts] には、次のタブがあります。 <ul style="list-style-type: none"> [Latest] : 全体の平均オンボーディング時間が表示されます。 <p>[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。</p> <ul style="list-style-type: none"> [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。 <p>左ペインで選択したタブに応じて、[Trend] > [Baseline] の下に追加のタブが表示されます。たとえば、[Association]、[Authentication]、または [DHCP] データの [Authentication]、[Time Baseline]、または [Failure Baseline] タブが表示されます。</p> <p>(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。</p> <p>(注) [Baseline]、[Time Baseline]、および [Failure Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析の機能については、AI ネットワーク分析を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 (87 ページ) および Cisco AI Network Analytics の概要 (9 ページ) を参照してください。</p> <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> 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]	<p>[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。</p> <ul style="list-style-type: none"> 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]	<p>[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。</p> <ul style="list-style-type: none"> 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]	<p>[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。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> [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。 <p>(注) [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析の機能については、AI ネットワーク分析を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 (87 ページ) および Cisco AI Network Analytics の概要 (9 ページ) を参照してください。</p> <p>重要 SSID 機械学習の基準チャートを表示するには、[Filter] オプションからサイトと SSID を選択する必要があります。</p> <ul style="list-style-type: none"> 基準チャートの詳細は、異なる色で表示されます。 <ul style="list-style-type: none"> 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]	<p>[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。</p> <p>次の 2 種類のチャートから構成されます。</p> <ul style="list-style-type: none"> • 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。 <p>(注) [Baseline] タブは、近い将来に廃止される予定です。AI ネットワーク分析の機能については、AI ネットワーク分析を有効にする必要があります。Cisco AI Network Analytics データ収集の設定 (87 ページ) および Cisco AI Network Analytics の概要 (9 ページ) を参照してください。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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	<p>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。</p>
[View Details]	<p>[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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> 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。 <ul style="list-style-type: none"> クライアント数別のデータタイプカテゴリ : [Top Locations]、[Top Access Points]、[Top Host Device Types]、[Top SSIDs]、[Top Bands]、および [Top Host Operating Systems]。 そのセグメント内のクライアントの詳細データが格納されたテーブル。




ステップ 7 ネットワーク内のクライアントに関する詳細情報を表示するには、[Client Devices] ダッシュレットを使用します。このダッシュレットには、次の機能があります。

[Client Devices] ダッシュレット	
アイテム	説明
[Type]	クライアントのタイプに基づいてテーブルをフィルタ処理します。オプションは、[Wired] および [Wireless] クライアントです。

[Client Devices] ダッシュレット	
アイテム	説明
ヘルス (Health)	<p>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。</p> <ul style="list-style-type: none">• すべて• Inactive : 正常性スコアが 0 のクライアントデバイス。• Poor : 正常性スコアが 1 ~ 3 のクライアントデバイス。• Fair : 正常性スコアが 4 ~ 7 のクライアントデバイス。• Good : 正常性スコアが 8 ~ 10 のクライアントデバイス。• No Data : データのないクライアントデバイス。
データ	<p>次のオプションを使用して、データタイプを基にテーブルをフィルタリングします。</p> <ul style="list-style-type: none">• [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
	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>[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。</p> <ul style="list-style-type: none"> • [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。 <p>(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。</p> <ul style="list-style-type: none"> • [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。 <p>(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、次の5分間の計算ウィンドウに含まれます。</p> <ul style="list-style-type: none"> • [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。 <p>• Last Seen</p> <ul style="list-style-type: none"> • [AP Name] (ワイヤレスクライアントの場合のみ) : アクセスポイントの名前が表示されます。 • [Switch] (有線クライアントの場合のみ) • [Port] (有線クライアントの場合のみ) • [Location] : クライアントの割り当て済みロケーションが表示されます。 • [Link Speed] (有線クライアントの場合のみ) : インターフェイスまたは物理ポートの速度容量を示します。ポートが特定の速度にネゴシエートされた場合は、ネゴシ

[Client Devices] ダッシュレット	
アイテム	説明
	<p>エートされた速度が表示されます。</p> <p>(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。</p>
[Tracked Clients]	[Tracked Clients] をクリックしてスライドインペインを表示します。このペインには、[MAC Address]、[Last detected]、[Tracking Duration]、[Description]、および [Randomized MACs] が含まれるテーブルが表示されます。
クライアントの [Client 360] の表示	<p>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。</p> <p>[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。</p>
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none">  をクリックします。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。
[Export]	<p>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。</p> <p>(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。</p>

クライアントデバイスの健全性のモニターとトラブルシューティング

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



(注) HA フェールオーバーが発生した場合、クライアントの正常性データの表示に 1 時間かかることがあります。

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

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

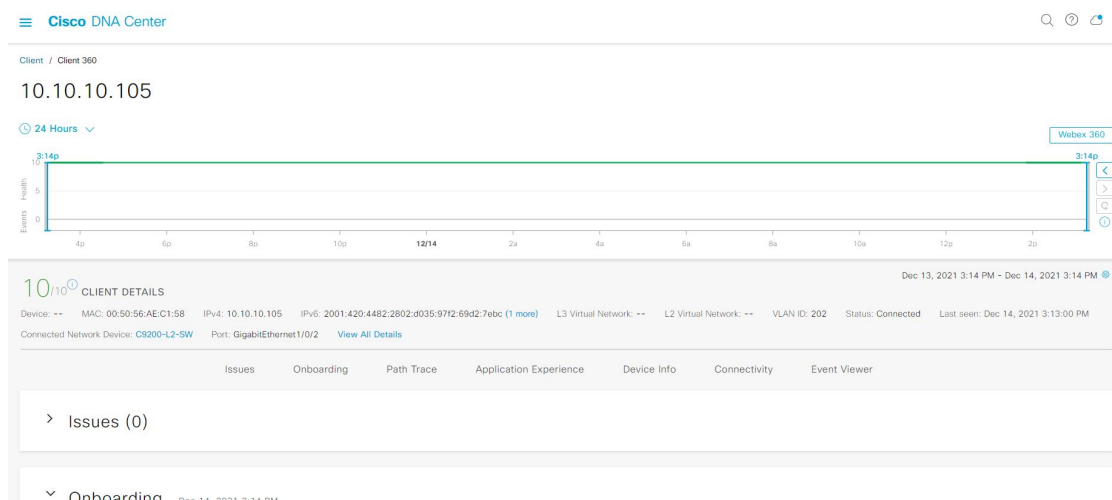
[Client Health] ダッシュボードが表示されます。

ステップ 3 次のいずれかを実行します。

- [クライアントデバイス (Client Devices)] 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索 (Search)] フィールド (右上端) に次のいずれかを入力します。ユーザ ID (Cisco ISE により認証済み)、IP アドレス、MAC アドレス。

[Client 360] ウィンドウに、クライアントデバイスの 360 度ビューが表示されます。

図 12: [クライアント 360 (Client 360)] ウィンドウ



ステップ 4 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

- 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。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [Apply] をクリックします。

ステップ 5 右上隅にある [Intelligent Capture] をクリックすると、特定のクライアントデバイスのキャプチャされたオンボーディングやデータパケットを表示、モニター、およびトラブルシューティングして、対処する必要がある潜在的な問題が存在するかどうかを確認できます。クライアントデバイスのライブキャプチャセッションの有効化 (381 ページ) を参照してください。

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

ステップ 6 タイムラインスライダの右上隅にある [Webex 360] をクリックして、クライアントの Webex ミーティングを表示し、監視します。ミーティング検索ポップアップウィンドウが表示されます。

Webex の統合を設定するには、『Cisco DNA Center Administrator Guide』の「Configure Webex Integration」を参照してください。

- 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。
- [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。
- このアプリケーションエクスペリエンス スライドインペインでは、次の機能を利用できます。

- **検索バー**：表示されたテーブルでミーティングを検索できます。
- **時間範囲フィルタ**：時間フィルタをクリックして、テーブルに表示するデータの時間範囲を指定します。
- クライアント ミーティングテーブルが表示されます。これには、ミーティング番号、ミーティング名、アプリケーション、ネットワーク接続時間、開始時刻、終了時刻、およびステータスが含まれます。

ミーティングを選択して、ミーティングの品質 KPI データを表示できます。これは、アプリケーション (Webex API を使用して取得されたデータ) とネットワーク (NetFlow を使用して取得されたデータ) の遅延に基づくオーディオ品質、ビデオ品質、および共有品質を示す水平バーとしてテーブルの下に表示されます。ドロップダウンリストを使用して、送信および受信オプションに基づいてデータをフィルタ処理し、パケット損失、ジッターなどのメトリックに関連するアプリケーションとネットワークの遅延グラフを表示できます。

ステップ 7 タイムラインスライダを使用すると、一定期間のクライアントデバイスに関する正常性およびイベント情報を表示できます。タイムラインスライダには、次の機能があります。

- **[Health]**：タイムラインスライダの上にカーソルを合わせると、5 分の時間枠におけるクライアントの正常性スコアと KPI が表示されます。色付きの円が付いた KPI は、個々のクライアントの正常性スコアの算出に使用されます。

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

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

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

- [Onboarding] : タイムラインスライダにカーソルを合わせると、関連付け、認証、DHCPを含むクライアントのオンボーディング時間が表示されます。
- [Events] : イベントデータは、色分けされた垂直バーとしてグラフに表示されます。緑の垂直バーは、成功したイベントを示し、赤の垂直バーは失敗したイベントを示します。

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

ステップ 8 タイムラインの下にある [Client Details] 領域で、個々のクライアントの正常性スコアを確認します。

個々のクライアントの正常性スコアは、クライアントのオンボーディングステータス、RSSI、および SNR を集約したものです。

ユーザー ID で検索する場合、表示される個別のクライアントヘルススコアは、そのユーザーに関連付けられているすべての監視対象クライアントデバイスの最も低いスコアです。詳細については、「[個別のクライアントヘルススコア \(163 ページ\)](#)」を参照してください。

MAC アドレスまたは IP アドレスで検索する場合、個別のクライアントヘルススコアはそのクライアントデバイスのヘルススコアです。

ヘルススコアの色は、その重大度を示します。正常性は 1 ~ 10 のスケールで計測されます。10 はベストスコアを示します。0 はクライアントデバイスが非アクティブであり、該当する正常性データが存在しないことを示します。

- : クライアントデバイスが不適切です。ヘルススコアの範囲は 1 ~ 3 です。
- : クライアントデバイスが適切です。ヘルススコアの範囲は 4 ~ 7 です。
- : クライアントデバイスが良好です。ヘルススコアの範囲は 8 ~ 10 です。
- : クライアントデバイスが非アクティブです。ヘルススコアは 0 です。

(注) ネットワークから切断されているクライアントの場合、スコアは - と表示されます。

ステップ 9 タイムラインの下にある [Client Details] 領域で、次の情報を確認します。

- ワイヤレスクライアントの場合、このエリアには、その OS バージョン、MAC アドレス (デバイス MAC と RCM を含む)、IPv4 および IPv6 アドレス、接続された VLAN ID、接続ステータス、最終検出タイムスタンプ、接続されたネットワークデバイス、SSID、最後の既知のロケーションなどのクライアントデバイスに関する情報が表示されます。
- 有線クライアントの場合、このエリアには、MAC アドレス、IPv4 および IPv6 アドレス、接続された VLAN ID、接続ステータス、最終検出タイムスタンプ、接続されたネットワークデバイス、ポート、最後の既知のロケーションなどのクライアントデバイスに関する情報が表示されます。
- PoE 対応デバイスの場合、[IEEE Class]、[Negotiated Power Level]、および [PoE Status] の各要素もクライアント詳細エリアに表示されます。

ステップ 10 [Client Details] エリアで [View All Details] をクリックします。クライアントデバイスに関する追加の詳細を含むスライドインペインが開きます。

ステップ 11 問題、オンボーディング、イベントビューア、パストレース、アプリケーション エクスペリエンスに関する情報、および詳細情報を表示するには、折りたたみカテゴリを使用します。

問題のカテゴリ

対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。

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

スライドインペインでは、次の操作を実行できます。

- この問題を解決するには、次の手順を実行します。
 1. ドロップダウンリストから [Resolve] を選択します。
 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。
- 問題を無視するには、次の手順を実行します。
 1. ドロップダウンリストから [Ignore] を選択します。
 2. スライダで問題を無視する時間数を設定します。
 3. [Confirm] をクリックします。
 4. 無視された問題の一覧を表示するには [Ignored Issues] をクリックします。

問題のタイプの詳細については、[問題の表示と管理 \(231 ページ\)](#) を参照してください。

オンボーディングカテゴリ

クライアントがどのようにネットワークに参加したかを示すトポロジ。AAA や DHCP などのサービスの情報も含まれます。

有線クライアントのトポロジの例：クライアント > スイッチ > ルータ

ワイヤレスクライアント トポロジの例：クライアント > SSID > アクセス ポイント > ワイヤレス コントローラ

トポロジでは、次の操作を実行できます。

- ノードをクリックして、ノードに関する情報が表示されたスライドインウィンドウを表示します。
- リンクの端（ドット）にマウスカースルを合わせると、リンクのステータスとポートの詳細が表示されます。
- デバイスのグループにカーソルを合わせて、ポップアップから [View Devices List] をクリックすると、デバイスのリストとその詳細が表示されます。
- [Onboarding] エリアの右上隅にある [Search] フィールドで、特定のデバイスを検索できます。特定のノードが選択され、デバイスの対応する情報が表示されます。

イベントビューカテゴリ

[For Wireless Clients] : シナリオと、各シナリオにつながる一連のサブイベントが一覧されます。これにより、どのサブイベントの間に問題が発生したのかを特定できます。次のシナリオがワイヤレスコントローラ向けに用意されています。

- **再認証 (Reauthentication)**

- [Broadcast Rekey] : 同一のキーによる暗号化データ量を制限するため、セッションキー（実行中の通信の暗号化キー）を変更するプロセス。

- **オンボーディング**

- **DHCP**

- **[Delete]**

- **内部ローミング**

- **内部ローミング**

- **ASSOC**

- **AUTH**

- **EAP**

- **DISASSOC**

- **DEAUTH**

- **11r 障害**

- **OKC 障害**

- **EAP 障害**

問題が発生するとイベントは赤色でマークされます。そうでない場合は緑色です。[Event Viewer] テーブルには、障害に関する情報（エラーメッセージ、クライアントが接続されている AP とワイヤレスコントローラ、イベント発生時のタイムスタンプなど）が表示されます。イベントをクリックすると、右側のペインにそのイベントに関する詳細情報が表示されます。

有線クライアントの場合: ISE サーバーイベント、スイッチシステムレベルの syslog、スイッチポートまたはインターフェイス固有のイベント、およびクライアント固有のイベントがリストされます。各イベントカテゴリのメッセージのリストについては、「[有線クライアントのイベントビューアに表示されるメッセージ \(161 ページ\)](#)」を参照してください。

成功したイベントは緑色で表示されます。正常性スコアに影響する障害イベントは赤色で表示されます。[Event Viewer] テーブルには、障害に関する情報（メッセージのタイプ、有線クライアントデバイスの接続先のデバイス情報、イベント発生時のタイムスタンプなど）が表示されます。イベントをクリックすると、右側のペインにそのイベントに関する詳細情報が表示されます。

パストレースのカテゴリ

[新しいパストレースの実行 (Run New Path Trace)] をクリックすると、指定した送信元デバイスと接続先デバイス間のネットワーク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 \(411 ページ\)](#) を参照してください。

アプリケーションエクスペリエンスのカテゴリ

クライアント デバイスで実行中のアプリケーション、およびその質的および量的なメトリック。

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

[アプリケーションエクスペリエンスとアプリケーションの可視性について \(165 ページ\)](#) 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 \(173 ページ\)](#) を参照してください。

詳細情報のカテゴリ

次のタブのいずれかをクリックして、対応する情報を表示します。

- [Device Info] : デバイスについての基本情報が表示されます。Samsung デバイスについては、このタブに、ビルド番号、製造元、国番号、デバイスタイプ (モバイル、タブレットなど)、ホストのオペレーティングシステムといった詳細情報が表示されます。
HW モデル、SW バージョン、AC/DC 電圧などの **ステーション情報** の詳細は、Intel デバイスについてのみ表示されます。
- [RF] : ワイヤレスデバイスでのみ使用できます。
- [User Defined Network] : UDN 対応のネットワークデバイスでのみ使用できます。このタブには、登録済みの UDN、接続された UDN の詳細、デバイスの MAC アドレス、デバイスの所有者、デバイス名、デバイスタイプ、および現在のステータスが表示されます。
- [Connectivity] : [Retries] という新しい接続 KPI が表示されます。無線接続の再試行回数が再試行チャートに表示されます。
- [PoE] : このタブは、PoE 対応クライアントで使用できます。
- [iOS Analytics] : Apple デバイスでのみ使用できます。
- [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。

有線クライアントのイベントビューアに表示されるメッセージ

[Client 360] ウィンドウで有線クライアントのイベントビューアに表示されるメッセージのリストを次の表に示します。

ISE サーバーイベント
Client AUTH FAILURE Client AUTH SUCCESS
スイッチシステムレベルの syslog
ALLDEADSERVER <ul style="list-style-type: none"> • 到達不可能なデバイス • 到達可能デバイス
スイッチポートまたはインターフェイス固有のイベント
トラップイベント <ul style="list-style-type: none"> • リンクダウン • リンクアップ PM-4-ERR_DISABLE ILPOWER-5-POWER_GRANTED ILPOWER-5-IEEE_DISCONNECT ILPOWER-5-INVALID_IEEE_CLASS ILPOWER-4-LOG_OVERDRAWN ILPOWER-3-SHUT_OVERDRAWN
クライアント固有のイベント
DOT1X-5-FAIL MAB-5-FAIL

クライアントの正常性スコアと KPI メトリックについて

ここでは、クライアントの正常性スコアと KPI メトリックの計算方法について説明します。

クライアントヘルススコア

クライアントの正常性スコア（ワイヤレスまたは有線）は、ターゲットカテゴリ内の正常なクライアントデバイス数（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8～10のクライアントデバイス）÷100（そのカテゴリのクライアントデバイスの総数）

個々のクライアントヘルススコアは、クライアントオンボーディングスコアとクライアント接続スコアの合計です。クライアントヘルススコアの範囲は1～10で、非アクティブなクライアントのスコアは0です。これは、次のとおり計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態で、認証および認可が成功し、IPアドレスを受信しています。クライアントスコアは10です。

ワイヤレスクライアント：クライアントがネットワークに参加しており、RSSIおよびSNR KPIの観点から接続が良好な状態です。

クライアントオンボーディングスコア

クライアントオンボーディングスコアは、ネットワークに接続中のクライアントデバイスのエクスペリエンスを示します。

- クライアントがネットワークに正常に接続している場合、スコアは4です。
- クライアントがネットワークに接続できない場合、スコアは1です。
- クライアントがアイドル状態の場合、スコアは0です。

クライアントオンボーディングスコアは、次のように計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態であり、認証と認可に成功しており、IPアドレスを受信されています。

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1～4です。クライアントがネットワークに正常に接続している場合、スコアは4です。クライアントがネットワークに接続できない場合、スコアは1です。

クライアント接続スコア

クライアント接続スコアは、デバイスがネットワークに接続された後のクライアントデバイスのエクスペリエンスを示します。スコアは、次のように計算されます。

有線クライアント：接続スコアは、2または6になります。リンクエラーにより、次のように、接続スコアとその結果の全体的な正常性スコアが決まります。

- クライアントオンボーディングは正常に行われたもののリンクエラーが発生した場合、接続スコアは2、全体的な正常性スコアは6です。

- クライアントオンボーディングが正常に行われ、クライアントとファーストホップスイッチの間にリンクエラーが発生していない場合、接続スコアは6、全体的なヘルススコアは10です。

ワイヤレスクライアント：接続スコアは、0、4、または10になります。RSSIとSNRの範囲によって接続スコアが決定され、その結果の全体的なヘルススコアはRSSI主導の接続スコアとSNR主導の接続スコアの加重平均として計算されます。

RSSI 主導の接続スコア	
クライアントの RSSI	RSSI 主導の接続スコア
RSSI が -72 dBm 以下の場合。	クライアントは、RSSI 主導の接続スコア 4 を獲得し、正常性が中程度であると見なされます。
RSSI が -72 dBm より大きい場合。	クライアントは、RSSI 主導の接続スコア 10 を獲得し、正常性が良好であると見なされます。

SNR 主導の接続スコア	
クライアントの SNR	SNR 主導の接続スコア
SNR が 9 以下の場合。	クライアントは、SNR 主導の接続スコア 4 を獲得し、正常性が中程度であると見なされます。
SNR が 9 より大きい場合。	クライアントは、SNR 主導の接続スコア 10 を獲得し、正常性が良好であると見なされます。

個別のクライアントヘルススコア

個々のクライアントヘルススコアは、クライアントオンボーディングスコアとクライアント接続スコアの合計です。クライアントヘルススコアの範囲は1～10で、非アクティブなクライアントのスコアは0です。これは、次のとおり計算されます。

有線クライアント：最初のスイッチへのリンクがアップ状態で、認証および認可が成功し、IPアドレスを受信しています。クライアントスコアは10です。

ワイヤレスクライアント：クライアントがネットワークに参加しており、RSSIおよびSNR KPIの観点から接続が良好な状態です。

クライアントのオンボーディングと接続性	クライアント正常性スコアの結果
クライアントがオンボーディングに失敗した場合。	クライアントの正常性スコアは1で、不良な状態であると見なされます。
クライアントのRSSIとSNRがしきい値を下回っている場合。	クライアントの正常性スコアは4で、正常性が中程度であると見なされます。

クライアントの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 \(165 ページ\)](#)
- [サポートされるプラットフォーム \(166 ページ\)](#)
- [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 \(168 ページ\)](#)
- [アプリケーションの正常性の前提条件 \(171 ページ\)](#)
- [アプリケーションテレメトリ設定のプロビジョニング \(173 ページ\)](#)
- [ホストのアプリケーションエクスペリエンスの表示 \(173 ページ\)](#)
- [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 \(175 ページ\)](#)
- [すべてのアプリケーションの健全性のモニター \(176 ページ\)](#)
- [アプリケーションの健全性のモニター \(184 ページ\)](#)
- [アプリケーションの正常性スコア設定の設定 \(193 ページ\)](#)
- [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 \(194 ページ\)](#)

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

アシュアランスは、複雑なアプリケーションデータを処理し、その結果をアシュアランス正常性ダッシュボードで提示することで、アプリケーションのパフォーマンスに関するインサイトを提供します。

正常性データは、デバイスの観点 ([Device 360] ウィンドウ)、ユーザーの観点 ([Client 360] ウィンドウ)、アプリケーションの観点 ([Application 360] ウィンドウ) でそれぞれ提供されます。

データの収集元に応じて、次の一部またはすべての情報を確認できます。

- Application Name
- スループット
- DSCP マーキング
- パフォーマンスメトリック (遅延、ジッター、パケット損失)

アプリケーション名とスループットを総称して定量的メトリックと呼びます。定量的メトリックのデータは、アプリケーション可視性を有効にすることで得られます。

DSCP マーキングとパフォーマンスメトリック（遅延、ジッター、パケット損失）は、総称して定性的メトリックと呼ばれます。定性的メトリックのデータは、アプリケーションエクスペリエンスを有効にすることで得られます。

アプリケーションの可視性

アプリケーション可視性のデータは、IOS-XEを実行しているスイッチ、およびAireOSを実行しているワイヤレスコントローラから収集されます。

IOS-XEを実行しているスイッチについては、物理レイヤのアクセススイッチポートに双方向（入力および出力）で適用される事前定義されたNBARテンプレートを使用してアプリケーション可視性のデータが収集されます。

AireOSを実行しているワイヤレスコントローラについては、ワイヤレスコントローラでアプリケーション可視性のデータが収集され、そのデータがストリーミングテレメトリを使用してCisco DNA Centerに送られます。

Application Experience

アプリケーションエクスペリエンスのデータは、Cisco IOS-XEルータプラットフォームから、Cisco Performance Monitor (PerfMon) 機能とシスコのアプリケーション応答時間 (ART) メトリックを使用して収集されます。

ルータプラットフォームの例には、ASR 1000、ISR 4000、CSR 1000v などがあります。Cisco DNA Center と互換性があるデバイスについては、『[Cisco DNA Center 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 Cisco DNA トラフィック テレメトリ アプリ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 \(166 ページ\)](#) を参照してください。

サポートされるプラットフォーム

次の表に、サポートされるプラットフォーム、データ収集のタイプ、およびソフトウェアとライセンスの要件を示します。



(注) Cisco DNA Center と互換性があるデバイスについては、『[Cisco DNA Center Compatibility Matrix](#)』を参照してください。

シスコのプラットフォームにおけるアプリケーションエクスペリエンスとアプリケーション可視性のサポート Cisco DNA Center		
プラットフォーム	Data Collection	注記
Cisco IOS-XE ルータ	アプリケーションエクスペリエンスのデータ収集	<ul style="list-style-type: none"> • アクティブなNBAR2ライセンスが必要。 • IOS XE 16.3 以上のソフトウェアバージョン。 • 最適化 APM の場合：IOS XE 17.3 以上のソフトウェアバージョン。
Catalyst 9000 シリーズ スイッチ	9200、9300、9400 のアプリケーション可視性のデータ収集	<ul style="list-style-type: none"> • Cisco DNA Advantage ライセンスが必要です。 • 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 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	<ul style="list-style-type: none"> • Cisco DNA 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。
Cisco 9800 シリーズ ワイヤレスコントローラ	Flex/Fabric SSID のアプリケーション可視性のデータ収集。 中央スイッチング/ローカル SSID のアプリケーションエクスペリエンスのデータ収集。	<ul style="list-style-type: none"> • 最適化 APM の場合：IOS XE 16.12.1 以上のソフトウェアバージョン。

シスコのプラットフォームにおけるアプリケーションエクスペリエンスとアプリケーション可視性のサポート Cisco DNA Center		
プラットフォーム	Data Collection	注記
Cisco DNA トラフィック テレメトリ アプライアンス	アプリケーションエクスペリエンスのデータ収集。	<ul style="list-style-type: none"> • Cisco DNA Advantage ライセンスが必要です。 • 最適化 APM の場合 : IOS XE 17.3 以上のソフトウェアバージョン。

デバイスでのアプリケーションテレメトリ有効化の基準

Cisco DNA Center では、新しい自動選択アルゴリズムに基づいてインターフェイスと WLAN を選択し、該当するすべてのインターフェイスと WLAN でアプリケーションテレメトリを自動的に有効にします。

アプリケーションテレメトリは、Cisco DNA Center を介してプロビジョニングされた WLAN にプッシュされます。



- (注)
- 従来のタギングベースのアルゴリズムがサポートされ、インターフェイスまたは WLAN の新しい自動選択アルゴリズムよりも優先されます。
 - 自動選択アルゴリズムからタギングベースのアルゴリズムに切り替える場合は、タグ付き SSID をデバイスに対してプロビジョニングする前にテレメトリを無効にする必要があります。

次の表に、サポートされているすべてのプラットフォームについて、従来のタギングベースのアルゴリズム（キーワード **lan** を使用）と新しい自動選択アルゴリズムに基づくインターフェイスと WLAN の選択基準を示します。

プラットフォーム	従来のタギングベースのアルゴリズム	自動選択アルゴリズム
Router	<ul style="list-style-type: none"> • インターフェイスの説明に lan キーワードが含まれている。12 • インターフェイスが物理インターフェイスである。 • インターフェイスに管理 IP アドレス以外の IP アドレスがある。 	<ul style="list-style-type: none"> • インターフェイスに管理 IP アドレス以外の IP アドレスがある。 • インターフェイスが次のいずれでもない。 <ul style="list-style-type: none"> • WAN <p>(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。</p> <p>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。</p> <p>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。</p> • 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	<ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • インターフェイスが物理インターフェイスである。 • アクセスポートにネイバーがない。 • インターフェイスが次のいずれでもない。 <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 リリース 16.12.1 以降	<p>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}</p> <p>(注) テレメトリ設定を更新する場合は、テレメトリを無効にしてから、設定の変更後にテレメトリを有効にする必要があります。</p>	SSID が混在している場合、つまりローカルモード、フレックスモード、およびファブリックモードの場合は、Cisco Application Visibility and Control (AVC) の基本レコードが設定されます。すべてのSSID がローカルモードの場合、最適化 APM レコードが設定されます。
Cisco DNA トラフィックテレメトリアプライアンスと最適化 APM プロファイルおよび IOS リリース 17.3 以降	<ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • インターフェイスが物理インターフェイスである。 • インターフェイスが管理インターフェイス (GIGABITETHERNET0、GIGABITETHERNET0/0、MGMT0、FASTETHERNET0、および FASTETHERNET1) ではない。

¹ **lan** キーワードは、大文字と小文字の区別はなく、スペース、ハイフン、または下線で区切ることができます。

² ネットワークデバイスを再同期して、**lan** インターフェイスの説明を読み取ります。

アプリケーションの正常性の前提条件

ここでは、ルータ、AireOS ワイヤレスコントローラ、スイッチのアプリケーションの正常性に関連する前提条件を示します。

ルータのアプリケーションエクスペリエンスの前提条件

- Cisco IOS XE ソフトウェアのアクティブな NBAR2 ライセンスが必要です。
- レイヤ 3 ネットワーク内のアプリケーションフローは可視化されません。
- 管理インターフェイスに関連付けられたトラフィックは、アプリケーションエクスペリエンスに含まれません。
- ポートは ETA に対して有効にできません。
- アシュアランスでアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイス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（168 ページ）](#)を参照してください。

スイッチのアプリケーション可視性の前提条件

- Cisco IOS XE ソフトウェアが必要です。
- Cisco DNA Advantage ライセンスが必要です。
- **switchport mode access** コマンドが含まれているアクセスポートにのみ実装されません。
- L2 論理インターフェイスのサポートは使用できません。
- スイッチポートが AP に接続されて **switchport mode access** が設定されている場合、可視性が制限されます。
- ポートは ETA に対して有効にできません。
- IPv4 フローのみがモニターされます。
- 管理インターフェイス Gig0/0 は、NetFlow エクスポートの送信元インターフェイスとして使用できません。
- アシュアランスでアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイス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（168 ページ）](#)を参照してください。

AireOS ワイヤレスコントローラのアプリケーション可視性の前提条件

- Cisco DNA Advantage ライセンスが必要です。
- AireOS ソフトウェアを搭載したワイヤレスコントローラでのみサポートされ、IOS XE ソフトウェアを搭載したワイヤレスコントローラではサポートされません。
- Cisco AireOS ワイヤレスコントローラでは NetFlow を有効にする必要があります。
- アシュアランスでアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイス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（168 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（168 ページ）](#)を参照してください。
- アシュアランスでアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイス間でクロックを同期する必要があります。

アプリケーション エクスペリエンスの前提条件 Cisco DNA トラフィック テレメトリ アプライアンス

- Cisco DNA Advantage ライセンスが必要です。
- 最適化 APM には IOS XE ソフトウェアが必要です。[デバイスでのアプリケーションテレメトリ有効化の基準（168 ページ）](#)を参照してください。
- アシュアランスでアプリケーションの正常性データを表示するには、Cisco DNA Center とデバイス間でクロックを同期する必要があります。

- CAPWAP でカプセル化されたワイヤレストラフィックの可視性を有効にするには、Cisco DNA トラフィック テレメトリ アプライアンス で **ip nbar Classification tunneled-traffic CAPWAP** コマンドを手動で入力します。

アプリケーションテレメトリ設定のプロビジョニング

テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 (85 ページ) の説明に従って、グローバルテレメトリ設定を構成します。

- ステップ 1** メニューアイコン (☰) をクリックして、**[Provision]>[Network Devices]>[Inventory]** の順に選択します。
- [Inventory] ウィンドウには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。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、次のいずれかを実行します。
- (注) アプリケーションテレメトリのオプションは、Cisco DNA Center からのアプリケーションテレメトリの有効化がデバイスでサポートされている場合のみ有効になります。
 - a) [Enable Application Telemetry] : 選択したデバイスでアプリケーションテレメトリを設定します。
 - b) [Disable Application Telemetry] : 選択したデバイスからアプリケーションテレメトリ設定を削除します。
- ステップ 4** [Apply] をクリックします。
- [Application Telemetry] 列には、テレメトリの設定ステータスが表示されます。デフォルトの列設定で [Application Telemetry] 列が表示されない場合は、列見出しの右端にある省略記号アイコン (⋮) 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 \(21 ページ\)](#)、または [LLDP を使用したネットワークの検出 \(37 ページ\)](#) を参照してください。

- ネットワークデバイスで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 \(173 ページ\)](#) 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 \(171 ページ\)](#) を参照してください。

ステップ 1 [Client 360] ウィンドウで、[Application Experience] カテゴリを展開します。

ステップ 2 [Application Experience] カテゴリから、次の操作を実行できます。

- a) 特定のビジネス関連グループから、それに対応するタブをクリックすることで、アプリケーションエクスペリエンスデータをテーブル形式で表示します。タブは、[Business Relevant]、[Business Irrelevant]、または [Default] です。

(注) 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]、[7 Days] です。デフォルトは、[24 Hours] です。

- b) テーブルでアプリケーションエクスペリエンスデータを表示します。

- [Name] : アプリケーション名。
- [Health] : 正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。詳細については、[個別アプリケーションの正常性スコア \(194 ページ\)](#) 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エーション (ミリ秒単位) (最大と平均)。

- c) アプリケーションエクスペリエンスメトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、および [Application Server Latency] です。

- (注) Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレスコントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

ネットワークデバイスのアプリケーションエクスペリエンスの表示

この手順を使用して、ネットワークデバイスで稼働しているアプリケーションの質的および量的なメトリックを表示できます。

始める前に

- デバイス（ルータ、スイッチ、ワイヤレスコントローラ、およびアクセスポイント）が検出されたことを確認します。 [IP アドレス範囲を使用したネットワークの検出（29 ページ）](#)、[CDP を使用したネットワークの検出（21 ページ）](#)、または [LLDP を使用したネットワークの検出（37 ページ）](#) を参照してください。
- ネットワークデバイスで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（173 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（171 ページ）](#) を参照してください。

ステップ 1 [Device 360] ウィンドウで、[Application Experience] カテゴリを展開します。

ステップ 2 [Application Experience] カテゴリから、次の操作を実行できます。

- a) 対応するタブ（[Business Relevant]、[Business Irrelevant]、[Default]）をクリックして、特定のビジネスとの関連性グループからアプリケーションエクスペリエンスデータを表形式で表示します。

(注) 表示されるデータは、[Client 360] ウィンドウでドロップダウンメニューから選択した時間に基づきます。オプションは、[3 Hours]、[24 Hours]（デフォルト）、または [7 Days] です。
- b) 適切なフィルタ（[All VRFs] および [All Interfaces]）を使用して、特定の VRF または特定のルータインターフェイスのアプリケーションエクスペリエンスデータをフィルタ処理します。

(注) [All VRFs] および [All Interfaces] フィルタは、ルータでのみ使用できます。
- c) テーブルでアプリケーションエクスペリエンスデータを表示します。
 - [Name] : アプリケーション名。
 - [Health] : 正常性スコアはパケット損失、遅延、およびジッターのメトリックの組み合わせに基づいて計算されます。正常性スコアの計算にアプリケーション遅延を含めることもできます。

(注) 正常性スコアは、Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。

- [Usage Bytes] : このアプリケーションに対してクライアントが転送したバイト数。
- [Average Throughput] : クライアントとサーバー間を流れているアプリケーショントラフィックのレート (Mbps 単位)。
- [DSCP] : アプリケーションの現在 ([Observed]) とデフォルト ([Expected]) の DSCP 値。

(注) このメトリックは、最適化 APM については提供されません。

- [Packet Loss] : パケット損失のパーセンテージ (最小と平均)。
- [Network Latency] : ネットワーク遅延時間 (最大と平均) (ミリ秒単位)。
- [Jitter] : ネットワーク上のデータパケット間の時間遅延のバリエーション (ミリ秒単位) (最大と平均)。

- d) アプリケーションエクスペリエンスメトリックをチャート形式で表示するには、アプリケーションの横にあるオプションボタンをクリックします。メトリックは、[Throughput]、[Packet Loss]、[Jitter]、[Network Latency]、[Client Network Latency]、[Server Network Latency]、[Application Server Latency]、および [Application Response Time] です。

(注) Cisco Catalyst 9200 スイッチ、Cisco Catalyst 9300 スイッチ、または Cisco AireOS ワイヤレスコントローラからエクスポートされるアプリケーション可視性のデータは、アプリケーション名、使用率、スループットのデータのみです。

すべてのアプリケーションの健全性のモニター

この手順を使用して、サイトにおけるアプリケーションのグローバルビューを表示します。

始める前に

- デバイス (ルータ、スイッチ、ワイヤレスコントローラ、およびアクセスポイント) が検出されたことを確認します。[IP アドレス範囲を使用したネットワークの検出 \(29 ページ\)](#)、[CDP を使用したネットワークの検出 \(21 ページ\)](#)、または[LLDP を使用したネットワークの検出 \(37 ページ\)](#) を参照してください。
- ネットワークデバイスで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 \(173 ページ\)](#) 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 \(171 ページ\)](#) を参照してください。

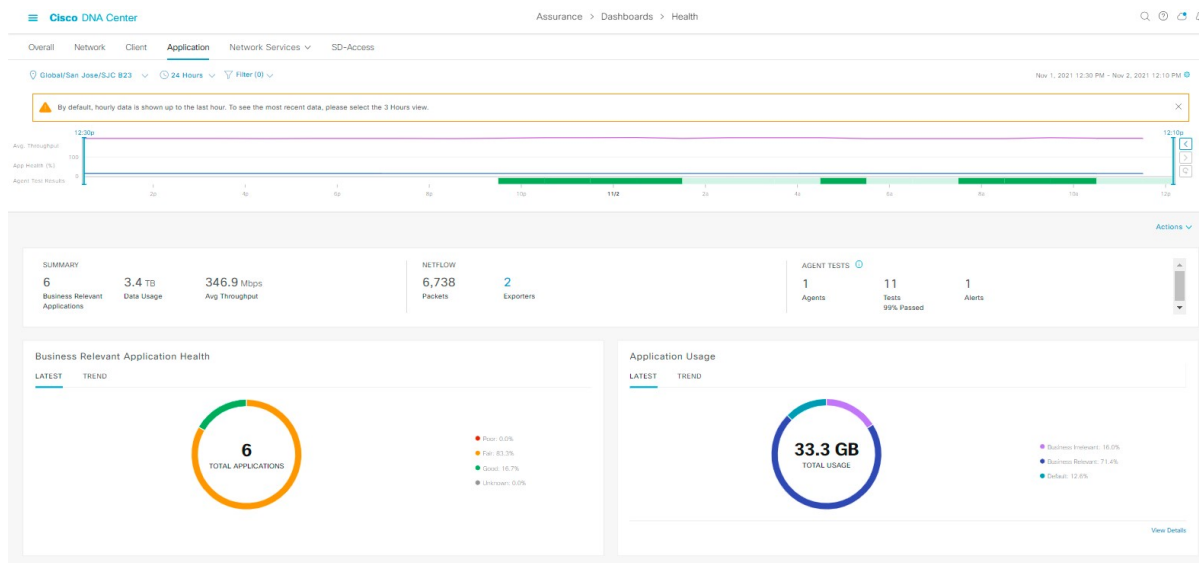
ステップ1 [Health]メニューアイコン (☰) をクリックして、アシュアランス >。

[Overall health] ダッシュボードが表示されます。




ステップ2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

図 13: [Application Health] ダッシュボード



ステップ3 次の機能には、[Application] 正常性ダッシュボードの上部のメニューバーを使用します。

[Application] 正常性ダッシュボードの上部のメニューバー	
アイテム	説明
 Global  [Location] ドロップダウンリスト	クリックすると、ロケーションアイコンが表示されます。ロケーションアイコンをクリックすると、[Site List View]が表示されます。特定のサイトまたはビルディングからアプリケーション情報を表示するには、適切な行で[Apply]をクリックします。ダッシュボード上の情報が、選択に応じて更新されます。
 [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。 <ol style="list-style-type: none"> ドロップダウンメニューで範囲の長さ ([3 Hours]、[24 Hours]、または [7 days]) を選択します。 [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。 [Apply] をクリックします。

[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
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 (340 ページ) および カスタム ダッシュボードの作成 (335 ページ) を参照してください。
アプリケーションの正常性タイムラインスライダ	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の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。
Netflow	NetFlow パケットの合計数を表示します。 エクスポートの合計数を表示します。エクスポートをクリックして、デバイス名、パケット数、レコード数、およびレート制限ドロップを含むテーブルを表示するスライドインペインを表示します。

[Summary] ダッシュレット	
アイテム	説明
Enterprise Agent Tests	<p>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、合格したテストの割合、アラート、およびアクティブなアラートの総数を表示します。</p> <p>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。</p> <ul style="list-style-type: none"> 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。 <p>ThousandEyes の統合を設定するには、『Cisco DNA Center Administrator Guide』の「<i>Configure ThousandEyes Integration</i>」を参照してください。</p>

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]	<p>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 (194 ページ) を参照してください。</p> <p>次のチャートが表示されます。</p> <ul style="list-style-type: none"> アプリケーション数分布トレンドチャートでは、すべてのビジネス関連のアプリケーション数が、正常性スコアに基づき積み上げ面グラフで時系列順に表示されます。 円グラフでは、ビジネス関連のアプリケーション数が、アプリケーションの正常性スコア別に分類されて示されます。カテゴリをクリックすると、カテゴリ内で正常性スコアが最も低いアプリケーションのリストが表示されます。

[Application Health] ダッシュレット	
アイテム	説明
[Application Usage]	<ul style="list-style-type: none"> 円グラフ：アプリケーションのビジネス関連性グループによって分類されたアプリケーション使用率の合計が表示されます。カテゴリをクリックすると、カテゴリ内の使用状況別に、上位 10 個のアプリケーションのリストが表示されます。 (注) アプリケーションの使用状況は、アプリケーションの双方向トラフィックから取得されます。 詳細の表示：[View Details] をクリックすると、追加の詳細情報を含むスライドインペインが開きます。スライドインペインでは、次の操作を実行できます。 <ul style="list-style-type: none"> [All Applications]、[Business Relevant]、[Business Irrelevant]、および [Default] タブをクリックすると、アプリケーションの使用率と使用率別上位 10 個のアプリケーションが記載されたチャートが表示されます。 スライドインペインの右上にあるドロップダウンリストを使用すると、アプリケーショングループまたはトラフィッククラス別にチャートをフィルタリングできます。 チャート内のカテゴリをクリックすると、[Application] テーブルにアプリケーションとその詳細情報が表示されます。



ステップ 6 次の機能については、[Application] ダッシュレットを使用します。

[Application] ダッシュレット	
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] があります。
[Health]	<p>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。</p> <ul style="list-style-type: none"> [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 4～7 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	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>アプリケーション名をクリックして、アプリケーションの 360 度ビューを表示することもできます。アプリケーションの健全性のモニター (184 ページ) を参照してください。</p> <ul style="list-style-type: none"> • アプリケーションテーブルには、webex-video、webex-audio、webex-app-sharing などの新しいアプリケーションが一覧表示されます。これらは、データが NetFlow データから収集される [Webex] の下にグループ化されます。 <p>[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 (189 ページ) を参照してください。</p> <ul style="list-style-type: none"> • [Health] : アプリケーションの正常性スコアが表示されます。 • [Business Relevance] : 可能な値は、[Business Relevant]、[Business Irrelevant]、および [Default] です。 • [Usage Bytes] : このアプリケーションに転送されたバイト数。 • [Average Throughput] : クライアントとサーバー間のアプリケーショントラフィックのフローレート (Mbps 単位)。 • [Packet Loss (%)] : パケット損失の割合。 • [Network Latency] : 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。

[Application] ダッシュレット	
アイテム	説明
⋮	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none"> ⋮ をクリックします。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。
[Export]	<p>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。</p> <p>(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。</p>

ステップ7 [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。

Enterprise Agent Tests	
アイテム	説明
[Enterprise Agent Tests] テーブル	<p>[Enterprise Agent Tests] 情報を表形式で表示します。デフォルトでは、エージェントテーブルには次の情報が表示されます。</p> <ul style="list-style-type: none"> • [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。 • [# of Alerts] : エージェントテストの総数を表示します。
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none"> 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。
 Export	<p>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。</p>

アプリケーションの健全性のモニター

この手順を使用して、特定のアプリケーションの詳細を表示します。

-
- ステップ 1** [Health]メニューアイコン (☰) をクリックして、**アシュアランス** >。
[Overall health] ダッシュボードが表示されます。
- ステップ 2** [Application] タブをクリックします。
[Application Health] ダッシュボードが表示されます。
- ステップ 3** [Application] テーブルで、アプリケーション名をクリックします。
[Application 360] ウィンドウが開き、アプリケーションの 360 度ビューが表示されます。
- ステップ 4** 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。
- 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。
 - [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
 - [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]	<p>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。</p> <p>(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。</p>
[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。ステップ 8 を参照してください。
[Exporters] タブ	クリックすると、NetFlow トラフィックを Cisco DNA Center に送信するデバイスのリストとその他の詳細情報が表示されます。「ステップ 9」を参照してください。

ステップ 9 [Issues] をクリックして、次の情報を確認します。

問題
<p>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。</p> <p>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。</p> <p>スライドインペインでは、次の操作を実行できます。</p> <ul style="list-style-type: none"> この問題を解決するには、次の手順を実行します。 <ol style="list-style-type: none"> ドロップダウンリストから [Resolve] を選択します。 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。 <ol style="list-style-type: none"> ドロップダウンリストから [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ます。 [Confirm] をクリックします。 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。 <p>問題のタイプの詳細については、問題の表示と管理 (231 ページ) を参照してください。</p>

ステップ 10 [Exporters] をクリックして、次の情報を確認します。

エクスポータ	
アイテム	説明
[Device]	<p>NetFlow トラフィックを Cisco DNA Center に送信しているデバイス（ルータ、スイッチ、ワイヤレスコントローラ、アプライアンスなど）のリストが表示されます。</p> <p>(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。</p> <p>「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.）」</p>

エクスポータ	
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 グラフ	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Thoughtput]	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 グラフ	
チャート	説明
[Latency]	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>(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。</p>
[Jitter]	<p>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）。</p> <p>(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。</p>
[DSCP]	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

ステップ 12 [Application Endpoint] のテーブルで、アプリケーションにアクセスしているクライアントのリストを確認します（メトリックチャートの後に表示されます）。


Cisco DNA Center で管理されるクライアントのみを表示する場合は、[Managed Clients] タブをクリックします。

このテーブルには、各クライアントの詳細が表示されます。これには、識別子（ユーザー ID、ホスト名、IP アドレス、MAC アドレスのうち、この順序で使用可能なもの）、クライアント、クライアントの正常性、アプリケーションの正常性、使用状況、デバイスタイプ、MAC アドレス、VLAN ID などの情報が含まれます。

アクティブクライアントについては、[Identifier] 列をクリックして [Client 360] ウィンドウを開くことができます。

このテーブルには、クライアントが最大 100 個まで表示されます。追加のクライアントを表示するには、[Show More] をクリックします。

ステップ 13 （任意） テーブルに表示するデータをカスタマイズします。

-  をクリックします。
オプションのリストが表示されます。

- b) テーブルに表示するデータのチェックボックスをオンにします。
- c) [Apply] をクリックします。

ステップ 14 (任意) テーブルデータを CSV ファイルにエクスポートするには、[Export] をクリックします。

(注) テーブルの列が選択されていない場合、使用可能なすべての列のデータがエクスポートの対象になります。アプリケーションテーブルに適用されているフィルタは、エクスポート対象のデータに適用されます。

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。

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

[Overall health] ダッシュボードが表示されます。

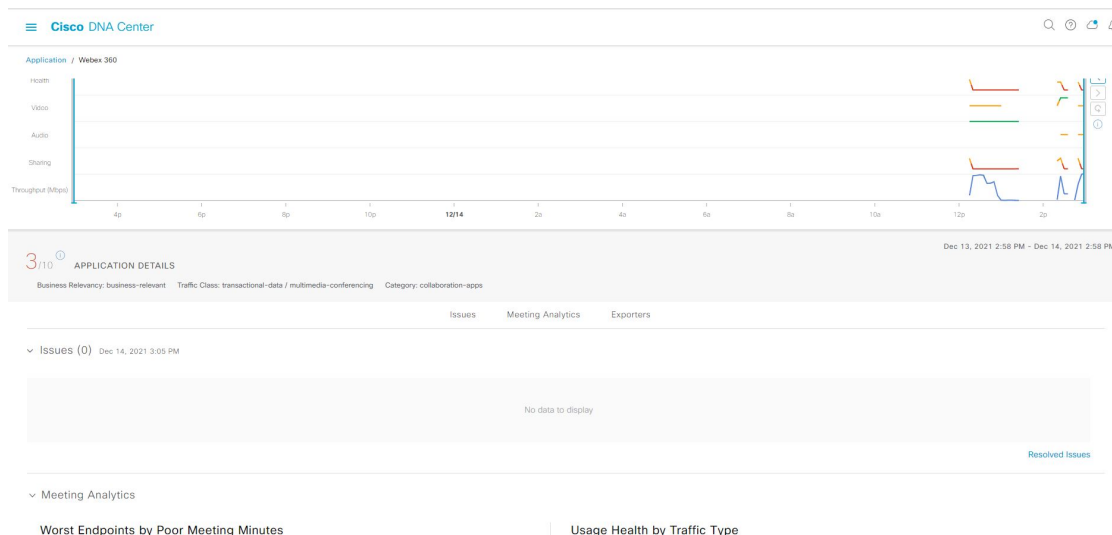
ステップ 2 [Application] タブをクリックします。

[Application Health] ダッシュボードが表示されます。

ステップ 3 [Application] テーブルで、[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 14: Webex 360



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。

- 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。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [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。「ステップ 9」を参照してください。
[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。手順 10 を参照してください。
[Exporters] タブ	クリックすると、NetFlow トラフィックを Cisco DNA Center に送信するデバイスのリストとその他の詳細情報が表示されます。ステップ 11 を参照してください。

ステップ 9 [Issue] カテゴリの問題に関する情報を確認できます。

- 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。
- スライドインペインでは、次の操作を実行できます。
 - この問題を解決するには、次の手順を実行します。
 - [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. スライダー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 \(231 ページ\)](#) 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。

<p>不良な会議時間の比較による下位エンドポイント</p> <p>[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。</p>
<p>トラフィックタイプ別の使用状況正常性</p> <p>[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。</p> <p>[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。</p> <p>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。</p>

ステップ 11 [Exporters] をクリックして、次の情報を確認します。

エクスポータ	
アイテム	説明
[Device]	<p>NetFlow トラフィックを Cisco DNA Center に送信しているデバイス (ルータ、スイッチ、ワイヤレスコントローラ、アライアンスなど) のリストが表示されます。</p> <p>(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。</p> <p>「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.)」</p>

エクスポート	
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 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、次の手順を実行します。

メトリック グラフ	
チャート	説明
[Usage]	特定のアプリケーションに対してクライアントが転送したバイト数。
[Throughput]	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。 <ul style="list-style-type: none"> • 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。

メトリック グラフ	
チャート	説明
[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。

アプリケーションの正常性スコア設定の設定

アプリケーションの正常性スコアを設定するには、次の手順を実行します。トラフィッククラスごとに KPI のしきい値を変更し、計算に含める KPI を指定すると、アプリケーションの正常性スコアの計算をカスタマイズできます。

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

ステップ 2 [Application Health] タブをクリックします。

ステップ 3 アプリケーションカテゴリのタブをクリックして、正常性スコアの計算設定をカスタマイズします。

このタブには、アプリケーションの正常性スコアの計算に影響する KPI が表示されます。

ステップ 4 [KPI Name] 列で、KPI 名のリンクをクリックします。

KPI のスライドインペインが表示されます。

ステップ 5 KPI の正常性スコアを次のように設定します。

- [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。
- [Weight] : 有効な重みは 1 - 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）= $90 \text{（正常性スコアが 8～10 のビジネス関連アプリケーション数）} \div 100 \text{（ビジネス関連アプリケーションの総数）}$

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 = $(\text{Latency_Weight} * \text{Latency_VoS_Score} + \text{Jitter_Weight} * \text{Jitter_VoS_Score} + \text{PacketLoss_Weight} * \text{PacketLoss_VoS_Score}) \div (\text{Latency_Weight} + \text{Jitter_Weight} + \text{PacketLoss_Weight})$



- (注) 正常性スコアは、Cisco Catalyst 9000 シリーズ スイッチおよび Cisco AireOS ワイヤレスコントローラについては提供されません。これらのデバイスは、正常性スコアの計算に必要な KPI をポーリングしません。

個別アプリケーションの正常性スコアを計算するためのワークフローは次のとおりです。

1. KPI（ジッター、遅延、パケット損失）を取得します。
2. フローレコードの DSCP 値に基づいて、アプリケーションのトラフィッククラスを決定します。

3. 各トラフィッククラスと KPI メトリックの Cisco Validated Design (CVD) しきい値を使用して、KPI 番号をサービススコア検証 (VoS スコア) に変換します。
4. アプリケーションのトラフィッククラスと許容度レベルに基づいて、KPI の重み付けを行います。重み付けは RFC4594 に基づきます。
5. アプリケーションの正常性スコアを計算します。これは、パケット損失、ネットワーク遅延、およびジッターの加重平均です。



第 9 章

ネットワークサービスの監視

- [AAA ネットワークサービスの監視 \(197 ページ\)](#)
- [DHCP ネットワークサービスの監視 \(200 ページ\)](#)

AAA ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラによって報告されたすべての AAA サーバートランザクションを表示および監視します。



(注) AAA 制約事項

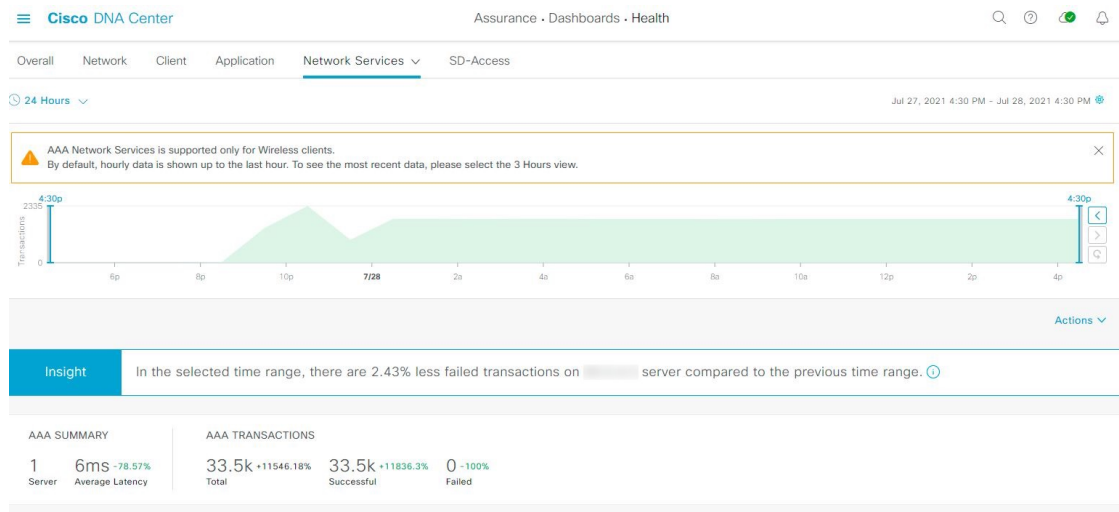
- AAA ネットワークサービスは、ワイヤレスクライアントおよびローカルモードをサポートします。
- AAA ネットワークサービスは、次をサポートしていません。
 - AireOS ワイヤレスコントローラ
 - フレックスモードまたはファブリックモード

始める前に

バージョン 17.6.1 以降の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラがインストールされており、ローカルモード AP で展開されていることを確認します。

- ステップ 1** メニューアイコン (☰) をクリックして、**[Assurance] > [Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。
- ステップ 2** **[Network Services] > [AAA]**を選択します。
[AAA] ダッシュボードが表示されます。

図 15: [AAA] ダッシュボード



- ステップ 3** 左上隅にある時間範囲設定 (🕒) をクリックして、表示するデータの時間範囲を指定します。
- 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。
 - [Start Date] と時刻、[End Date] と時刻を指定します。
 - [Apply] をクリックします。
- ステップ 4** 右上隅にある自動更新設定 (⚙️) をクリックして、サポートされている アシユアランス ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。
- ステップ 5** タイムラインスライダを使用して、一定期間における AAA サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには、次の機能があります。
- タイムラインスライダにカーソルを合わせると、5 分の時間枠の AAA サーバートランザクションが表示されます。
 - タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。
- ステップ 6** タイムラインスライダの下にある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。
- [EditDashboard] : 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 \(340 ページ\)](#) および [カスタム ダッシュボードの作成 \(335 ページ\)](#) を参照してください。
- ステップ 7** タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した AAA サーバートランザクションの割合を表示します。
- ステップ 8** AAA の概要ダッシュレットを使用して、次の情報を確認できます。

AAA の概要	
アイテム	説明
AAA の概要	ネットワークの AAA サーバーの数と平均遅延（ミリ秒単位）を表示します。
AAA トランザクション	ネットワーク内の AAA トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合を表示します。

ステップ 9 次の機能には、AAA サーバーダッシュレットを使用します。

最も大きい遅延が発生した上位サイト
<p>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。</p> <p>[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントにカーソルを合わせると、AAA サーバーの遅延が最も大きいサイトを表示できます。</p> <p>水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。</p>
トランザクションエラーが発生した上位サイト
<p>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。</p> <p>[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントまたはそれに対応する凡例にカーソルを合わせると、AAA サーバーのトランザクションエラーが最も多いサイトを表示できます。</p> <p>水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。</p>
AAA サーバーの遅延
<p>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。</p> <p>[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、AAA サーバーの遅延を表示できます。</p> <p>水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。</p>

AAA サーバートランザクション



このチャートには、ワイヤレスコントローラによって報告された各 AAA サーバーの平均 AAA サーバートランザクションステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、AAA サーバーのトランザクションを表示できます。

水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

ステップ 10 次の機能には、WLC による AAA サーバーダッシュレットを使用します。

WLC による AAA サーバーダッシュレット

アイテム	説明
AAA サーバーテーブル	AAA サーバーの IP、WLC 名、WLC の場所、トランザクション、障害、平均遅延などを含むテーブル形式で AAA サーバー情報を表示します。 [AAA Server IP] をクリックしてスライドインペインを開き、AAA サーバーの平均遅延およびトランザクションチャートを表示します。 水平バーとして表示されるデータを選択して、上位の AAA サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。
 Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 1. [Table Appearance] タブで、テーブルの密度とストライピングを設定します。 2. [Edit Table Columns] タブで、テーブルに表示するデータのチェックボックスをオンにします 3. [Apply] をクリックします。

DHCP ネットワークサービスの監視

この手順を使用して、ネットワーク内のワイヤレスコントローラによって報告されたすべての DHCP サーバートランザクションを表示および監視します。

**(注) DHCP の制限事項**

- DHCP ネットワークサービスは、ワイヤレスクライアントおよびローカルモードをサポートします。
- DHCP ネットワークサービスは、以下をサポートしていません。
 - SD-Access ファブリッククライアント
 - AireOS ワイヤレスコントローラ
 - フレックスモードまたはファブリックモード

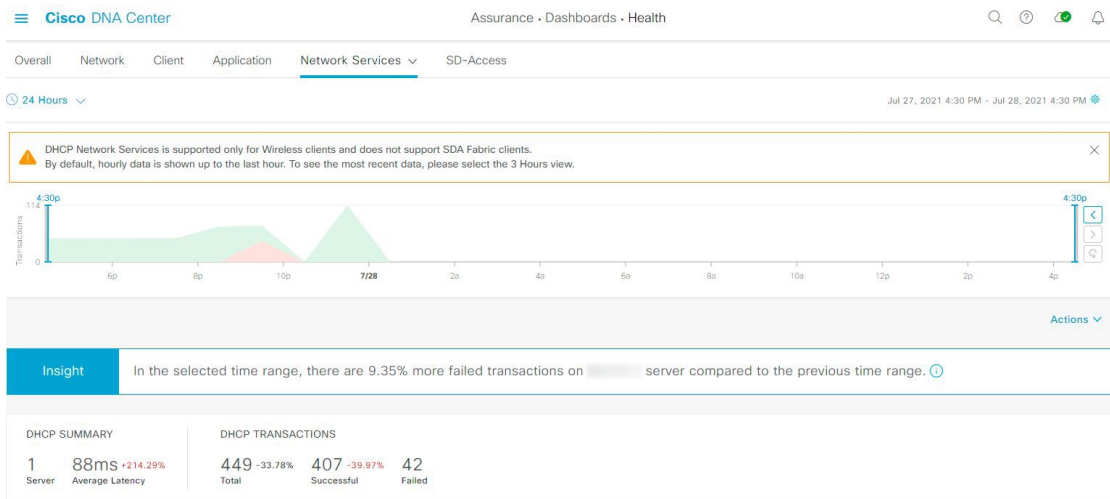
始める前に

バージョン 17.6.1 以降の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラがインストールされていることを確認します。

ステップ 1 メニューアイコン (☰) をクリックして、**[Assurance] > [Health]**の順に選択します。
[Overall] 正常性ダッシュボードが表示されます。

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

図 16: [DHCP] ダッシュボード



ステップ 3 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

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

c) [Apply] をクリックします。

ステップ 4 右上隅にある自動更新設定 (⚙️) をクリックして、サポートされている アシユアランス ページで [Data Auto Refresh] を 5 分の更新間隔で有効または無効にします。

ステップ 5 タイムラインスライダを使用して、一定期間における DHCP サーバーの成功および失敗したトランザクションの合計に関する情報を表示します。タイムラインスライダには、次の機能があります。

- タイムラインスライダにカーソルを合わせると、5 分の時間枠の DHCP サーバートランザクションが表示されます。
- タイムラインをダブルクリックすると、1 時間の期間タイムラインスライダが表示されます。ウィンドウ全体が更新され、該当する 1 時間の最新情報が表示されます。

ステップ 6 タイムラインスライダの下にある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- [EditDashboard] : 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 \(340 ページ\)](#) および [カスタム ダッシュボードの作成 \(335 ページ\)](#) を参照してください。

ステップ 7 タイムラインの下にある [Insight] エリアを使用して、現在および以前の時間範囲と比較して、成功した DHCP サーバートランザクションの割合を表示します。

ステップ 8 DHCP の概要ダッシュレットを使用して、次の情報を確認できます。

DHCP の概要	
アイテム	説明
DHCP Summary	ネットワークの DHCP サーバーの数と平均遅延 (ミリ秒単位) が表示されます。
DHCP Transactions	ネットワーク内の DHCP トランザクション、成功したトランザクション、および失敗したトランザクションの合計数の割合が表示されます。

ステップ 9 次の機能には、DHCP サーバーダッシュレットを使用します。

最も大きい遅延が発生した上位サイト
<p>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。</p> <p>[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。</p> <p>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。</p>

トランザクションエラーが発生した上位サイト

チャートには、DHCP サーバーのトランザクションエラーが最も多い上位サイトが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、チャートの色のセグメントまたはそれに対応する凡例にカーソルを合わせると、DHCP サーバーのトランザクションエラーが最も多いサイトを表示できます。

水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、および AP に基づいてクライアントテーブルをフィルタ処理できます。

DHCP サーバーの遅延

このチャートには、各 DHCP サーバーにおける DHCP 平均遅延が表示されます。[All]、[Discover-offer]、または [Request-Ack] に基づいて遅延をフィルタ処理できます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、DHCP サーバーの遅延を表示できます。

水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

DHCP サーバートランザクション

このチャートには、ワイヤレスコントローラによって報告された各 DHCP サーバーの平均 DHCP サーバートランザクションステータスが表示されます。[All]、[Failures]、または [Successes] に基づいてステータスをフィルタ処理できます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインから、フィルタの選択に基づいてチャートを表示して、DHCP サーバーのトランザクションを表示できます。

水平バーとして表示されるデータを選択して、上位の DHCP サーバー、サイト、SSID、AP などに基づいてクライアントテーブルをフィルタ処理できます。

ステップ 10 次の機能には、WLC による DHCP サーバーダッシュレットを使用します。

WLC による DHCP サーバーダッシュレット	
アイテム	説明
DHCP サーバーテーブル	<p>DHCP サーバーの IP、WLC 名、WLC の場所、トランザクション、障害、平均遅延などを含むテーブル形式で DHCP サーバー情報を表示します。[DHCP Server IP] をクリックしてスライドインペインを開き、サーバーの平均遅延およびトランザクションチャートを表示します。</p> <p>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。</p>

WLC による DHCP サーバーダッシュレット	
アイテム	説明
 Export	デバイス情報を CSV ファイルにエクスポートするには、[Export] をクリックします。
	テーブルに表示するデータをカスタマイズします。 <ol style="list-style-type: none">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 \(205 ページ\)](#)
- [SD-Access ファブリックの正常性の監視とトラブルシューティング \(209 ページ\)](#)
- [ファブリックサイトの正常性の監視 \(216 ページ\)](#)
- [トランジットおよびピアネットワークの正常性の監視 \(220 ページ\)](#)
- [仮想ネットワークの正常性の監視 \(225 ページ\)](#)
- [仮想ネットワークの正常性スコア \(229 ページ\)](#)

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。

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

ファブリックサイトの追加

始める前に

IP デバイストラッキング (IPDT) がすでにサイトに設定されている場合にのみ、ファブリックサイトを作成できます。

ステップ 1 メニューアイコン (☰) をクリックして、**[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** [Create Fabric Sites and Fabric Zones] 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、[Workflow]>[Create Fabric Sites]の順に選択します。
- ステップ 4** [Create Fabric Sites and Fabric Zones] 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、ファブリックゾーン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、[Monitor wired clients] 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** [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。
 - [Closed Authentication] : 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。
 - [Open Authentication] : 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。
 - [Low Impact] : 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。
 - [None]
 - 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。
 - [First Authentication Method] : [802.1x] または [MAC Authentication Bypass (MAB)] を選択します
 - [802.1x Timeout (in seconds)] : スライダーを使用して、802.1x タイムアウトを秒単位で指定します。
 - [Wake on LAN] : [Yes] または [No] を選択します。
 - [Number of Hosts] : [Unlimited] または [Single] を選択します。
 - [BPDU Guard] : 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。
 - [Pre-Authentication Access Control List] : トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[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ます。ルールの説明を入力します。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 8** [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。

- ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックし、表示されたネットワーク階層からファブリックサイトを選択します。
- 後でファブリックゾーンを指定するには、[Setup Fabric Zones Later] をクリックします。

ステップ 9 [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 10 [Deploy] をクリックします。

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

ファブリックへのデバイスの追加

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

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

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



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

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

- [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グレー色で表示されます。
- ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
- 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで[Inventory] > [Resync] を実行して、デバイス情報を再同期してください。



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

ステップ 1 メニューアイコン (☰) をクリックして、[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は、次の [Fabric] オプションが表示されます。

オプション	説明
エッジノード	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 [Add] をクリックします。

次のタスク

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

SD-Access ファブリックの正常性の監視とトラブルシューティング

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

始める前に

アシュアランスを設定します。「[基本的な設定のワークフロー \(15 ページ\)](#)」を参照してください。

ファブリックサイトを監視およびトラブルシューティングするには、最初にファブリックサイトを構成する必要があります。[ファブリックサイトの追加 \(205 ページ\)](#) および [ファブリックへのデバイスの追加 \(207 ページ\)](#) を参照してください。

マルチサイト ファブリック サイトの詳細情報については、[Cisco Digital Network Architecture Center ユーザー ガイド](#)の「Provision Your Network」の章を参照してください。



- (注) サブテンドノードと拡張ノードは、ファブリックの正常性の対象にはなりません。ファブリックのプロビジョニング中、これらのノードには、エッジ、ボーダー、コントロールプレーンなどのファブリックロールが割り当てられません。

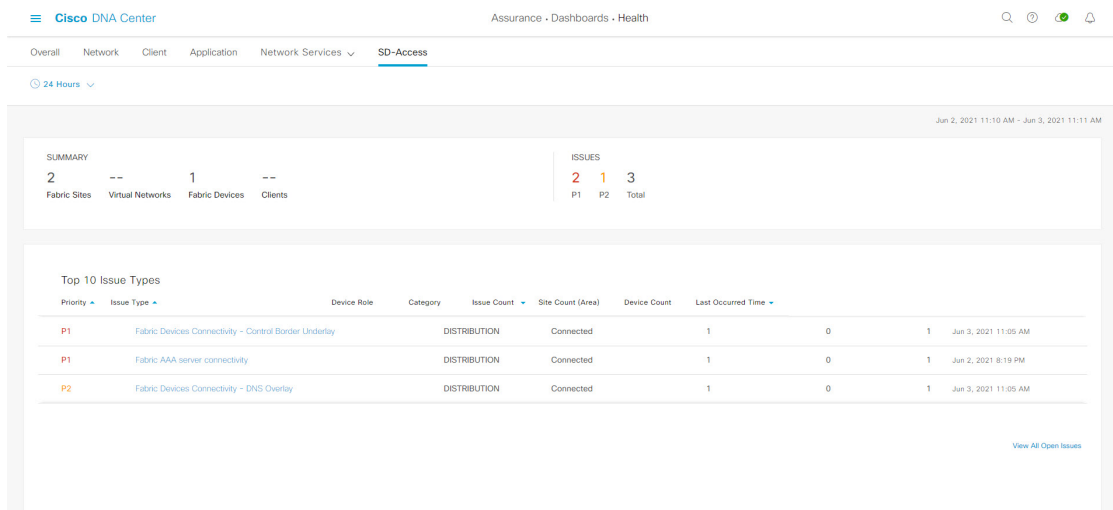
ステップ 1 [Health]メニューアイコン (☰) をクリックして、**アシュアランス** >。

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

図 17: [Network Health] ダッシュボード



ステップ 3 上部のメニューバーにある時間範囲設定 (🕒) をクリックして、ダッシュボードに表示するデータの時間範囲を指定します。

- 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。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [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]	<ul style="list-style-type: none"> [Fabric Sites] : ファブリックサイトの数。 [Virtual Networks] : 仮想ネットワークの数。 [Fabric Endpoints] : ファブリックエンドポイントの数。 [Endpoints] : エンドポイントの数。 [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。
問題	<ul style="list-style-type: none"> [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のインスタンスをクリックします。必要に応じて、次の操作を実行できます。


- 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。
- 問題のインスタンスを無視するには、次の手順を実行します。
 1. [Status] ドロップダウンリストから、[Ignore] を選択します。
 2. スライダで問題を無視する時間数を設定します。
 3. [Confirm] をクリックします。

[View All Issues] をクリックすると、[Open Issues] ウィンドウが開きます。


ステップ 6 [Fabric Sites] ダッシュレットを使用して、ネットワーク内のファブリックサイトに関する詳細情報を表示します。このダッシュレットには、次の機能があります。

[Fabric Sites] ダッシュレット

アイテム	説明
[Health]	<p>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。</p> <ul style="list-style-type: none"> • すべて • [Inactive] : 正常性スコアが 0 のファブリックサイト。 • [Poor] : 正常性スコアが 1 ~ 3 のファブリックサイト。 • [Fair] : 正常性スコアが 4 ~ 7 のファブリックサイト。 • [Good] : 正常性スコアが 8 ~ 10 のファブリックサイト。 • [No Data] : データのないファブリックサイト。

[Fabric Sites] ダッシュレット	
アイテム	説明
[Fabric Site] テーブル	<p>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。</p> <ul style="list-style-type: none"> • [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 (216 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] : <ul style="list-style-type: none"> • [Overall] : ファブリックサイトの全体的な正常性。 • [Fabric Site 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]	<p>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。</p> <p>(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。</p>
	<p>テーブルの表示をカスタマイズします。</p> <ol style="list-style-type: none"> 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には、次の機能があります。


[Virtual Networks] ダッシュレット	
アイテム	説明
[Health]	<p>次のオプションを使用して、仮想ネットワークの正常性を基にテーブルをフィルタ処理します。</p> <ul style="list-style-type: none"> • [All] • [Inactive]: ヘルス スコアが 0 の仮想ネットワーク。 • [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	<p>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。</p> <ul style="list-style-type: none"> • [VN Name]: 仮想ネットワークの名前。 <p>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 (225 ページ) を参照してください。</p> <ul style="list-style-type: none"> • [# 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]: <ul style="list-style-type: none"> • [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]	<p>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。</p> <p>(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。</p>
	<p>テーブルの表示をカスタマイズします。</p> <ol style="list-style-type: none"> 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には、次の機能があります。

表 19 : [Transits and Peer Networks]

アイテム	説明
[Health]	<p>次のオプションを使用して、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を基にテーブルをフィルタ処理します。</p> <ul style="list-style-type: none"> • [All] • [Inactive] : 正常性スコアが0のトランジットネットワークおよびピアネットワーク。 • [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。

アイテム	説明
[Transits and Peer Networks] テーブル	<p>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、[Transits and Peer Networks] テーブルには次の情報が表示されます。</p> <ul style="list-style-type: none"> • [Transit/ Peer Network 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 (225 ページ) を参照してください。 • [Type] : 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。 • [Associated Fabric Sites] • [Transit and Peer Networks Health] : <ul style="list-style-type: none"> • [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。
[Export]	<p>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。</p> <p>(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。</p>

アイテム	説明
	<p>テーブルの表示をカスタマイズします。</p> <ol style="list-style-type: none"> [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。 [Edit Table Columns] タブで、テーブルに表示するデータを選択します。 [Apply] をクリックします。

ファブリックサイトの正常性の監視

この手順を使用して、特定のファブリックサイトの詳細を表示します。

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

[Overall health] ダッシュボードが表示されます。

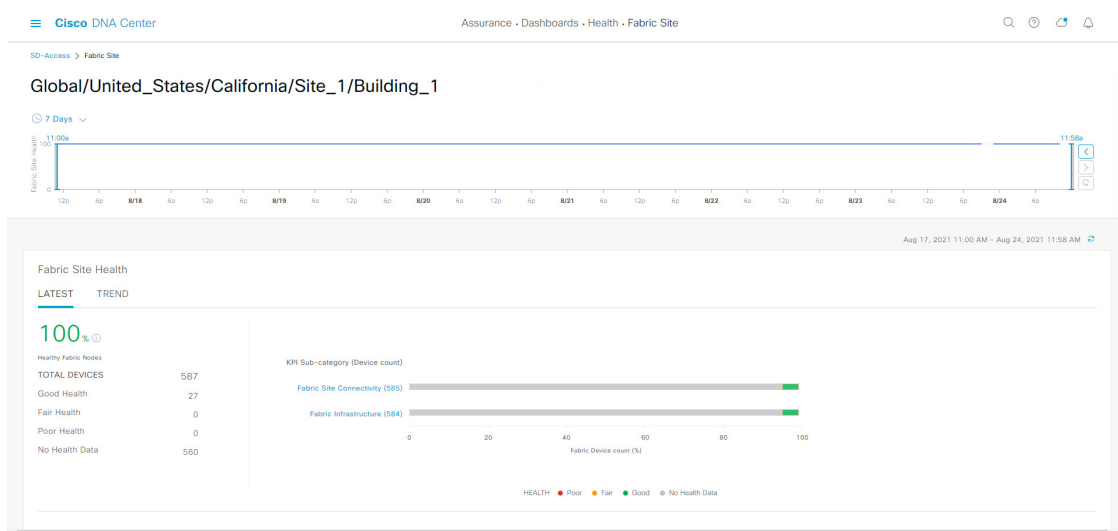
ステップ 2 [SD-Access] タブをクリックします。

[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 360] ウィンドウが表示されます。

図 18: Fabric Site 360



ステップ 4 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

- a) ドロップダウンリストから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。
- b) [開始日付 (Start Date)]と時刻、[終了日付 (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。

[Fabric Site Health] : 正常性は、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスヘルスには含まれません。ファブリックサブカテゴリの正常性は、基礎となる KPI スコアの最小値です。

(注) KPI は正常性スコアに含まれません

[Fabric Site Connectivity] : コントロールプレーンに到達できません。

[Fabric Infrastructure] :

時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。この境界により、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。




ファブリックサイトの正常性	
アイテム	説明
Latest	<p>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。</p> <ul style="list-style-type: none"> • [Health Fabric Nodes] : 選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices] : ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts] : この色分けされたスナップショット ビュー チャートは、過去 5 分間のファブリックサイトの接続とインフラストラクチャを示します。 <p>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。</p> <p>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です。</p> <p>グラフ内のハイパーリンクされたファブリックカテゴリをクリックしてサイドペインを開き、それぞれの KPI サブカテゴリを表示することもできます。</p> <ul style="list-style-type: none"> • [Fabric Site Connectivity] : コントロールプレーンの到達可能性。 • [Fabric Control Plane] : LISP セッションステータス。 • [Fabric Infrastructure] : INFRA VN の AAA サーバーステータスと Pub-Sub セッションステータス。
Trend	<p>[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。</p> <p>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。</p> <ul style="list-style-type: none"> ● : 不良なネットワークデバイス。ヘルススコアの範囲は 1～3 です。 ● : 中程度のネットワークデバイス。ヘルススコアの範囲は 4～7 です。 ● : 良好なネットワークデバイス。ヘルススコアの範囲は 8～10 です。 ● : 正常性データなし。ヘルススコアは 0 です。

ステップ 7 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題
<p>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。</p> <p>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。</p> <p>スライドインペインでは、次の操作を実行できます。</p> <ul style="list-style-type: none"> • この問題を解決するには、次の手順を実行します。 <ol style="list-style-type: none"> 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。 <ol style="list-style-type: none"> 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。 <p>問題のタイプの詳細については、問題の表示と管理 (231 ページ) を参照してください。</p>

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

[Networks Devices] ダッシュレット	
アイテム	説明
[Type]	オプション ([All]、[Fabric Control Plane]、[Fabric Border]、[Fabric Edge]、[Fabric WLC]、[Fabric AP]、[Extended Node]) を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
ファブリックサイトの正常性	次のオプションを使用して、ファブリックサイトの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 <ul style="list-style-type: none"> • [All] • [Poor] : 正常性スコアが 1 ~ 3 のデバイス。 • [Fair] : 正常性スコアが 4 ~ 7 のデバイス。 • [Good] : 正常性スコアが 8 ~ 10 のデバイス。 • [No Health] : 正常性データのないデバイス。

[Networks Devices] ダッシュレット	
アイテム	説明
ファブリックノードテーブル	<p>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。</p> <p>(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。</p> <p>[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。</p> <p>[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。</p> <p>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。</p>
[Device 360]	<p>[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。</p> <p>[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。</p>
 Export	<p>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。</p>
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none">  をクリックします。 オプションのリストが表示されます。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。

トランジットおよびピアネットワークの正常性の監視

この手順を使用して、特定のトランジットネットワークの詳細を表示します。

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

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

[SD-Access health] ダッシュボードが表示されます。

ステップ 3 [Transit and Peer Network] テーブルで、トランジットの名前をクリックします。

ファブリックサイトの 360° ビューを提供する [Transit Site 360] ウィンドウが表示されます。

図 19: トランジット 360



ステップ 4 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

- ドロップダウンリストから、時間範囲として [3 hours]、[24 hours]、または [7 days] を選択します。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [Apply] をクリックします。

ステップ 5 正常性タイムラインスライダを使用して、より詳細な時間範囲の正常性スコアや品質情報を確認します。タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Transit Network Health] : 正常性は、このサイトの正常なファブリックノードの割合です。コントロールプレーンのデバイスの正常性は含まれません。ファブリックサブカテゴリの正常性は、基礎となる KPI スコアの最小値です。

[Transit Site Control Plane] : トランジットの LISP セッションや PubSub セッションなどの KPI サブカテゴリを一覧表示します。トランジット正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

- [Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。
- [Latest] : ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。
- [Trend] : 過去 24 時間のデータが表示されます。

ステップ 6 タイムラインの下にある [Transit Health] エリアで、次の情報を確認します。




トランジットの正常性	
アイテム	説明
Latest	<p>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。</p> <ul style="list-style-type: none"> • [Health Fabric Nodes] : 選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices] : ネットワークデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts] : この色分けされたスナップショット ビュー チャートは、過去 5 分間のトランジット コントロール プレーンを示します。 <p>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。</p> <p>チャート内のハイパーリンクされた [Transit Control Plane] をクリックしてサイドペインを開き、トランジットコントロールプレーンの次の KPI サブカテゴリを表示することもできます。</p> <ul style="list-style-type: none"> • [LISP session from Border to Transit Control Plane] • [PubSub session from Border to Transit Control Plane] <p>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。</p>
Trend	<p>[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。</p> <p>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。</p> <ul style="list-style-type: none"> ● : 不良なネットワークデバイス。ヘルススコアの範囲は 1～3 です。 ● : 中程度のネットワークデバイス。ヘルススコアの範囲は 4～7 です。 ● : 良好なネットワークデバイス。ヘルススコアの範囲は 8～10 です。 ● : 正常性データなし。ヘルススコアは 0 です。

ステップ 7 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題
<p>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。</p> <p>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。</p> <p>スライドインペインでは、次の操作を実行できます。</p> <ul style="list-style-type: none"> • この問題を解決するには、次の手順を実行します。 <ol style="list-style-type: none"> 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。 <ol style="list-style-type: none"> 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。 <p>問題のタイプの詳細については、問題の表示と管理 (231 ページ) を参照してください。</p>




ステップ 8 次の機能には、[Associated Fabric Sites] ダッシュレットを使用します。

[Associated Fabric Sites] ダッシュレット	
アイテム	説明
[Health]	<p>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。</p> <ul style="list-style-type: none"> • [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	<p>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]。</p>

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

ステップ 9 次の機能には、[Fabric Nodes] ダッシュレットを使用します。

[Fabric Nodes] ダッシュレット	
アイテム	説明
[Type]	オプション ([All]、[Transit Control Plane]、[Border]) を使用して、ファブリックノードタイプに基づいてテーブルをフィルタ処理します。
[Transit and Peer Network Health]	次のオプションを使用して、トランジットの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 <ul style="list-style-type: none"> • [All] • [Poor] : 正常性スコアが 1 ~ 3 のデバイス。 • [Fair] : 正常性スコアが 4 ~ 7 のデバイス。 • [Good] : 正常性スコアが 8 ~ 10 のデバイス。 • [No Health] : 正常性データのないデバイス。

[Fabric Nodes] ダッシュレット	
アイテム	説明
ファブリックノードテーブル	<p>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。</p> <p>(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。</p> <p>[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。</p> <p>[Device Transit Health] の [Overall] 列で、正常性スコアの上にマウスカーソルを合わせます。全体の [Device Transit Health] スコアが、すべての KPI メトリックの正常性とパーセンテージとともに表示されます。</p> <p>[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。</p>
[Device 360]	<p>[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。</p> <p>[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。</p>
 Export	<p>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。</p>
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none">  をクリックします。 オプションのリストが表示されます。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。

仮想ネットワークの正常性の監視

この手順を使用して、特定の仮想ネットワークの詳細を表示します。

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

[Overall health] ダッシュボードが表示されます。

ステップ 2 [SD-Access] タブをクリックします。

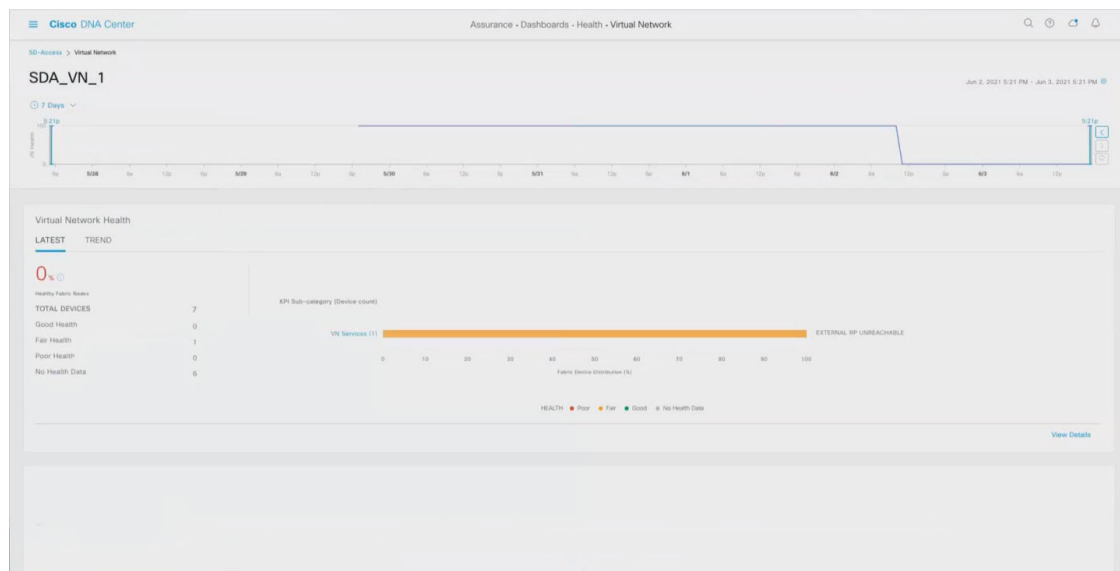
[SD-Access health] ダッシュボードが表示されます。

ステップ 3 下にスクロールし、[Virtual Network] をクリックします。

ステップ 4 [Virtual Network] テーブルで、仮想ネットワークの名前をクリックします。

仮想ネットワークの 360 度ビューを提供する [Virtual Network 360] ウィンドウが表示されます。

図 20: Virtual Network 360



ステップ 5 左上隅にある時間範囲設定 (🕒) をクリックして、ウィンドウに表示するデータの時間範囲を指定します。

- 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。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [Apply] をクリックします。

ステップ 6 仮想ネットワークの正常性タイムラインスライダを使用して、より詳細な時間範囲の仮想ネットワークの正常性スコアや仮想ネットワークの品質情報を確認します。

タイムライン内でカーソルを合わせると、次の情報が表示されます。

[Virtual Network Health]: 正常性スコアは、正常なマルチキャスト VN サービスと VN コントロールプレーンの割合です。

VN 正常性スコアが低い場合は、[View Device List] をクリックして、低いスコアの原因となっているデバイスおよび関連するダウンセッションのリストを表示します。ハイパーリンクされたデバイスの名前をクリックすると、デバイス情報が表示されます。

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	<p>デフォルトで表示されます。2つのペインがあります。左側のペインには、仮想ネットワークの正常性の概要スコアとデバイスの合計数が表示されます。右側のペインには、チャートが表示されます。</p> <ul style="list-style-type: none"> • [Healthy Fabric Nodes] : 選択したサイトの正常な（良好な）ノードの割合。 • [Total Devices] : ファブリックデバイスの総数と、[Good Health]、[Fair Health]、[Poor Health]、および [No Health Data] のデバイスの数。 • [Charts] : この色分けされたスナップショット ビュー チャートには、[VN Control Plane] (Pub-Sub セッションステータス) や [VN Services] (マルチキャスト外部 RP) などの KPI サブカテゴリが表示されます。 <p>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。</p> <p>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。</p> <p>ハイパーリンクされたカテゴリをクリックして、詳細を示すサイドペインを開くこともできます。</p>
Trend	<p>[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。</p> <p>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。</p> <ul style="list-style-type: none"> ● : 不良なネットワークデバイス。ヘルス スコアの範囲は 1～3 です。 ● : 中程度のネットワークデバイス。ヘルス スコアの範囲は 4～7 です。 ● : 良好なネットワークデバイス。ヘルス スコアの範囲は 8～10 です。 ● : 正常性データなし。ヘルス スコアは 0 です。

ステップ 8 [Top 10 Issue Types] エリアを使用して、次の情報を表示します。

問題

対処する必要がある問題を表示します。問題は、タイムスタンプに基づいて一覧表示されます。直近の問題が最初にリストされます。

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




スライドインペインでは、次の操作を実行できます。

- この問題を解決するには、次の手順を実行します。
 1. ドロップダウンリストから [Resolve] を選択します。
 2. 解決済みの問題の一覧を表示するには [Resolved Issues] をクリックします。
- 問題を無視するには、次の手順を実行します。
 1. ドロップダウンリストから [Ignore] を選択します。
 2. スライダー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 \(231 ページ\)](#) を参照してください。

ステップ 9 次の機能には、[Virtual Network Devices] ダッシュレットを使用します。

[Virtual Network Devices] ダッシュレット	
アイテム	説明
[Type]	タイプに基づいてテーブルをフィルタ処理します。
[Virtual Network Health]	次のオプションを使用して、仮想ネットワークの全体的な正常性スコアに基づいてテーブルをフィルタ処理します。 <ul style="list-style-type: none"> • [All] • [Poor] : 正常性スコアが 1 ~ 3 のデバイス。 • [Fair] : 正常性スコアが 4 ~ 7 のデバイス。 • [Good] : 正常性スコアが 8 ~ 10 のデバイス。 • [No Health] : 正常性データのないデバイス。

[Virtual Network Devices] ダッシュレット	
アイテム	説明
[Virtual Network Devices] テーブル	<p>選択した項目のデバイス情報が表形式で表示されます。</p> <p>(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。</p> <p>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。</p>
[Device 360]	<p>[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。</p> <p>[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。</p>
 Export	<p>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。</p>
	<p>テーブルに表示するデータをカスタマイズします。</p> <ol style="list-style-type: none">  をクリックします。 オプションのリストが表示されます。 テーブルに表示するデータのチェックボックスをオンにします。 [Apply] をクリックします。

仮想ネットワークの正常性スコア

現在、マルチキャスト VN サービスが、VN 正常性スコアに関する唯一の KPI です。

仮想ネットワークの正常性スコア



第 11 章

問題の表示と管理

- [問題について](#) (231 ページ)
- [機械推論エンジンについて](#) (232 ページ)
- [VLAN に関連するレイヤ 2 ループの問題について](#) (232 ページ)
- [未解決の問題を表示](#) (233 ページ)
- [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](#) (247 ページ)
- [解決済みの問題の表示](#) (250 ページ)
- [無視された問題の表示](#) (252 ページ)
- [問題の解決または無視](#) (254 ページ)
- [無線にアクティビティなしの問題のトリガー](#) (256 ページ)
- [自動問題解決](#) (256 ページ)
- [グローバルな問題の設定の管理](#) (257 ページ)
- [カスタム問題の設定の管理](#) (258 ページ)
- [問題の通知の有効化](#) (259 ページ)
- [アシュアランス、Cisco AI Network Analytics、および MRE の問題](#) (261 ページ)

問題について

アシュアランスシステムガイド付きとガイドなしの両方のトラブルシューティングを提供します。アシュアランスは多くの問題に対してシステムガイド付きアプローチを提供します。このアプローチでは、複数の重要業績評価指標 (KPI) が関連付けられています。また、テストやセンサーからの結果に基づき問題の根本原因が特定された後に、考えられる解決策が提供されます。データの監視ではなく、問題点を浮き彫りにすることに重点が置かれています。アシュアランスでは、非常に頻繁にレベル 3 サポートエンジニアの作業が実行されます。

Cisco DNA Center では、Cisco AI Network Analytics を使用して AI 駆動型の問題を表示およびトラブルシューティングできます。Cisco AI Network Analytics は、高度な人工知能 (AI) や機械学習 (ML) テクノロジーを基盤としたクラウドベースの学習プラットフォームを活用して、問題のインテリジェントな検出と分析を実現します。異常を検知すると、根本原因を特定してトラブルシューティングを容易にします。

Cisco AI Network Analytics 次のタイプのクラウドベースの AI 駆動型の問題を検出できます。

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



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

機械推論エンジンについて

機械推論エンジン (MRE) は、ネットワーク自動化エンジンであり、人工知能 (AI) を使用して複雑なネットワーク運用ワークフローを自動化します。完全に自動化された推論エンジンに人間の知識と専門知識をカプセル化し、複雑な根本原因の分析、問題や脆弱性の検出、および手動または自動による是正処置の実行を支援します。MRE は、シスコのネットワークキング 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特できます。問題のリストについては、[MRE の問題 \(279 ページ\)](#) 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特 \(247 ページ\)](#)、[レイヤ 2 のループ問題に関与するインスタンスの詳細 \(241 ページ\)](#)、[PoE の問題に関する問題インスタンスの詳細 \(244 ページ\)](#) 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関する制約事項は、次のとおりです。

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



重要 現在、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 Cisco DNA 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。

未解決の問題を表示

次のカテゴリに分類される未解決の問題をすべて表示するには、次の手順を実行します。

- **しきい値ベースの問題**：アシュアランスによって検出された問題。
- **駆動型の問題**：Cisco AI Network Analytics によって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

Cisco DNA Center で Cisco AI Network Analytics アプリケーションをインストールおよび設定している場合は、次のタイプのクラウドベース AI 駆動型に関する問題を確認できます。

- **接続の問題**（オンボーディングの問題）：過剰な時間、過剰な障害回数、過剰な関連付け時間、過剰な関連付け障害回数、過剰な認証時間、過剰な認証障害回数、過剰な DHCP 時間、過剰な DHCP 障害回数。



(注) 接続の問題が表示されるようにするには、AP がサイトに適切に割り当てられていることを確認してください。

- **アプリケーションエクスペリエンスに関する問題**：無線スループットの合計、メディアアプリケーションのスループット、クラウドアプリケーションのスループット、コラボレーションアプリケーションのスループット、およびソーシャルアプリケーションのスループット。



(注) アプリケーションエクスペリエンスに関する問題を表示するには、ワイヤレスコントローラで **Application Visibility and Control (AVC)** が有効になっていることを確認してください。スループットの問題では、AVC データに基づいて基準化と異常検出を行います。

- **レイヤ2ループの問題と PoEの問題**：アシュアランスによって検出された、MRE ワークフローを使用してトラブルシューティングできる問題。[機械推論エンジンについて \(232 ページ\)](#) を参照してください。

始める前に

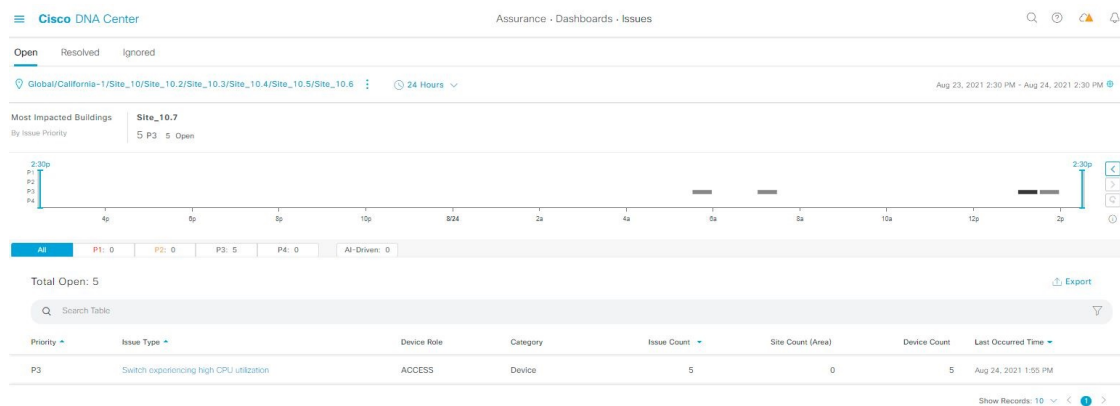
- 人工知能 (AI) および機械学習 (ML) テクノロジーを使用してインテリジェントな問題の検出と分析を行う AI 駆動型クラウドベースの問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認します。[Cisco AI Network Analytics データ収集の設定 \(87 ページ\)](#) を参照してください。
- syslog メッセージを表示するため、syslog が設定されていることを確認します。『Cisco Digital Network Architecture Center ユーザー ガイド』で「[テレメトリを使用した Syslog、SNMP トラップ、NetFlow コレクタサーバー、および有線クライアントデータ収集の設定 \(85 ページ\)](#)」を参照してください。









ステップ 1 次のいずれかを実行します。

- Cisco DNA Center ホームページの **アシュアランス [Summary]** > **[Critical Issues]** エリアで、**[View Details]** を選択します。
- メニューアイコン (☰) をクリックして、**[Assurance]** > **[Dashboards]** > **[Issues]** の順に選択します。

[Open Issues] ダッシュボードが表示され、次の情報が示されます。

図 21 : **[Open Issues]** ダッシュボード



[Open Issues] ダッシュボード	
アイテム	説明
 Global	<ul style="list-style-type: none"> 上部のメニューバーで  をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 ロケーションアイコンの横にある  をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 [Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Open Issues] ダッシュボードに表示されます。
 [Time Range] の設定	<p>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。</p> <ol style="list-style-type: none"> [24 時間 (24 Hours)] ドロップダウンリストで、時間範囲 ([3 時間 (3 hours)]、[24 時間 (24 Hours)]、または [7 日間 (7 days)]) を選択します。 [Start Date] と時刻、[End Date] と時刻を指定します。 [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
Most Impacted Areas	<p>問題のプライオリティに基づいて最も影響を受けるエリアに関する情報が表示されます。ハイパーリンクされたロケーションをクリックすると、問題が発生した建物とフロアにドリルダウンします。</p>
タイムラインスライダ	<p>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。</p> <p>色は、問題のプライオリティを表します。</p> <ul style="list-style-type: none">  : P1  : P2  : P3 および P4 <p>(注) 色の明度は重要性 (そのプライオリティ レベルで発生した問題数の多寡) を示します。たとえば、薄い黄色は、濃い黄色よりも (未解決の) P2 問題が少ないことを示します。</p>

[Open Issues] ダッシュボード	
アイテム	説明
Total Open	アクションを必要とする未解決の問題の合計数が表示されます。 [Total Open] の値は、選択したタブに応じて変わります。[All] (デフォルト)、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかを選択できます。

ステップ 2 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Open Issue] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル (事前割り当てされたもの)。
Issue Type	問題のタイプ。 (注) AI 駆動型の問題の場合、問題のタイプの前に AI アイコンが表示されます。
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ (接続、可用性、オンボード、使用状況など)。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 3 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題タイプに関するすべての問題が次の情報とともに一覧表示されます。

[Issue Instance] (最初のスライドインペイン)	
アイテム	説明
Open Issues	その問題タイプで未解決の問題の数。
Area	問題の影響を受けるビルディングとフロアの数。
[Device]	問題の影響を受けるデバイスの数。
[Actions] ドロップダウン リスト	個別に問題を解決または無視することも、一度に大量の問題を解決または無視することもできます。 問題の解決または無視 (254 ページ) を参照してください。

[Issue Instance] (最初のスライドインペイン)	
アイテム	説明
Issue	問題の説明。
Site	問題の影響を受けたサイト、ビルディング、またはフロア。
[Device]	問題の影響を受けたデバイス。デバイス名をクリックして、[Device 360] ウィンドウを開きます。
Device Type	問題の影響を受けたデバイスのタイプ。
Issue Count	この種類の問題が発生した回数。
Last Occurred Time	問題が発生した日付と時刻。
Last Updated Time	この問題の最終更新日時。
Updated By	この問題を更新したエンティティ名。

ステップ 4 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

(注) 推奨されるアクションには、その隣に [Run] ボタンが表示されます。[Run] をクリックすると、指定された CLI コマンドがデバイスで実行されます。

AI 駆動型の問題の場合、[Issue Instance Details] のスライドインペインに AI によって導出された固有の情報が表示されます。AI 駆動型の問題に関するインスタンスの詳細 (237 ページ) を参照してください。

機械推論をサポートするレイヤ 2 ループの問題については、[Issue Instance Details] スライドインペインに特定の情報が表示されます。レイヤ 2 のループ問題に関するインスタンスの詳細 (241 ページ) を参照してください。


機械推論をサポートする PoE の問題については、[Issue Instance Details] スライドインペインに特定の情報が表示されます。PoE の問題に関する問題インスタンスの詳細 (244 ページ) を参照してください。

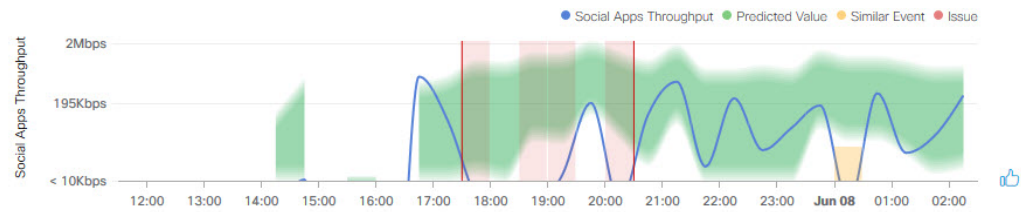
AI 駆動型の問題に関するインスタンスの詳細




(注) [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題を表示 (233 ページ)」のステップ 4 を参照してください。

AI 駆動型の問題が発生すると、[Issue Instance Details] (2 番目のスライドインペイン) に次の情報が表示されます。

[Issue Instance Details] (2 番目のスライドインペイン)	
アイテム	説明
Description	問題の説明。
[Status] ドロップダウンリスト	<p>問題のステータスを変更できます。次の手順を実行します。</p> <ul style="list-style-type: none"> 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 問題の報告を停止するには、次の手順を実行します。 <ol style="list-style-type: none"> [Status] ドロップダウンリストから、[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。
[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	<p>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。</p> <p>デフォルトでは、次の図に示すように、グラフは問題発生の前 6 時間にズームインされます。</p> <p>図 22: 問題のチャート</p>  <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>
Impact	<p>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。</p> <p>過剰なオンボーディング時間と失敗、過剰な DHCP、アソシエーション、または認証時間と失敗については、[Impacted Clients] タブと [Top 10 Impacted APs] タブが表示されます。</p> <p>合計無線スループットおよびアプリケーションスループット（クラウド、コラボレーション、メディアおよびソーシャル）については、[Impacted Clients] タブ、[Device Breakout] タブ、[Applications TX / RX] タブが表示されます。</p> <p>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。</p>

[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	<p>次の図に示すように、問題とその問題の原因として考えられるネットワーク関連の原因がチャートに表示されます。</p> <p>図 23: 根本原因の分析チャート</p> <p>過剰なオンボーディング時間と失敗については、[Network Causes] タブ、[Failed Distribution] タブ、[Failed Percentage] タブ、[Failed Count] タブが表示されます。</p> <p>過剰な DHCP、アソシエーション、または認証時間については、[Network Causes] タブ、[Top Impacted APs] タブ、[Top Impacted Times] タブが表示されます。</p> <p>過剰な DHCP、アソシエーション、または認証の失敗については、[Network Causes] タブ、[Top Impacted APs] タブ、[Top Impacted Failures] タブが表示されます。</p> <p>合計無線スループットおよびアプリケーションスループット（クラウド、コラボレーション、メディアおよびソーシャル）については、[Network Causes] タブが表示されます。</p> <p>タブをクリックすると、下のチャートが更新されます。</p> <p>追加された KPI のグラフを表示するには、[KPI]  アイコンをクリックし、KPI を選択してから、[Apply] をクリックします。</p>
Suggested Actions	この問題を解決するために実行できるアクションが表示されます。

レイヤ2のループ問題に関するインスタンスの詳細



(注) [Issue Instance Details] スライドインペインは、[Issue Instance Details] のワークフローの一部です。「未解決の問題を表示 (233 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 (232 ページ)」を参照してください。




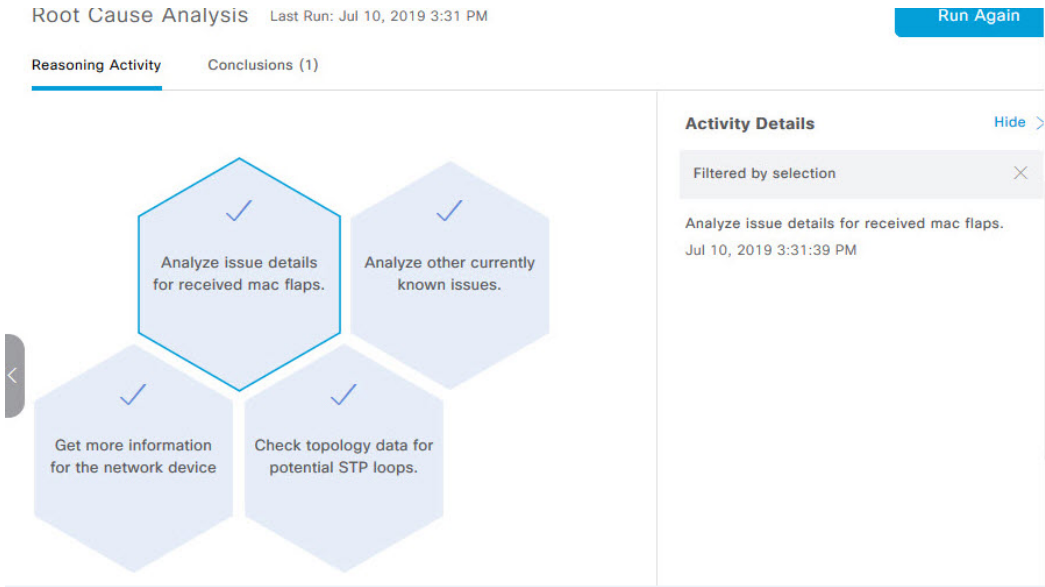
(注) レイヤー 2 ループのスケールに関する制約事項は、次のとおりです。

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

機械推論をサポートするレイヤー 2 のループ問題については、[Issue Instance Details] スライドインペインに次の情報が表示されます。

[Issue Instance Details] (2 番目のスライドインペイン)	
アイテム	説明
[Status] ドロップダウンリスト	<p>問題のステータスを変更できます。次の手順を実行します。</p> <ul style="list-style-type: none"> • 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 <ol style="list-style-type: none"> 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。
[Summary]	<p>問題の概要。デバイス、ルール、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。</p>
Problem Details	<p>問題についての簡単な説明と以下の項目が表示されます。</p> <ul style="list-style-type: none"> • [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、ルール、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	

アイテム	説明
	<p>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。</p> <ol style="list-style-type: none"> [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。 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。 [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。  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。 [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインにアクティビティの詳細が表示されます。 <p>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。</p> <p>(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。</p> <p>図 24: 推論アクティビティ</p> 

[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。「未解決の問題を表示 (233 ページ)」の **ステップ 4** を参照してください。

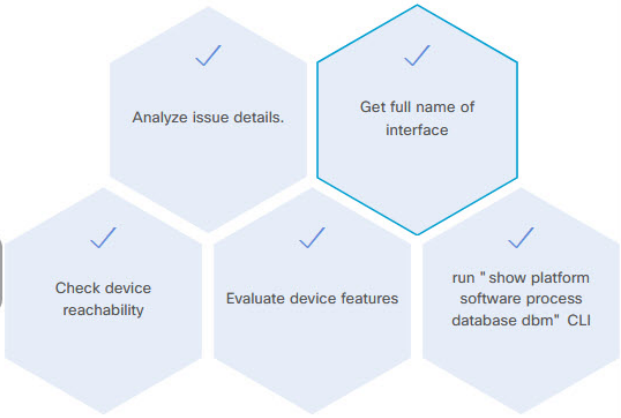
機械推論をサポートする PoE の問題については、[Issue Instance Details] スライドインペインに次の情報が表示されます。

[Issue Instance Details] (2 番目のスライドインペイン)	
アイテム	説明
[Status] ドロップダウンリスト	問題のステータスを変更できます。次の手順を実行します。 <ul style="list-style-type: none"> 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 問題の報告を停止するには、次の手順を実行します。 <ol style="list-style-type: none"> [Status] ドロップダウンリストから、[Ignore] を選択します。 スライダを使用して、問題を無視する時間数を設定し、[Confirm] をクリックします。
[Summary]	問題の概要。デバイス、ルール、時間、場所、考えられる根本原因などの情報が含まれます。
Problem Details	問題の簡単な説明と次の情報が提供されます。 <ul style="list-style-type: none"> [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
	<p>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。</p> <ol style="list-style-type: none"> 1. [Run Machine Reasoning] をクリックすると、MRE によるトラブルシューティングが開始されます。トラブルシューティングが完了すると、[Machine Reasoning Completed] ダイアログボックスが表示されます。 2. このポップアップダイアログボックスで、[View Details] をクリックします。[Root Cause Analysis] エリアが表示されます。デフォルトでは [Conclusions] タブが開き、根本原因分析の詳細が表示されます。 3. [Conclusions] エリアで [View Relevant Activities] をクリックすると、アクティビティの詳細が表示されます。このアクティビティは、根本原因分析の各ステップで使用されたコマンドを示します。 4.  アイコンをクリックして、このページの情報が役に立ったかどうかについてフィードバックを入力してください。 5. [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインに [Activity Details] が表示されます。 <p>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。</p> <p>(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。</p> <p>図 25: 推論アクティビティ</p>

アイテム	説明
	<div data-bbox="472 342 1503 961"> <p>Root Cause Analysis Last Run: Oct 12, 2020 12:43 PM Run Again ⓘ</p> <p>Reasoning Activity Conclusions (1)</p>  <p>Activity Details Hide ></p> <p>Filtered by selection ✕</p> <ul style="list-style-type: none"> Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ Get full name of interface Oct 12, 2020 12:43:53 PM ⓘ </div> <p>6. MRE を再実行する場合は、[Run Again] をクリックします。</p>

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

アシュアランスによって検出された有線クライアントの問題を表示し、MRE ワークフローを使用してトラブルシューするには、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 \(279 ページ\)](#) 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 \(90 ページ\)](#) を参照してください。

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

[Overall health] ダッシュボードが表示されます。

ステップ 2 [Client] タブをクリックします。

[Client Health] ダッシュボードが表示されます。

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

ステップ 3 [Wired Clients] サマリーエリアで、[View Details] をクリックしてスライドインペインを開きます。

ステップ 4 スライドインペインの [Wired Clients] チャートで、[Authentication] または [DHCP] をクリックします。

[Authentication] をクリックすると、チャートの下に [Top Authentication Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。認証に失敗したクライアントのリストを示すテーブルも表示されます。

[DHCP] をクリックすると、チャートの下に [Top DHCP Failure Reason]、[Top Location]、[Top Switch]、[Top Host Device Type] の情報が表示されます。テーブルも表示されます。

ステップ 5 次のいずれかを実行します。


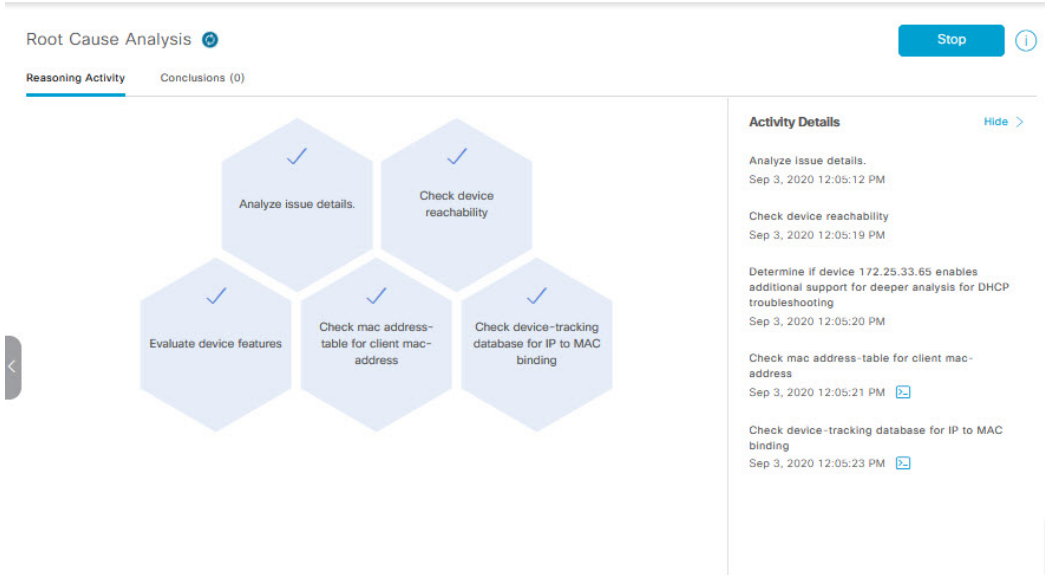
- SUPER-ADMIN-ROLE 権限を持つユーザーの場合は、検索ツールにクライアントの MAC アドレスを入力します。
- テーブルの [Identifier] 列で、ハイパーリンクされた識別子をクリックします。

クライアントの [Client 360] ウィンドウが表示されます。

ステップ 6 [Client 360] ウィンドウの [Issues] ダッシュレットで、認証または DHCP の問題をクリックします。

[Issue Details] ウィンドウに、次の情報が表示されます。

問題の詳細	
アイテム	説明
[Status] ドロップダウンリスト	<p>問題の現在のステータスが表示されます。このステータスは変更できます。次の手順を実行します。</p> <ul style="list-style-type: none"> • 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。 • 問題の報告を停止するには、次の手順を実行します。 <ol style="list-style-type: none"> 1. [Status] ドロップダウンリストから、[Ignore] を選択します。 2. スライダーで問題を無視する時間数を設定し、[Confirm] をクリックします。
[Summary]	問題の概要。デバイス、ロール、時間、場所、考えられる根本原因などの情報が含まれます。

問題の詳細	
アイテム	説明
Root Cause Analysis	<p>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。</p> <ol style="list-style-type: none"> [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。 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。 [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。  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。 [Reasoning Activity] タブをクリックすると、MRE がどのようにしてその結論に到達したのかがわかります。各推論アクティビティは、次の図に示すように、七角形のブロックで表示されます。各七角形ブロックをクリックすると、右側のペインにアクティビティの詳細が表示されます。 <p>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。</p> <p>(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。</p> <p>図 26: 推論アクティビティ</p>  <ol style="list-style-type: none"> MRE を再実行する場合は、[Run Again] をクリックします。

解決済みの問題の表示

次のカテゴリに分類される解決済みの問題をすべて表示するには、次の手順を実行します。

- しきい値ベースの問題：アシュアランスによって検出された問題。
- AI 駆動型の問題：Cisco AI Network Analyticsによって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

始める前に

AI 駆動型の解決済みの問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認してください。Cisco AI Network Analytics データ収集の設定 (87 ページ) を参照してください。





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

[Open Issues] ダッシュボードが表示されます。

ステップ 2 [Resolved] タブをクリックします。


[Resolved Issues] ウィンドウが表示されます。

ステップ 3 [Resolved Issues] ウィンドウには、次の情報が表示されます。

[Resolved Issues] ウィンドウ	
アイテム	説明
	<ul style="list-style-type: none"> • 上部のメニューバーで  をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 • ロケーションアイコンの横にある  をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 • ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 • [Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Resolved Issues] ダッシュボードに表示されます。

[Resolved Issues] ウィンドウ	
アイテム	説明
[24 Hours] ドロップダウンリスト	<p>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。</p> <ol style="list-style-type: none"> [24 時間 (24 Hours)] ドロップダウンリストで、時間範囲 ([3 時間 (3 hours)], [24 時間 (24 Hours)], または [7 日間 (7 days)]) を選択します。 [Start Date] と時刻、[End Date] と時刻を指定します。 [Apply] をクリックします。 <p>これにより、タイムラインの範囲が設定されます。</p>
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。
[Total Resolved]	<p>解決済みの問題の合計数を示します。</p> <p>[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。</p>

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Resolved Issue] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル (事前割り当てされたもの)。
Issue Type	<p>問題のタイプ。</p> <p>(注) AI 駆動型の問題の場合、問題のタイプの前に  アイコンが表示されます。</p>
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ (接続、可用性、オンボード、使用状況など)。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題タイプに関するすべての解決済み問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプ、問題を更新したエンティティ名などの情報が表示されます。

問題状況がなくなった場合、システムによる自動解決として処理され、[Updated By] 列には [System] と表示されます。[自動問題解決 \(256 ページ\)](#) を参照してください。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細（問題を解決したエンティティ名とタイムスタンプ）が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

無視された問題の表示

無視されたとしてマークされているすべての問題を表示するには、次の手順を実行します。無視された問題は、次のカテゴリに分類されます。

- しきい値ベースの問題：アシュアランスによって検出された問題。
- AI 駆動型の問題：Cisco AI Network Analytics によって検出された問題。これらの問題は、特定のネットワーク環境の予測基準からの乖離度に基づいてトリガーされます。

始める前に

AI 駆動型の無視された問題を表示するには、Cisco AI Network Analytics データ収集が設定されていることを確認します。[Cisco AI Network Analytics データ収集の設定 \(87 ページ\)](#) を参照してください。





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

[Open Issues] ダッシュボードが表示されます。


ステップ 2 [Ignored] タブをクリックします。

[Ignored Issues] ウィンドウが表示されます。

ステップ 3 [Ignored Issues] ウィンドウには、次の情報が表示されます。

[Ignored Issues] ウィンドウ	
アイテム	説明
 Global	<ul style="list-style-type: none"> 上部のメニューバーで  をクリックして、サイト階層からサイト、建物、またはフロアを選択します。 ロケーションアイコンの横にある  をクリックし、[Site Details] を選択して [Sites] テーブルを表示します。 ドロップダウンリストから [Hierarchical Site View] または [Building View] を選択します。選択した項目に基づいて、テーブルが更新されます。 [Go to sites] 列でサイトまたは建物の  をクリックすると、そのロケーションのデータのみが [Ignored Issues] ダッシュボードに表示されます。
[24 Hours] ドロップダウンリスト	<p>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。</p> <ol style="list-style-type: none"> [24 時間 (24 Hours)] ドロップダウンリストで、時間範囲 ([3 時間 (3 hours)]、[24 時間 (24 Hours)]、または [7 日間 (7 days)]) を選択します。 [Start Date] と時刻、[End Date] と時刻を指定します。 [Apply] をクリックします。 これにより、タイムラインの範囲が設定されます。
タイムラインスライダ	より詳細な時間範囲を指定できます。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。
Total Ignored	<p>無視された問題の合計数が表示されます。</p> <p>[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。</p>

ステップ 4 [All]、[P1]、[P2]、[P3]、[P4]、および [AI-Driven] のいずれかのタブをクリックすると、[Issue Type] テーブルにそのカテゴリの問題のリストが表示されます。

[Ignored Issues] ウィンドウの [Issue Type] 表	
アイテム	説明
Priority	問題タイプの優先度レベル (事前割り当てされたもの)。
Issue Type	<p>問題のタイプ。</p> <p>(注) AI 駆動型の問題の場合、問題のタイプの前に  アイコンが表示されます。</p>

[Ignored Issues] ウィンドウの [Issue Type] 表	
アイテム	説明
Device Role	問題が検出されたデバイスに割り当てられたロール。ロールは、[Access]、[Core]、[Distribution]、[Border Router]、または [Unknown] です。
Category	問題の種類が分類されるカテゴリ（接続、可用性、オンボード、使用状況など）。
Issue Count	この種類の問題が発生した回数。
Site Count (Area)	このタイプの問題が発生したサイトの数。
Device Count	このタイプの問題の影響を受けたデバイスの数。
Last Occurred Time	この問題が発生した最新の日付と時刻。

ステップ 5 [Issue type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] に、その問題のタイプのすべての無視された問題と、サイト、デバイス、デバイスタイプ、オカレンス、最後のオカレンスのタイムスタンプなどの情報が表示されます。

ステップ 6 [Issue Instances] スライドインペインの [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] に、問題に関する詳細が表示されます。問題に応じて、説明と推奨されるアクションが表示されます。

問題の解決または無視

次の手順により、問題の解決や無視を一括して、または個別に行うことができます。

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

[Open Issues] ダッシュボードが表示されます。

ステップ 2 複数の問題の解決や無視を一括して行うには、次の操作を実行します。

a) [Open Issues] ダッシュボードの [Issue Type] テーブルで、問題のタイプをクリックします。

最初のスライドインペイン [Issue Instances] が開き、その問題タイプに関するすべての未解決問題が一覧表示されます。このスライドインペインでは、問題の解決や無視を一括して行えます。

b) 次のいずれかを実行します。

- 特定の問題を解決または無視するには、問題の隣にあるチェックボックスをオンにします。
- 問題タイプのブラウザウィンドウに表示される未解決の問題をすべて解決または無視するには、[issue] 列の隣にあるチェックボックスをオンにします。ブラウザウィンドウに表示されるすべての問題が選択されます。

- 未解決の問題数が 25 を超えている場合（例：100）、最初の 25 件の問題がブラウザウィンドウに表示されます。未解決の問題をすべて選択するには、次の手順を実行します。

1. [Issue] 列の横にあるチェックボックスをオンにします。

最初の 25 件の問題が選択され、[Actions] ドロップダウンリストの横に [Select all number open issues] タブが表示されます。

2. [[Select all number open issues] をクリックすると、その問題タイプのすべての未解決問題（例：100 件すべての問題）が選択されます。

3. （オプション）ブラウザウィンドウで次の 25 件の問題を表示するには、ページの下部にある [Show More] をクリックします。次の 25 件の問題がブラウザウィンドウに追加され、表示される問題の数が 50 件に増えます。ブラウザウィンドウで次の 25 件の問題を表示するには、[Show More] をもう一度クリックします。

- c) 問題を解決するには、[Actions] ドロップダウンリストで [Resolve] を選択します。

警告ダイアログボックスが表示されます。[Warning] ダイアログボックスで [Yes] をクリックして、アクションを続行します。

問題が解決されると、[View resolved issues] タブが表示されます。[View All Issues] をクリックすると、[Resolved Issues] ウィンドウが開きます。

- d) 問題を無視するには、[Actions] ドロップダウンリストで [Ignore] を選択します。

スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。

問題が無視されると、[View ignored issues] タブが表示されます。[View ignored issues] をクリックすると、[Ignored Issues] ウィンドウが開きます。

- (注) 750 を超える問題を解決または無視しようとすると、アクションが完了するまでに 1 分ほどかかる可能性があることを知らせる警告メッセージが表示されます。

ステップ 3 問題を個別に解決または無視するには、次の手順を実行します。

- a) [Issue Instances] スライドインペイン（最初のスライドインペイン）の [issue] 列で、問題をクリックします。

2 番目のスライドインペイン [Issue Instance Details] が開き、問題に関する詳細が表示されます。この 2 番目のスライドインペインで、表示している問題を解決または無視できます。

- b) 問題を解決するには、[Status] ドロップダウンメニューで [Resolve] を選択します。

- c) 問題の報告を停止するには、次の手順を実行します。

1. [Status] ドロップダウンリストから、[Ignore] を選択します。

2. スライダで問題を無視する時間数を設定し、[Confirm] をクリックします。

無線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、**アシュアランス > [Manage] > [Issue Settings]**に移動します。[グローバルな問題の設定の管理 \(257 ページ\)](#) 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

次のタイプの問題については、問題の状態が存在しなくなった場合、システムは自動的に問題を解決します。

- インターフェイスが停止した。
- ワイヤレスコントローラ/スイッチ/ルータが到達不能である。
- 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。



(注) 次のいずれかの状態が解消した場合、システムによって自動的にこの問題が解決されます。

- この無線でクライアント数が 0 である。
- RX データまたは管理フレーム数が増えていない。
- AP 無線チャンネルの使用率が 0 である。

問題が解決されると、**[Resolved Issues] > [Issue Instance]** slide-in paneの [Updated By] 列に [System] と表示されます。[解決済みの問題の表示 \(250 ページ\)](#) 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。トリガー可能な特定の問題を有効または無効にする、問題の優先順位を変更する、問題がトリガーされるしきい値を変更する、トリガーされたときに問題を外部通知に登録するといった操作を実行できます。

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

[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 設定する問題のタイプを表示するには、**[DEVICE TYPE]** と **[CATEGORY]** フィルタを設定します。

AI 駆動型の問題を表示するには、**[CATEGORY]** フィルタの **[AI-Driven]** タブをクリックします。

ステップ 3 [Issue Name] 列の問題をクリックすると、次の設定を含むスライドインペインが開きます。

(注) いくつかの問題については、設定に加えられた変更は複数のデバイスタイプで共有されます。スライドインペインで、情報アイコン (i) にカーソルを合わせると、影響を受けるデバイスタイプが表示されます。

- a) 問題がトリガー可能かどうかを有効または無効にするには、**[Enabled]** トグルをクリックします。
- b) 問題の優先順位を設定するには、**[Priority]** ドロップダウンリストをクリックし、優先順位を選択します。次のオプションがあります。
 - [P1] : ネットワーク運用に幅広い影響を与える可能性がある、早急な対応を必要とする重大な問題。
 - [P2] : 複数のデバイスまたはクライアントに影響を与える可能性がある重大な問題。
 - [P3] : 局所的または最小限の影響を与える軽微な問題。
 - [P4] : ただちに問題になるものではないが、対処するとネットワークのパフォーマンスを最適化できる警告レベルの問題。
- c) (一部の問題のみ) **[Trigger Condition]** エリアで、問題が報告される条件のしきい値を変更できます。

(注) 「無線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 \(256 ページ\)](#) を参照してください。

トリガー条件の例 :

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
アクセスポイントのメモリ使用率が 90% を超えた
```

- d) (任意) 設定に変更がある場合は、[View Default Settings] の上にカーソルを置くと、デフォルトの問題が表示されます。問題の設定をすべてデフォルト値に復元するには、[Use Default] をクリックします。
- e) [Apply] をクリックします。

ステップ 4 (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 \(259 ページ\)](#) を参照してください。

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。これらの設定はアシュアランスのネットワークプロファイルと呼ばれ、アシュアランスと Cisco DNA Center の両方から管理できます。

アシュアランス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、[デバイスの健全性のモニターとトラブルシューティング \(109 ページ\)](#) 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。

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

Cisco DNA Center によってプロファイルが追加され、[Edit Profile] ウィンドウが表示されます。

ステップ 5 設定する問題のタイプを表示するには、[DEVICE TYPE] と [CATEGORY] フィルタを設定します。

ステップ 6 [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に、影響を受けるデバイスタイプを示す注意が Cisco DNA Center によって表示されます。

- ステップ 7** この問題の Cisco DNA Center によるモニター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 8** 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 9** (一部の問題のみ) [Trigger Condition] エリアで、問題が報告される条件のしきい値を変更できます。トリガー条件の例 :
- ```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%
```
- ステップ 10** (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 11** [Apply] をクリックします。
- ステップ 12** (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 13** このプロファイルサイトを割り当てるには、[Assign Sites] をクリックします。このプロファイルに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。
- ステップ 14** [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

アシュアランスで特定の問題がトリガーされたときに外部通知を受信するには、次の手順を実行します。問題がトリガーされてステータスが変わると、アシュアランスは、REST または電子メール通知を生成できます。

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

[Issue Settings] ウィンドウが表示されます。

ステップ2 [Manage Subscriptions] をクリックします。

[Events] ウィンドウが表示されます。

ステップ3 登録するイベントのチェックボックスをオンにします。

(注) Cisco DNA Center プラットフォームの [Event] の名前は、アシュアランスの [Issue Name] と同じです。

ステップ4 [Subscribe] をクリックします。

[Subscribe] ダイアログボックスが表示されます。

ステップ5 [Subscribe] ダイアログボックスで、サブスクリプションの詳細を入力します。

- a) [Name] フィールドに、サブスクリプション名を入力します。
- b) [Subscription Type] ドロップダウンリストをクリックして、通知タイプを選択します。REST または電子メール通知を受信できます。

| 通知タイプ   | 詳細                                                                                                                                                                                                                                                                                                                                                                                |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [REST]  | <p>問題/イベントがトリガーされたときに、REST 通知を受信します。次の設定を行います。</p> <ul style="list-style-type: none"> <li>• [Select an existing endpoint] または [Create a new endpoint] のどちらかのオプションを選択して、そのエンドポイントを指定し、そのエンドポイントの後続のフィールドを設定します。</li> <li>• 信頼できる証明書</li> <li>• [HTTP Method] : [POST] または [PUT] を選択できます。</li> <li>• [Headers] : [Header Key] フィールドと [Header Value] フィールドにヘッダーの詳細を入力します。</li> </ul> |
| [EMAIL] | <p>問題/イベントがトリガーされたときに電子メール通知を受信します。</p> <p><b>重要</b> 電子メール通知を受信するには、[System Settings] &gt; [Email configuration] ウィンドウで、電子メールサーバーが設定されていることを確認します。</p>                                                                                                                                                                                                                            |

- c) [Subscribe] をクリックします。

問題/イベントのサブスクリプションが作成されます。問題/イベントがトリガーされると、ステータス変更の通知が送信されます。



## 次のタスク

Cisco DNA Center プラットフォーム で既存のイベントサブスクリプションを表示および管理できます。詳細については、『*Cisco DNA Center Platform User Guide*』の「*Working with Events*」を参照してください。

# アシュアランス、Cisco AI Network Analytics、および MRE の問題

## ルータの問題

アシュアランス で検出されるルータの問題を次の表に示します。

| ルータの問題 |                                         |                                                                           |
|--------|-----------------------------------------|---------------------------------------------------------------------------|
| カテゴリ   | 問題の名称                                   | 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を接続しているインターフェイスがダウンしています。                                       |
| 接続性    | レイヤ 2 のループ症状                            | ネットワークデバイスでホスト MAC アドレスのフラッピングが見られます。                                     |
| 接続性    | ネットワークデバイスインターフェイスの接続 - BGP フラップ        | ネイバーとのボーダーゲートウェイ プロトコル (BGP) 接続がフラッピングしています。                              |
| 接続性    | ネットワーク デバイス インターフェイスの接続 - EIGRP 隣接関係の障害 | ネイバーとの Enhanced Interior Gateway Routing Protocol (EIGRP) 隣接関係に障害が発生しました。 |
| 接続性    | ネットワークデバイスインターフェイスの接続 - インターフェイスダウン     | デバイス上のインターフェイスがダウンしています。                                                  |
| 接続性    | ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害  | デバイスで Intermediate System Intermediate System (ISIS) の隣接関係に障害が発生しました。     |
| 接続性    | ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害  | ネイバーとの Open Shortest Path First (OSPF) 隣接関係に障害が発生しました。                    |

| ルータの問題    |                                  |                                                                                              |
|-----------|----------------------------------|----------------------------------------------------------------------------------------------|
| カテゴリ      | 問題の名称                            | 概要                                                                                           |
| 接続        | WAN インターフェイスダウン                  | WAN ネットワークに接続しているインターフェイスがダウンしています。                                                          |
| 接続されている状態 | SGT のアクセスポリシーのインストールに失敗          | セキュリティグループタグ (SGT) のセキュリティグループアクセスコントロールリスト (SGACL) アクセスポリシーのインストールに失敗しました。                  |
| 接続されている状態 | ルータインターフェイスの入出力エラー率が高い           | インターフェイスの入出力エラー率が高くなっています。                                                                   |
| 接続されている状態 | ルータインターフェイスの入出力破棄率が高い            | インターフェイスの入出力破棄率が高くなっています。                                                                    |
| 接続されている状態 | ルータインターフェイスの入力/出力使用率が高い          | インターフェイスの入出力使用率が高くなっています。                                                                    |
| 接続されている状態 | ルータ WAN インターフェイスの入出力破棄率が高い       | WAN インターフェイスの入出力破棄率が高くなっています。                                                                |
| 接続されている状態 | ルータ WAN インターフェイスの入力/出力使用率が高い     | WAN インターフェイスの入出力使用率が高くなっています。                                                                |
| 接続されている状態 | デバイスでSGTアクセスポリシーのダウンロードに失敗       | セキュリティグループタグ (SGT) のセキュリティグループアクセスコントロールリスト (SGACL) アクセスコントロールエントリ (ACE) のダウンロードに失敗しました。     |
| 接続されている状態 | デバイスでSGTアクセスポリシーのインストールに失敗       | セキュリティグループタグ (SGT) のアクセスポリシーのインストールに失敗しました。ロールベースのアクセスコントロールリスト (RBACL) でポリシールールエラーが見つかりました。 |
| 接続されている状態 | ポリシーサーバーからSGTアクセスポリシーをダウンロードできない | セキュリティグループタグ (SGT) のアクセスポリシーのソースリストをダウンロードできませんでした。                                          |
| 接続されている状態 | デバイスでSGTアクセスポリシーのアンインストールに失敗     | セキュリティグループタグ (SGT) のセキュリティグループアクセスコントロールリスト (SGACL) アクセスポリシーのアンインストールに失敗しました。                |
| デバイス      | DNA Centerとネットワークデバイスの時間差        | Cisco DNA Center とデバイスの間には過剰なタイムラグがあります。                                                     |
| デバイス      | syslog イベントに基づく問題 - 高温           | 高温に関連する syslog イベントの単一オカレンスによって作成された問題。                                                      |
| デバイス      | ルータの高 CPU 使用率                    | デバイスで CPU 使用率が高くなっています。                                                                      |

| ルータの問題 |                         |                                       |
|--------|-------------------------|---------------------------------------|
| カテゴリ   | 問題の名称                   | 概要                                    |
| デバイス   | ルータの高メモリ使用率             | デバイスでメモリ使用率が高くなっています。                 |
| 可用性    | ネットワークデバイスの HA スイッチオーバー | ネットワークデバイスで高可用性 (HA) スイッチオーバーが発生しました。 |
| 可用性    | ルータ到達不能                 | ネットワークデバイスがコントローラから到達不能です。            |

## コア層、ディストリビューション層、およびアクセス層に関する問題

アシュアランスによって検出されるコア層、ディストリビューション層、およびアクセス層の問題を次の表に示します。

| コア層、ディストリビューション層、およびアクセス層に関する問題 |                                         |                                                                           |
|---------------------------------|-----------------------------------------|---------------------------------------------------------------------------|
| カテゴリ                            | 問題の名称                                   | 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を接続しているインターフェイスがダウンしています。                                       |
| 接続性                             | レイヤ 2 のループ症状                            | ネットワークデバイスでホスト MAC アドレスのフラッピングが見られます。                                     |
| 接続性                             | ネットワークデバイスインターフェイスの接続 - BGP フラップ        | ネイバーとの BGP 接続がフラッピングしています。                                                |
| 接続性                             | ネットワーク デバイス インターフェイスの接続 - EIGRP 隣接関係の障害 | ネイバーとの EIGRP (Enhanced Interior Gateway Routing Protocol) 隣接関係に障害が発生しました。 |
| 接続性                             | ネットワークデバイスインターフェイスの接続 - インターフェイスダウン     | デバイス上のインターフェイスがダウンしています。                                                  |
| 接続性                             | ネットワーク デバイス インターフェイスの接続 - ISIS 隣接関係の障害  | デバイスで Intermediate System Intermediate System (IS-IS) の隣接関係に障害が発生しました。    |
| 接続性                             | ネットワーク デバイス インターフェイスの接続 - OSPF 隣接関係の障害  | ネイバーとの Open Shortest Path First (OSPF) 隣接関係に障害が発生しました。                    |

## コア層、ディストリビューション層、およびアクセス層に関する問題

| コア層、ディストリビューション層、およびアクセス層に関する問題 |                                        |                                                                   |
|---------------------------------|----------------------------------------|-------------------------------------------------------------------|
| カテゴリ                            | 問題の名称                                  | 概要                                                                |
| 接続                              | WAN インターフェイスダウン                        | WAN ネットワークに接続しているインターフェイスがダウンしています。                               |
| 接続性                             | ネットワークデバイスでデュアルアクティブ検出リンクに障害発生         | ネットワークデバイス <i>Switch Name</i> 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 <i>Switch Name</i> 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 <i>Switch Name</i> で StackWise リンクに障害が発生しました。          |
| 接続されている状態                       | ファブリックデバイスの接続-ボーダーオーバーレイ               | ファブリックエッジが仮想ネットワーク内のファブリックボーダーへの接続を失いました。                         |
| 接続されている状態                       | ファブリックデバイスの接続-ボーダーアンダーレイ               | ファブリックエッジが物理ネットワーク内のファブリックボーダーへの接続を失いました。                         |
| 接続されている状態                       | ファブリックデバイスの接続 - コントロールボーダーアンダーレイ       | ファブリックノードは、物理ネットワーク内の同じ場所に配置されたファブリックボーダーとコントロールプレーンへの接続を失いました。   |
| 接続されている状態                       | ファブリックデバイスの接続 - コントロールアンダーレイ           | ファブリックノードは、物理ネットワーク内のファブリック コントロールプレーンデバイスへの接続を失いました。             |
| 接続されている状態                       | ファブリックデバイスの接続 - DHCP オーバーレイ            | ファブリックノードが仮想ネットワーク内の DHCP サーバーへの接続を失いました。                         |
| 接続されている状態                       | ファブリックデバイスの接続 - DHCP アンダーレイ            | ファブリックノードが物理ネットワーク内の DHCP サーバーへの接続を失いました。                         |
| 接続されている状態                       | ファブリックデバイスの接続-DNS オーバーレイ               | ファブリックノードが仮想ネットワーク内の DNS サーバーへの接続を失いました。                          |
| 接続されている状態                       | ファブリックデバイスの接続-DNS アンダーレイ               | ファブリックノードが物理ネットワーク内の DNS サーバーへの接続を失いました。                          |
| 接続されている状態                       | ファブリックデバイスの接続 - 外部 URL                 | ユーザーがプロビジョニングした外部 URL にファブリックボーダーが到達できません。                        |
| 接続されている状態                       | ファブリックデバイスの接続 - ISE サーバー               | ファブリックエッジが物理ネットワーク内の ISE サーバーへの接続を失いました。                          |
| 接続されている状態                       | SGT のアクセスポリシーのインストールに失敗                | SGT の SGACL アクセスポリシーのインストールに失敗しました。                               |

| コア層、ディストリビューション層、およびアクセス層に関する問題 |                                  |                                                                |
|---------------------------------|----------------------------------|----------------------------------------------------------------|
| カテゴリ                            | 問題の名称                            | 概要                                                             |
| 接続されている状態                       | スイッチインターフェイスの入出力エラー率が高い          | スイッチインターフェイスの入出力エラー率が高くなっています。                                 |
| 接続されている状態                       | スイッチインターフェイスの入出力破棄率が高い           | スイッチインターフェイスの入出力破棄率が高くなっています。                                  |
| 接続されている状態                       | スイッチインターフェイスの入出力使用率が高い           | インターフェイスの入出力使用率が高くなっています。                                      |
| 接続されている状態                       | デバイスでSGTアクセスポリシーのダウンロードに失敗       | SGTのSGACL ACEのダウンロードに失敗しました。                                   |
| 接続されている状態                       | デバイスでSGTアクセスポリシーのインストールに失敗       | SGTのアクセスポリシーのインストールに失敗しました。RBACLでポリシー規則エラーが検出されました。            |
| 接続されている状態                       | ポリシーサーバーからSGTアクセスポリシーをダウンロードできない | SGTのアクセスポリシーのソースリストをダウンロードできませんでした。                            |
| 接続されている状態                       | デバイスでSGTアクセスポリシーのアンインストールに失敗     | SGTのSGACLアクセスポリシーのアンインストールに失敗しました。                             |
| デバイス                            | デバイスリブートクラッシュ                    | ハードウェアまたはソフトウェアのクラッシュによりデバイスがリブートしました。                         |
| デバイス                            | デバイス時間のずれ Cisco DNA Center       | Cisco DNA Center とデバイス間に過剰なタイムラグがあります。                         |
| デバイス                            | ネットワークデバイスでインターフェイスのフラッピングが発生    | ポートインターフェイスがスイッチでフラッピングしています。                                  |
| デバイス                            | syslog イベントに基づく問題 - 高温           | 高温に関連する syslog イベントの単一オカレンスによって作成された問題。                        |
| デバイス                            | syslog イベントに基づく問題 - POE          | 電源に関連する syslog イベントの単一オカレンスによって作成された問題。                        |
| デバイス                            | PoE ポートがエラー状態                    | PoE ポートがエラーにより無効になっていることが syslog イベントで報告されました。                 |
| デバイス                            | PoE 受電デバイスに障害フラグあり               | PoE ポートに接続された PoE 対応デバイスに障害フラグが設定されていることが syslog イベントで報告されました。 |
| デバイス                            | PoE 受電デバイスへの電力供給拒否               | PoE ポートに接続された PoE 対応デバイスへの電力供給が拒否されたことが syslog イベントで報告されました。   |

## コントローラの問題

| コア層、ディストリビューション層、およびアクセス層に関する問題 |                         |                                          |
|---------------------------------|-------------------------|------------------------------------------|
| カテゴリ                            | 問題の名称                   | 概要                                       |
| デバイス                            | スタックメンバーの削除             | スタックメンバーが削除されました。                        |
| デバイス                            | スタックメンバーが互換性のないイメージを実行  | スタックメンバーが互換性のないイメージを実行しています。             |
| デバイス                            | スイッチの高 CPU 使用率          | デバイスで CPU 使用率が高くなっています。                  |
| デバイス                            | スイッチの高メモリ使用率            | デバイスでメモリ使用率が高くなっています。                    |
| デバイス                            | スイッチファンの障害              | スイッチのファンに障害が発生しました。                      |
| デバイス                            | スイッチの電源障害               | スイッチの電源に障害が発生しました。                       |
| デバイス                            | 高 TCAM 使用率の問題           | レイヤ 2、レイヤ 3、QoS、および SGACL での TCAM 枯渇の問題。 |
| 可用性                             | ネットワークデバイスの HA スイッチオーバー | ネットワークデバイスで HA スイッチオーバーが発生しました。          |
| 可用性                             | スイッチ到達不能                | デバイスが到達不能です。                             |
| 使用率<br>(Utilization)            | マップキャッシュの上限に達した         | マップキャッシュエントリがマップサーバーの上限を超えました。           |

## コントローラの問題

アシュアランスによって検出されるコントローラの問題を次の表に示します。

| コントローラの問題 |                                 |                                                       |
|-----------|---------------------------------|-------------------------------------------------------|
| カテゴリ      | 問題の名称                           | 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を接続しているインターフェイスがダウンしています。                   |
| 接続されている状態 | ファブリック WLC と MapServer の接続性     | ファブリック 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 Cisco DNA Center      | Cisco DNA Center とデバイス間に過剰なタイムラグがあります。                |
| 可用性       | ネットワークデバイスの HA スイッチオーバー         | ネットワークデバイスで HA スイッチオーバーが発生しました。                       |

| コントローラの問題            |                   |                                         |
|----------------------|-------------------|-----------------------------------------|
| カテゴリ                 | 問題の名称             | 概要                                      |
| 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に障害が発生しました。             |
| 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 リブートクラッシュ。                  |
| 可用性                  | WLC 到達不能          | デバイスが到達不能です。                            |
| 使用率<br>(Utilization) | 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<br>(Utilization) | WLC 高メモリ使用率       | ワイヤレスコントローラに高メモリ使用率が発生しています。            |

## アクセスポイントの問題

アシュアランスによって検出されるアクセスポイントの問題を次の表に示します。

| アクセスポイントの問題          |                      |                                                          |
|----------------------|----------------------|----------------------------------------------------------|
| カテゴリ                 | 問題の名称                | 概要                                                       |
| 可用性                  | AP のカバレッジホール         | AP にカバレッジホールがあります。                                       |
| 可用性                  | Cisco WLC からの AP の切断 | AP が切断されています。                                            |
| 可用性                  | AP のフラッピング           | AP でフラッピングが発生しています。この問題は、AP が 15 分以内に 2 回以上フラップすると発生します。 |
| 可用性                  | AP のリブートクラッシュ        | ハードウェアまたはソフトウェアのクラッシュにより AP がリブートしました。                   |
| 使用率<br>(Utilization) | AP の高 CPU 使用率        | AP で CPU 使用率が高くなっています。                                   |
| 使用率<br>(Utilization) | AP の高メモリ使用率          | AP のメモリ使用率が高くなっています。                                     |
| 使用率<br>(Utilization) | 無線の高使用率 (2.4 GHz)    | AP の 2.4 GHz 無線の使用率が高くなっています。                            |
| 使用率<br>(Utilization) | 無線の高使用率 (5 GHz)      | AP の 5 GHz 無線の使用率が高くなっています。                              |

## アクセスポイントの問題

| 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<br>(Utilization) | 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。                                                                                                                                                                                                                                             |
| 使用率<br>(Utilization) | 無線でのアクティビティなし (2.4 GHz) | AP の 2.4 GHz 無線 x でアクティビティがありません。                                                                                                                                                                                                                                       |
| 使用率<br>(Utilization) | 無線でのアクティビティなし (5 GHz)   | AP の 5 GHz 無線 x でアクティビティがありません。                                                                                                                                                                                                                                         |
| 使用率<br>(Utilization) | 無線でのアクティビティなし (6GHz)    | AP の 6 GHz 無線 x でアクティビティがありません。                                                                                                                                                                                                                                         |
| AP 異常                | AP 異常                   | AP で異常が発生しました。                                                                                                                                                                                                                                                          |
| 可用性                  | フロアでの RF (2.4 GHz) の低下  | <p>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。</p> <p>無線周波数 (RF) の低下の問題には次のようなものがあります。</p> <ul style="list-style-type: none"> <li>• 単一の問題は、干渉またはノイズが、30 分以内に特定の AP 帯域のしきい値を超えた場合にトリガーされます。</li> <li>• グローバルな問題は、少なくとも 1 つの AP の干渉またはノイズが、30 分以内にしきい値を超えた場合にトリガーされます。</li> </ul> |
| 可用性                  | フロアでの RF (5 GHz) の低下    | <p>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。</p> <p>RF の低下の問題には次のようなものがあります。</p> <ul style="list-style-type: none"> <li>• 単一の問題は、干渉またはノイズが、30 分以内に特定の AP 帯域のしきい値を超えた場合にトリガーされます。</li> <li>• グローバルな問題は、少なくとも 1 つの AP の干渉またはノイズが、30 分以内にしきい値を超えた場合にトリガーされます。</li> </ul>         |



| 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         | 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。<br><br>RF の低下の問題には次のようなものがあります。 <ul style="list-style-type: none"> <li>• 単一の問題は、干渉またはノイズが、30 分以内に特定の AP 帯域のしきい値を超えた場合にトリガーされます。</li> <li>• グローバルな問題は、少なくとも 1 つの AP の干渉またはノイズが、30 分以内にしきい値を超えた場合にトリガーされます。</li> </ul> |
| 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

アシュアランスによって検出される有線クライアントの問題を次の表に示します。

| 有線クライアントの問題 |                            |                                                                                              |
|-------------|----------------------------|----------------------------------------------------------------------------------------------|
| カテゴリ        | 問題の名称                      | 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 | 有線クライアント認証に失敗しました。Dot1.x を使用するユーザーデバイス認証のエラーです。<br><br>(注) この問題は、単独の有線クライアントにのみ適用されます。       |
| オンボーディング    | 有線クライアント認証エラー - MAB エラー    | 有線クライアント認証に失敗しました。ユーザーデバイス認証が MAC 認証バイパスの問題により失敗しました。<br><br>(注) この問題は、単独の有線クライアントにのみ適用されます。 |

## ワイヤレスクライアントの問題

アシュアランスによって検出されるワイヤレスクライアントの問題を次の表に示します。

## ワイヤレスクライアントの問題



(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除外 - IP 盗難の問題                        | ワイヤレスクライアントの除外 - IP 盗難の問題が発生しました。                                  |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - AAA サーバーによるクライアントの拒否          | ワイヤレスクライアントの接続失敗 - AAA サーバーによりクライアントが拒否されました。                      |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウト               | ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウトが発生しました。                         |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアント PMK が見つからない            | ワイヤレスクライアントの接続失敗 - クライアント PMK が見つかりません。                            |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウト                 | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証に失敗しました。                      |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウト              | ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウトが発生しました。                        |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - DHCP タイムアウト                   | ワイヤレスクライアントの接続失敗 - DHCP タイムアウトが発生しました。                             |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスの取得失敗 | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスを取得できませんでした。            |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - 不正な PSK                       | ワイヤレスクライアントは接続に失敗し、除外されました。クライアントの PSK は設定された WLAN PSK と一致しませんでした。 |

| 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 - セキュリティパラメータの不一致         | ワイヤレスクライアントの接続失敗 - セキュリティパラメータが一致していません。          |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - WLC 設定エラー               | ワイヤレスクライアントの接続失敗 - 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。              |
| 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     | ワイヤレスクライアントの AP 間のローミング失敗 - ワイヤレスコントローラ設定が一致しません。 |

## ワイヤレスクライアントの問題

| 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 - 認証タイムアウトによる過剰な時間               | ワイヤレスクライアントの接続に時間がかかる - 認証タイムアウトにより過剰な時間がかかります。                |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害による過剰な時間           | ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害により過剰な時間がかかります。            |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーによる過剰な時間              | ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーによる過剰な時間がかかりました。              |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - WLC の障害による過剰な時間                | ワイヤレスクライアントの接続に時間がかかる - ワイヤレスコントローラ の障害による過剰な時間。               |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - AAA サーバーまたはネットワークの遅延による過剰な認証時間 | ワイヤレスクライアントの接続に時間がかかる - AAA サーバーまたはネットワークの遅延により過剰な認証時間がかかりました。 |
| オンボーディング       | ワイヤレスクライアントの除外 - IP 盗難の問題                              | ワイヤレスクライアントの除外 - IP 盗難の問題が発生しました。                              |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - AAA サーバーによるクライアントの拒否                | ワイヤレスクライアントの接続失敗 - AAA サーバーによりクライアントが拒否されました。                  |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウト                     | ワイヤレスクライアントの接続失敗 - AAA サーバーのタイムアウトが発生しました。                     |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアント PMK 未検出                      | ワイヤレスクライアントの接続失敗 - クライアント PMK が見つかりません。                        |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウト                    | ワイヤレスクライアントの接続失敗 - DHCP サーバーのタイムアウトが発生しました。                    |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証失敗                | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより認証に失敗しました。                  |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトによる IP アドレス取得失敗        | ワイヤレスクライアントの接続失敗 - クライアントのタイムアウトにより IP アドレスを取得できませんでした。        |

| ワイヤレスクライアントの問題 |                                                             |                                                                                    |
|----------------|-------------------------------------------------------------|------------------------------------------------------------------------------------|
| カテゴリ           | 問題の名称                                                       | 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 - DHCPサーバーまたはクライアントのタイムアウトによる IP アドレスを取得失敗 | ワイヤレスクライアントの接続失敗 - DHCPサーバーまたはクライアントのタイムアウトにより IP アドレスを取得できませんでした。                 |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - 不正な PSK                                  | ワイヤレスクライアントは接続に失敗し、除外されました。クライアントの PSK は設定された WLAN PSK と一致していませんでした。               |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - セキュリティパラメータの不一致                          | ワイヤレスクライアントの接続失敗 - 認証中にセキュリティパラメータが一致していません。                                       |
| オンボーディング       | ワイヤレスクライアントの接続失敗 - WLC 設定エラー                                | ワイヤレスクライアントの接続失敗 - 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 のクライアント除外ポリシー                     | ワイヤレスクライアントのローミング失敗 - クライアントはワイヤレス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。                   |
| オンボーディング       | ワイヤレスクライアントのローミング失敗 - クライアントがローミングの前に除外される                  | ワイヤレスクライアントのローミング失敗 - クライアントがローミングの前に除外されました。                                      |
| オンボーディング       | ワイヤレスクライアントのローミング失敗 - WLC 設定の不一致                            | ワイヤレスクライアントの AP 間のローミング失敗 - ワイヤレスコントローラ設定が一致していません。                                |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害による過剰な時間                | ワイヤレスクライアントの接続に時間がかかる - DHCP サーバーの障害により過剰な時間がかかりました。                               |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラー                           | ワイヤレスクライアントの接続に時間がかかる - ログイン情報エラーにより過剰な時間がかかりました。                                  |
| オンボーディング       | ワイヤレスクライアントの接続に時間がかかる - WLC の障害                             | ワイヤレスクライアントの接続に時間がかかる - ワイヤレスコントローラの障害による過剰な時間。                                    |
| 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。                    |

## AAA 障害の根本原因分析の問題を有効にする

| 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                                                                   |
| 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の問題を有効にする

Cisco DNA 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。

Cisco DNA 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。

アシュアランス で AAA 障害の根本原因分析の問題を有効にするには、次の手順を実行します。

**ステップ 1** Cisco DNA Center で、[System] > [Settings] > [External Services] > [Authentication and Policy Servers] の順に選択し、Cisco ISE を Cisco DNA Center に追加して設定します。この手順により、Cisco ISE ポリシーサーブスノード (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、Cisco DNA 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ロギングカテゴリの [Failed Attempts]、[Authentication Flow Diagnostics]、および [RADIUS Diagnostics] に追加します。

Cisco ISE syslog を Cisco DNA Center に送信できるようになりました。Cisco DNA 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。

## アプリケーションの問題

アシュアランス によって検出されるアプリケーションの問題を次の表に示します。

| アプリケーションの問題 |                     |                             |
|-------------|---------------------|-----------------------------|
| カテゴリ        | 問題の名称               | 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

アシュアランス で検出されるセンサーの問題を次の表に示します。

同じフロアにある 2 つ以上のセンサーが 30 分間のテストに失敗した場合、センサーは失敗の根本原因に基づいて問題を報告することがあります。これらのセンサーの問題はすべてグローバルな問題です。つまり、すべてのフロアのセンサーの問題がエスカレーションされて、[Issues] ダッシュボードに表示されます。

| センサーの問題 |                          |                                                    |
|---------|--------------------------|----------------------------------------------------|
| カテゴリ    | 問題の名称                    | 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。 |

## ■ センサーの問題

| 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 - iPerf テストネットワークエラー | iPerfのネットワークエラーが原因で、複数のセンサーがiPerfテストを実行できませんでした。                  |
| センサーテスト | センサー - iPerf 未定義のエラー      | 未定義エラーが原因で、複数のセンサーがiPerfテストを実行できませんでした。                           |
| センサーテスト | センサー - IPSLA IP アドレスなし    | 複数のセンサーが Cisco DNA Center から IPSLA テスト IP アドレスを受信していないことを報告しています。 |
| センサーテスト | センサー - IPSLA 応答なし         | 複数のセンサーが IPSLA テストで IPSLA 応答側からの応答がないことを報告しています。                  |
| センサーテスト | センサー - IPSLA ソケットエラー      | 複数のセンサーが IPSLA テストソケットエラーを報告しています。                                |
| センサーテスト | センサー - IPSLA テスト失敗        | 複数のセンサーが IPSLA テスト失敗を報告しています。                                     |
| センサーテスト | センサー - IPSLA 非対応プローブタイプ   | 複数のセンサーが IPSLA テスト非対応プローブタイプを報告しています。                             |
| センサーテスト | センサー - メールサーバーのテスト失敗      | 複数のセンサーがメールサーバーに接続できなかったことを報告しています。                               |
| センサーテスト | センサー - メールサーバーに到達不能       | 複数のセンサーがメールサーバーに到達できないことを報告しています。                                 |
| センサーテスト | センサー - NDT サーバーなし         | 複数のセンサーが速度テスト NDT サーバーが存在しないことを報告しています。                           |
| センサーテスト | センサー - オンボーディングの障害        | センサーがワイヤレスネットワークに接続できませんでした。                                      |
| センサーテスト | センサー - Outlook サーバーのテスト失敗 | 複数のセンサーが Outlook Web アクセスに接続できなかったことを報告しています。                     |
| センサーテスト | 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 - 速度テストの一般的なエラー       | 複数のセンサーが速度テストの一般的な障害を報告しています。                 |
| センサーテスト | センサー - 速度テストのアップリンクタイムアウト  | 複数のセンサーが速度テストでのアップリンクテストのタイムアウトを報告しています。      |
| センサーテスト | センサー - 速度テスト URL エラー       | クエリサーバーへのアクセス中、複数のセンサーが速度テスト URL エラーを報告しています。 |
| センサーテスト | センサー - 到達不能なホスト            | 複数のセンサーがホストへの ping の失敗を報告しています。ホストに到達できません。   |
| センサーテスト | センサー - 到達不能な RADIUS        | 複数のセンサーが RADIUS サーバーに到達できないことを報告しています。        |
| センサーテスト | センサー - Web 認証の失敗           | 複数のセンサーが、クライアントが Web 認証テストに失敗していることを報告しています。  |
| センサーテスト | センサー - Web サーバーのテスト失敗      | 複数のセンサーが Web サーバーからページをロードできなかったことを報告しています。   |
| センサーテスト | センサー - Web サーバーに到達不能       | 複数のセンサーが Web サーバーに到達できないことを報告しています。           |
| センサーテスト | センサー - Web ソケットエラー         | 複数のセンサーがテスト中に速度テスト websocket エラーを報告しています。     |
| センサーテスト | センサー - 速度テストのアップリンクプロキシエラー | 複数のセンサーが速度テストのアップリンクテストでプロキシエラーを報告しています。      |

## AI 駆動型の問題

Cisco AI Network Analytics によって検出される AI 駆動型の問題を次の表に示します。

| AI 駆動型の問題 |                       |                                                                            |
|-----------|-----------------------|----------------------------------------------------------------------------|
| カテゴリ      | 問題の名称                 | 概要                                                                         |
| 接続の問題     |                       |                                                                            |
| オンボーディング  | Ⓜ 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。 |

| AI 駆動型の問題           |                                      |                                                                                                                |
|---------------------|--------------------------------------|----------------------------------------------------------------------------------------------------------------|
| カテゴリ                | 問題の名称                                | 概要                                                                                                             |
| オンボーディング            | AI 過剰な接続障害回数 - 基準から大きく乖離             | 通常と比較して、ネットワークでのオンボーディング時間がかなり長くなっています。クライアントは、 <i>SSID</i> 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、 <i>location</i> にある <i>SSID</i> 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 - <i>SSID</i> での時間が少なくとも <i>value%</i> 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 - <i>SSID</i> での障害回数が少なくとも <i>value%</i> 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 - <i>SSID</i> での時間が少なくとも <i>value%</i> 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 - <i>SSID</i> での障害回数が少なくとも <i>value%</i> 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 - <i>server_IP</i> からの取得時間が少なくとも <i>value%</i> 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 - <i>server_IP</i> での障害回数が少なくとも <i>value%</i> 増加しています。                                       |
| ネットワークの接続性に関する問題    |                                      |                                                                                                                |
| 接続性                 | AI ネットワークデバイスでホスト MAC アドレスのフラッピングが発生 | ネットワークでレイヤ 2 のループ症状が発生しています。                                                                                   |
| アプリケーションエクスペリエンスの問題 |                                      |                                                                                                                |
| スループット              | AI すべてのアプリケーションの合計無線スループットの低下        | ネットワーク内の AP で、すべてのアプリケーションの合計無線スループットが低下しています。これらの無線は <i>frequency</i> 帯域内にあります。これらの無線は <i>location</i> 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 <i>frequency</i> 帯域内にあります。これらの無線は <i>location</i> 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 <i>frequency</i> 帯域内にあります。これらの無線は <i>location</i> にあります。    |

| AI 駆動型の問題 |                               |                                                                                                              |
|-----------|-------------------------------|--------------------------------------------------------------------------------------------------------------|
| カテゴリ      | 問題の名称                         | 概要                                                                                                           |
| 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 <i>frequency</i> 帯域内にあります。これらの無線は <i>location</i> 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 <i>frequency</i> 帯域内にあります。これらの無線は <i>location</i> にあります。 |

## MRE の問題

次の表に、MRE ワークフローを使用してトラブルシューティング可能な アシユアランス で検出される問題を示します。

| MRE の問題     |                            |                                                                                              |
|-------------|----------------------------|----------------------------------------------------------------------------------------------|
| カテゴリ        | 問題の名称                      | 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 | 有線クライアント認証に失敗しました。Dot1.x を使用するユーザーデバイス認証のエラーです。<br><br>(注) この問題は、単独の有線クライアントにのみ適用されます。       |
| オンボーディング    | 有線クライアント認証エラー - MAB エラー    | 有線クライアント認証に失敗しました。ユーザーデバイス認証が MAC 認証バイパスの問題により失敗しました。<br><br>(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しました。                                      |





## 第 12 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 (281 ページ)
- デバイスイベントの表示 (281 ページ)

## イベントダッシュボードの概要

イベントダッシュボードは、デバイス（ルーター、スイッチ、ワイヤレスコントローラ、AP）の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、アシュアランス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。ただし、5000 を超えるイベントがある場合、エクスポート機能は無効になります。

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。

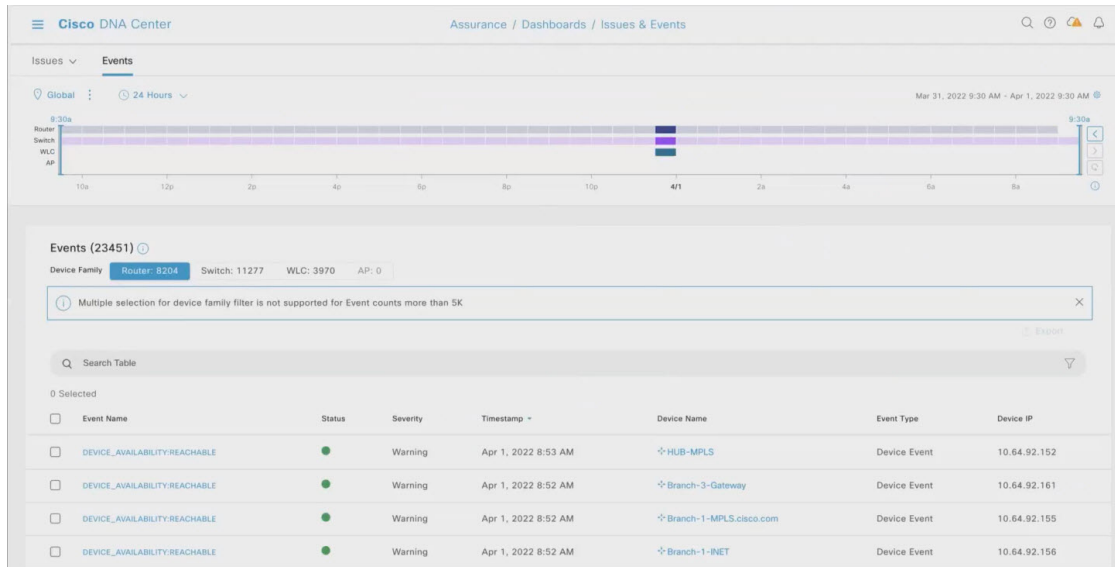
## デバイスイベントの表示

この手順を使用して、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を表示します。






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

[Events] ダッシュボードが開き、次の情報が表示されます。

図 27: Device Events ダッシュボード



### Device Events ダッシュボード

| アイテム                                                                                                    | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <ul style="list-style-type: none"> <li>上部のメニューバーで  <b>Global</b> 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。</li> <li>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、デバイス数と正常性パーセンテージを表示します。</li> <li>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。</li> <li>[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。</li> </ul> |
| <br>[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。 <ol style="list-style-type: none"> <li>[24 時間 (24 Hours)] ドロップダウンリストで、時間範囲 ([3 時間 (3 hours)]、[24 時間 (24 Hours)]、または [7 日間 (7 days)]) を選択します。</li> <li>[Start Date] と時刻、[End Date] と時刻を指定します。</li> <li>[Apply] をクリックします。</li> </ol> これにより、タイムラインの範囲が設定されます。                                                                                                                                                                                                                                                                                                        |

| Device Events ダッシュボード |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| タイムラインスライダ            | <p>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。</p> <p>色は、デバイスの種類を表します。</p> <ul style="list-style-type: none"> <li><span style="display: inline-block; width: 15px; height: 10px; background-color: #000080; margin-right: 5px;"></span> : ルータ</li> <li><span style="display: inline-block; width: 15px; height: 10px; background-color: #0000FF; margin-right: 5px;"></span> : スイッチ</li> <li><span style="display: inline-block; width: 15px; height: 10px; background-color: #008080; margin-right: 5px;"></span> : ワイヤレスコントローラ</li> <li><span style="display: inline-block; width: 15px; height: 10px; background-color: #808080; margin-right: 5px;"></span> : AP</li> </ul> <p>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のイベントが少ないことを示します。</p> |
| <b>Total Events</b>   | 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 [Family Type] で、[Router] タブ、[Switch] タブ、[Wireless Controller] タブ、または [AP] タブをクリックして、そのデバイスタイプのイベントのリストをテーブルに表示します。

| イベントの表             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Event Name</b>  | <p>イベントの名前。</p> <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Status</b>      | <p>デバイスのステータスです。</p> <p>色はイベントの重大度を表します。</p> <ul style="list-style-type: none"> <li><span style="display: inline-block; width: 10px; height: 10px; background-color: #FF0000; border-radius: 50%; margin-right: 5px;"></span> : エラー。</li> <li><span style="display: inline-block; width: 10px; height: 10px; background-color: #00FF00; border-radius: 50%; margin-right: 5px;"></span> : 警告。</li> <li><span style="display: inline-block; width: 10px; height: 10px; background-color: #0000FF; border-radius: 50%; margin-right: 5px;"></span> : 情報。</li> <li><span style="display: inline-block; width: 10px; height: 10px; background-color: #808080; border-radius: 50%; margin-right: 5px;"></span> : 使用できるデータがありません。</li> </ul> |
| <b>重大度</b>         | 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）。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Timestamp</b>   | イベントが発生した日付と時刻。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Device Name</b> | <p>イベントの影響を受けたデバイス名。</p> <p>デバイス名をクリックして、[Device 360] ウィンドウを開きます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>イベント タイプ</b>    | 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。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| イベントの表  |                |
|---------|----------------|
| アイテム    | 説明             |
| デバイス 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。

カードの中から、次のことができます。

- 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。
-





## 第 13 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 \(285 ページ\)](#)
- [センサーのプロビジョニング \(285 ページ\)](#)
- [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 \(291 ページ\)](#)
- [センサーの管理とバックホールの設定 \(299 ページ\)](#)
- [SCEP プロファイルの管理 \(304 ページ\)](#)
- [センサー主導テスト \(305 ページ\)](#)

## センサーとセンサー主導のテストについて

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

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

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

## センサーのプロビジョニング

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

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

(注) ソフトウェアリリース 1.3.1.2 よりも前の Cisco Aironet 1800s アクティブセンサーの場合は、センサーデバイスプロファイル **CiscoProvisioningSSID** を選択しないようにしてください。代わりに、バックホール用に独自の SSID を選択します。[バックホールの設定の管理 \(301 ページ\)](#) を参照してください。

Cisco ワイヤレス コントローラについては、[ワイヤレス コントローラのプロビジョニング SSID の有効化 \(286 ページ\)](#) を参照してください。

Cisco Catalyst ワイヤレス コントローラについては、[Cisco Catalyst ワイヤレスコントローラのシスコプロビジョニング SSID の有効化 \(287 ページ\)](#) を参照してください。

**ステップ 2** センサのバックホール設定を作成します。

『[バックホールの設定の管理 \(301 ページ\)](#)』を参照してください。

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

『[ワイヤレスまたはセンサー デバイスのプロビジョニング \(288 ページ\)](#)』を参照してください。

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

---

## ワイヤレス コントローラのプロビジョニング SSID の有効化

---

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

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

**ステップ 2** [Advanced] タブをクリックします。

[概要 (Summary) ] ページが表示されます。

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

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

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

**ステップ 5** [SSID] フィールドに「**TFTP**」と入力します。

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

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

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

**ステップ 9** [Apply] をクリックします。

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

## Cisco Catalyst ワイヤレスコントローラのシスコ プロビジョニング SSID の有効化

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

**ステップ 2** 左側のナビゲーションペインで、[設定 (Configuration)] > [クラウドサービス (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** [ネットワークアシュアランス (Network Assurance)] タブで、次の手順を実行します。

- a) [ネットワークアシュアランスの設定 (Network Assurance Configuration)] 領域で、[サービスステータス (Service Status)] トグルを [有効 (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 [ポリシータグ名 (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。  
[タグの管理 (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) [ポリシープロファイル (Policy Profile) ] ドロップダウンリストから、[CiscoSensorProvisioning] を選択します。
- g) ✓ をクリックします。
- h) [Save & Apply to Device] をクリックしてポリシータグを保存します。

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

## ワイヤレスまたはセンサー デバイスのプロビジョニング

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

### 始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『[Network Plug and Play Troubleshooting Guide for Cisco DNA Center](#)』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- ネットワーク階層内のサイトを定義します。『[ネットワーク階層の概要 \(46 ページ\)](#)』を参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。



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

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



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

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

**ステップ 1** メニューアイコン (☰) をクリックして、**[Provision] > [Plug and Play]**。

**ステップ 2** テーブル内のデバイスを表示します。

[フィルタ (Filter)] または [検索 (Find)] オプションを使用して、特定のデバイスを見つけることができます。

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

**ステップ 4** デバイス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。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。代わりに、サイトの定義やデバイスログイン情報の定義などの必須タスクを示すウィンドウが表示された場合は、[Add Site] をクリックしてサイトを定義し、[Add device credentials] をクリックしてデバイスログイン情報を定義する必要があります。これらは要求プロセスの前提条件であり、これらのタスクが完了したら、このウィンドウで [Refresh] をクリックしてデバイスの要求に戻ることができます。

**ステップ 5** (オプション) 必要に応じて、最初の列のデバイス名を変更します。

**ステップ 6** (オプション) 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP または ME (Mobility Express) を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、シスコワイヤレス コントローラ やセンサーデバイスには表示されません。

**ステップ 7** [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。AP デバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかのデバイスに割り当てるには、[Assign this

[Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

(注) Cisco DNA Center では、このサイトは AP PnP オンボーディング中に AP の場所として設定されません。[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。

**ステップ 8** [Next] をクリックします。

[Assign Configuration] ウィンドウが開きます。

**ステップ 9** (任意) テーブルに表示される列を変更するには、テーブル見出しの右端にある3つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

**ステップ 10** [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

- a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
- b) (任意) [デバイス名 (Device Name)] フィールドで、必要に応じてデバイス名を変更します。
- c) AP デバイスの場合、[Radio Frequency Profile] ドロップダウンリストで、デバイスに適用する無線周波数プロファイルを選択します。これは、1つのプロファイルをデフォルトとして指定した場合に設定できます。
- d) ワイヤレスコントローラ の場合、[Wireless Management IP]、[Subnet mask]、[Gateway]、[IP interface name]、また任意で [VLAN ID] の各フィールドに値を入力します。
- e) Mobility Express デバイスの場合は、[Wireless management IP]、[Subnet Mask]、および [Gateway] の各フィールドに値を入力します。
- f) ワイヤレスセンサーデバイスの場合、[Sensor Settings] ドロップダウンリストで、デバイスに適用するセンサーデバイスプロファイル (バックホール) を選択します。
 

(注) 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。
- g) 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。
- h) [Actions] 列の [他のデバイスに...を適用 (Apply ... to Other Devices)] をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

**ステップ 11** (オプション) ワイヤレスセンサーデバイスの場合、ソフトウェアイメージを割り当てるには、次の手順を実行します。

1. [Image] 列で、[Assign] をクリックします。
2. [Image] ドロップダウンリストから、ゴールデン ソフトウェア イメージを選択します。
3. [保存 (Save)] をクリックします。

**ステップ 12** デバイスが Cisco Catalyst 9800-CL ワイヤレスコントローラの場合は、[Configuration] 列の [Image] の横にある [Assign] をクリックし、次の手順を実行します。

- a) (オプション) [イメージ (Image)] ドロップダウンリストで、デバイスに適用するゴールデンソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが1つしかない場合は、そのイメージがデフォルトで選択されます。

b) [保存 (Save)] をクリックします。

**ステップ 13** 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスに[割り当て (Assign)] をクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

**ステップ 14** [Next] をクリックします。

[概要 (Summary)] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

**ステップ 15** 設定プレビューが成功したかどうかを確認するには、各デバイスの[Day-0 Config]列をチェックします。

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

**ステップ 16** [要求 (Claim)] をクリックします。

**ステップ 17** 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。

#### 次のタスク

ネットワーク設定を構成している場合は、デバイスでこれらの設定をプロビジョニングします。詳細については、[Cisco DNA Center ユーザガイド](#)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

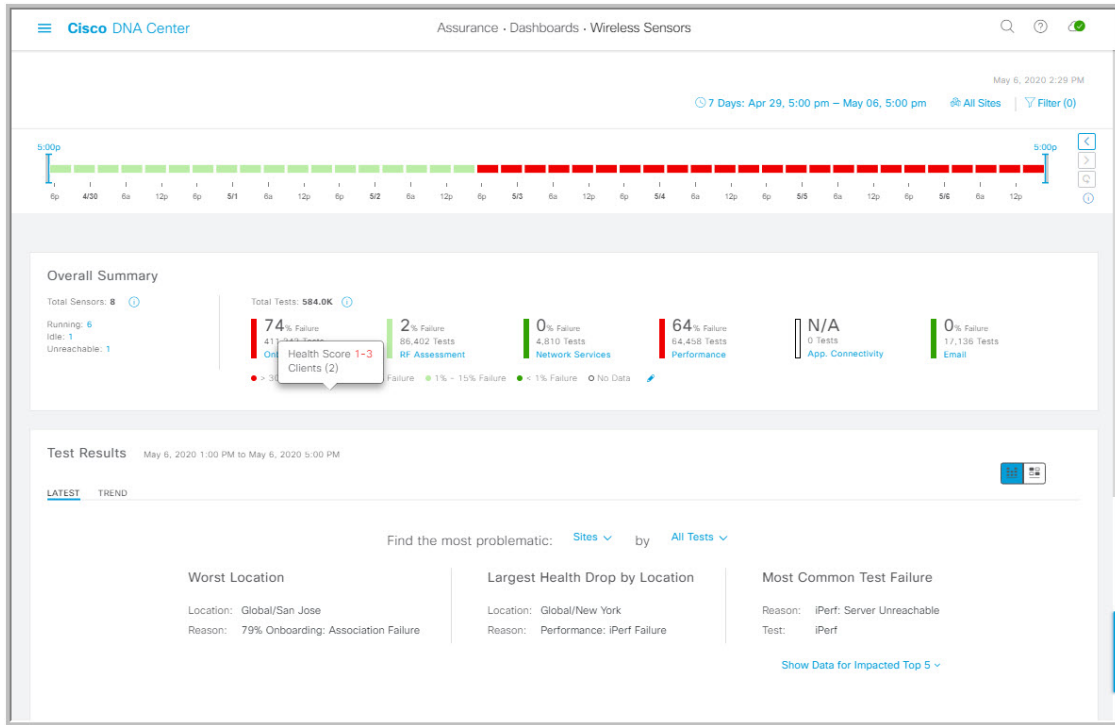
すべてのワイヤレスセンサーから受信したデータに基づくネットワーク正常性のグローバルビューを取得するには、次の手順を実行します。

#### 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 \(305 ページ\)](#) を参照してください。

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


図 28: [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                                                                                                                                                                                                                                                     |
| <br>時間範囲の設定 | ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 <ol style="list-style-type: none"> <li>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。</li> <li>[開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。</li> <li>[Apply] をクリックします。</li> </ol> |



| タイムラインエリア                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <br>階層ロケーションの設定 | ダッシュボードに表示するデータをネットワークのロケーションから選択できます。ダッシュボードにセンサーデータを表示するには、ネットワーク内のサイト、ビルディング、またはフロアのチェックボックスをオンにします。<br><br>(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                                                                                    | SSID および無線周波数帯域に基づいて、ダッシュボードに表示するデータを選択できます。<br><br>フィルタを追加するには、次の手順を実行します。 <ol style="list-style-type: none"> <li>1. [Filter] をクリックします。</li> <li>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。</li> <li>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。</li> <li>4. [Apply] をクリックします。</li> </ol> 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。 <ol style="list-style-type: none"> <li>1. [Filter] アイコンをクリックします。</li> <li>2. [Clear Filters] をクリックします。</li> </ol> |

**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せん。


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

| [Overall Health Summary] ダッシュレット |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [Total Sensors] エリア              | <p>ネットワーク内のすべてのセンサーとそのステータスの全体像が表示されます。センサーのステータスタイプは、次のとおりです。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [Unreachable] : センサーからハートビートが受信されませんでした。</li> </ul> <p>ステータスタイプの横にあるハイパーリンク番号をクリックすると、スライドインペインが開き、そのステータスのセンサーが表示されます。</p> <p>スライドインペインで [Name] カラムの下にあるセンサー名をクリックすると、そのセンサーの 360 度ビューが表示されます。「<a href="#">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 (297 ページ)</a>」を参照してください。</p> |

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

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

| [Test Results] ダッシュレット                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| [Latest] タブと [Trend] タブ                                                                                            | <p>これらのタブでは、ダッシュレットに表示するデータの範囲を定義します。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [Trend] : 過去 24 時間のデータが表示されます。</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|  [Heatmap View] と [Card View] トグル | <p>このトグルボタンで、ダッシュレットのビューを [Heatmap View] と [Card View] で切り替えることができます。</p> <p>デフォルトでは、[Heatmap View] が表示されます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|  [Heatmap View]                   | <p>次の統計カテゴリの上位 5 ランキングがダッシュレットの上部に表示されます。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [Most Common Test Failure] : テスト失敗率が最も高かったテストタイプ。</li> </ul> <p>各統計情報カテゴリの上位スポットのみが表示されます。[Show Data for Impact Top 5] をクリックすると、完全なランキングが表示されます。</p> <p>ランキングの下には、センサーテストエラーの結果がヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 色分けされたブロックをクリックすると、スライドインペインが開き、交差する部分のテスト結果に関する詳細が表示されます。</li> </ul> |

| [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。<br>データをソートするには、[Find the most problematic] エリアのドロップダウンリストを使用します。 |

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

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

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

[Sensor Dashboard] が表示されます。

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


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

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

- [Overall Summary] ダッシュレットで、ハイパーリンクされたテストカテゴリをクリックします。  
スライドインペインで、テーブルからセンサーのハイパーリンク名をクリックします。

- [Test Results] ダッシュレットで、ヒートマップから色分けされたボックスをクリックします。  
スライドインペインで、テーブルからセンサーのハイパーリンク名をクリックします。

センサーの360度ビューが表示されます。

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

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

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


イベントログの表示やダウンロードには、次の手順を実行します。

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

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

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

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

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

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

**テスト結果カテゴリ**

センサーテスト失敗の結果は、テスト対象の AP ごとにヒートマップでも表現されます。ヒートマップでは、テスト失敗率の重大度を示すために、ブロックが色分けされています。

- テストタイプ別にデータをソートするには、[Test Type] ドロップダウンリストを使用します。
- 特定の AP のヒートマップをフィルタ処理するには、検索フィールドを使用します。
- ブロックの上にカーソルを合わせると、テスト失敗の正確なパーセンテージ値が表示されます。
- [Latest] および [Trend] タブをクリックすると、カテゴリに表示されるデータの範囲が切り替わります。
  - [Latest] : ウィンドウの上部にあるタイムラインに、選択した時間枠のデータが表示されます。
  - [Trend] : 過去 24 時間のデータが表示されます。

### センサーパフォーマンスのトレンドカテゴリ

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

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

### ネイバー AP カテゴリ

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

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

(注) センサーは、30 分ごとにネイバー AP をスキャンします。

## センサーの管理とバックホールの設定

### ネットワーク内のセンサーの管理

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

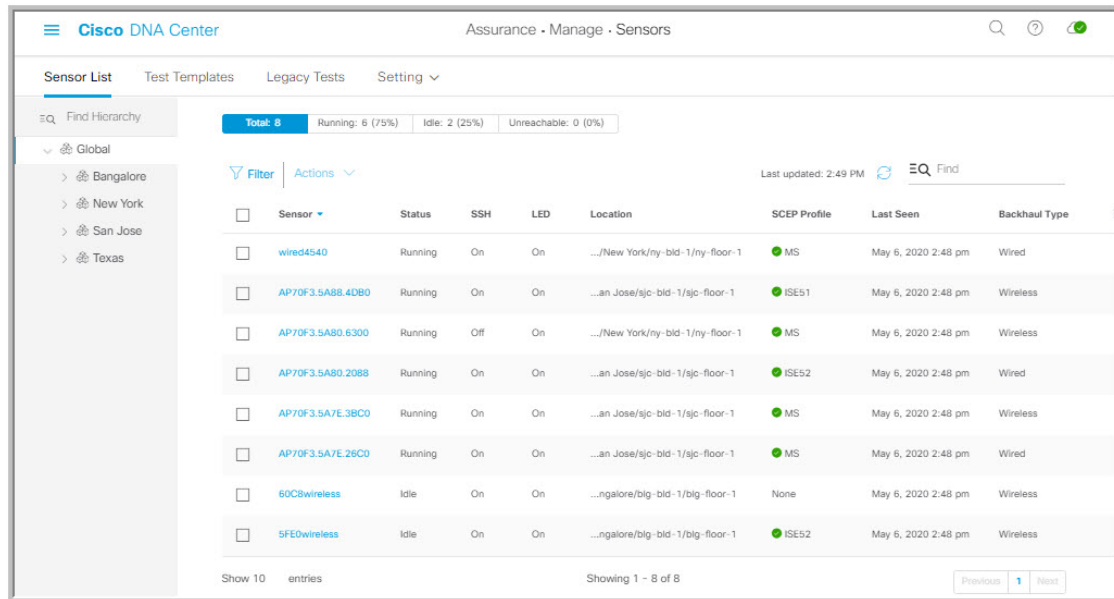
#### 始める前に

センサーがサイトに割り当てられていることを確認します。

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

[Sensor List] ウィンドウが表示されます。

図 29 : [Sensor List] ウィンドウ



**ステップ 2** 左側のペインで、表示するネットワーク階層を指定します。

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

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

**ステップ 4** テーブルに表示するデータをカスタマイズできます。

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

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

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

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



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

**ステップ 7** [Save] をクリックします。

**ステップ 8** センサーの名前を変更するには、次の手順を実行します。

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

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

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

## バックホールの設定の管理

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

永続的なワイヤレスバックホール接続の詳細については、[センサデバイスでの永続的なワイヤレスバックホール接続 \(303 ページ\)](#) を参照してください。

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

[Sensor List] ウィンドウが表示されます。

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

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

a) [Add Backhaul] をクリックします。

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

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

c) [Wired Backhaul] 領域で、次を設定します。

- [Level of Security] : 選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。

- **802.1x EAP** : Extensible Authentication Protocol (EAP) を有線 LAN で渡すために使用される規格。
- **Open** : セキュリティまたは認証は使用されません。

- [EAP Method] : [802.1x EAP] を選択した場合は、ドロップダウンリストからユーザ認証に次のいずれかの EAP 方式を選択する必要があります。

- [EAP-FAST] : 指定されたフィールドにユーザ名とパスワードを入力します。
- [PEAP-MSCHAPv2] : 指定されたフィールドにユーザ名とパスワードを入力します。
- [EAP-TLS] : [Enroll Using Certificate Bundle] または [Enroll Using SCEP] を選択します。

[Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

- [PEAP-TLS] : [Enroll Using Certificate Bundle] または [Enroll using SCEP] を選択します。

[Enroll Using Certificate Bundle] を選択した場合は、[Certificate Bundle] の下にあるドロップダウン矢印をクリックし、[+ Add New Certificate Bundle] をクリックして、ユーザ名と証明書バンドルパスワードを入力します。

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

- [Level of Security] : 選択した SSID で使用されている暗号化と認証タイプが表示されます。使用可能なセキュリティのオプションは次のとおりです。

- [WPA2 Enterprise] : 拡張可能認証プロトコル (EAP) (802.1x) を使用してより高レベルのセキュリティを実現し、リモート RADIUS サーバでネットワークユーザを認証および承認します。
- [WPA2-Personal] : パスフレーズまたは事前共有キー (PSK) を使用して、良好なセキュリティを実現します。ワイヤレスネットワークにアクセスするパスキーがあれば誰でも使用できます。

[WPA2パーソナル (WPA2 Personal)] を選択した場合は、[パスフレーズ (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) [保存 (Save) ] をクリックします。

**ステップ 4** 既存のバックホール設定を編集するには、次の手順を実行します。

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

**ステップ 5** バックホール設定を削除するには、次の手順を実行します。

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

---

## センサデバイスでの永続的なワイヤレスバックホール接続

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

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

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

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

## SCEP プロファイルの管理

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

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

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

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

a) **[Add SCEP Profiles]** をクリックします。

**[Create SCEP Profile]** ウィンドウが表示されます。

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

- **[SCEP Profile Name]** : SCEP プロファイルの名前を入力します。

- **[URL Base]** : 有効なサーバーを入力します。

(注) **ISE** の場合は、次のように入力します。

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

**Microsoft CA** の場合は、次のように入力します。

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

- **[Common Name]** : 有効な名前を入力します。

- **[State]**

- **[Country Code]**

- **[Locality]**

- **[Organization]**

- **[Organization Unit]**

- **[Email]**

- **[Sever certificate fingerprint]**

c) **[Save]** をクリックします。

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

a) SCEP プロファイルの横にあるチェックボックスをオンにします。

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

**ステップ 5** SCEP プロファイルを削除するには、次の手順を実行します。

a) SCEP プロファイルの横にあるチェックボックスをオンにします。

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

## センサー主導テスト

### テンプレートを使用したセンサー主導テストの作成と実行

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

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

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

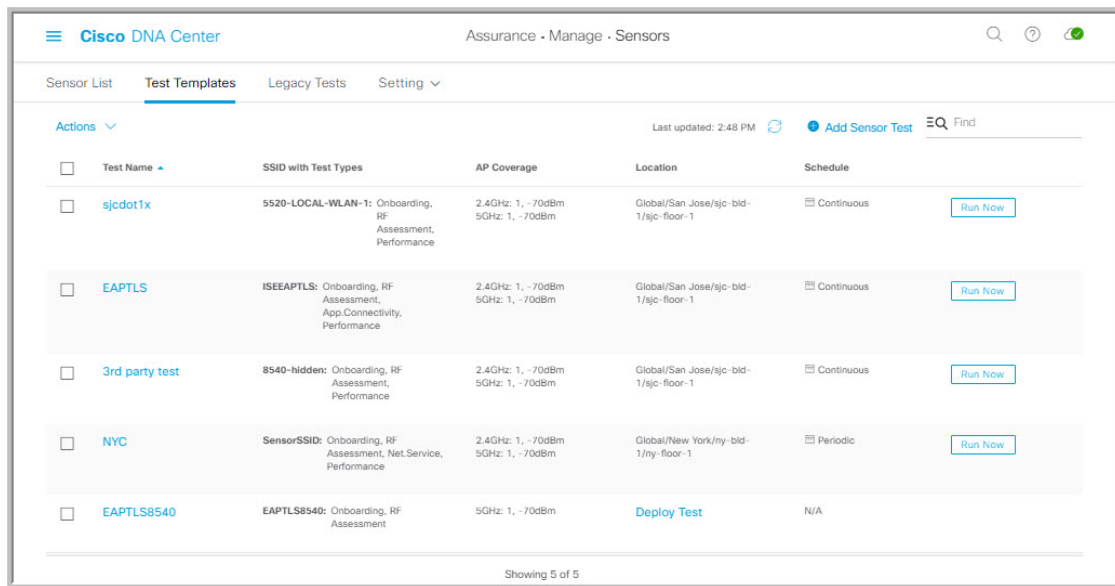
#### 始める前に

- Cisco Aironet 1800s アクティブ センサーを使用してセンサー主導のテストを実行している場合、必ず PnP を使用してセンサーをプロビジョニングし、[インベントリ (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 \(285 ページ\)](#) を参照してください。
- センサーテストテンプレートを再起動すると、そのテンプレート上のすべてのセンサーで同時にテストの実行が開始されるため、結果のグラフに周期的なパターンが現れることに注意してください。

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

**ステップ 2** [Test Templates] タブをクリックします。  
[Test Templates] ウィンドウが表示されます。

図 30: [Test Templates] ウィンドウ



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

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

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

ステップ5 [Next] をクリックします。

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

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

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

**ステップ 8** 次のプロキシ設定を指定します。

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

**ステップ 9** [Next] をクリックします。

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

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

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

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

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

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

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

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

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

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

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

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

#### **iPerf3 の制限事項**

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

- 特定の iPerf3 サーバーにおいて、2つのセンサーを同じポートに同時に接続することはできません。
- 「iPerf: サーバーがビジー状態 (iPerf: Server Busy)」エラーメッセージは、iPerf3 テストを実行しているセンサーの数に対応する十分な iPerf3 インスタンスがないことを示します。

この問題を解決するには、次のいずれかを実行します。

- iPerf3 サーバーインスタンスを追加します。これを行うには、既存のサーバーで iPerf3 テストをサポートするポートを拡張します。
- iPerf3 テストを実行するように設定されているセンサーの数を減らします。これを行うには、iPerf3 テスト用に別個のテンプレートを作成します。

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

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

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

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

(注) センサーテストの最大ファイルサイズは 5 MB です。

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

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

**ステップ 11** [Next] をクリックします。

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

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

(注) 最大 5 つの AP を選択できます。

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

**ステップ 13** [Next] をクリックします。



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

## センサー主導テストの管理

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

### 始める前に

センサー主導テストのテンプレートを作成します。[テンプレートを使用したセンサー主導テストの作成と実行 \(305 ページ\)](#) を参照してください。

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

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

[Test Templates] ウィンドウが表示されます。

図 31 : [Test Templates] ウィンドウ

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

**ステップ 3** テストテンプレートを複製するには、次の手順を実行します。

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

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

**ステップ 4** テストテンプレートを削除するには、次の手順を実行します。

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

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

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

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

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

---





## 第 14 章

# Wi-Fi 6E および 6 の対応状況のモニター

- [Wi-Fi 6E および 6 の対応状況とその利点について \(313 ページ\)](#)
- [Wi-Fi 6E および 6 ネットワークの対応状況の確認 \(314 ページ\)](#)

## Wi-Fi 6E および 6 の対応状況とその利点について

Wi-Fi 6E および 6 の対応状況機能を使用して、次のことを判断できます。

- Wi-Fi 6E および 6 対応クライアントの割合。
- Wi-Fi 6E および 6 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 および 6 ネットワークのメリットを最大限に活用するためのアクションに関する推奨事項が提供されます。

これらの推奨事項を提供するため、Cisco DNA Center は次の手順を実行します。

- 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、Cisco DNA 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 および 6 に対応しているかを判別します。
- 無線 LAN の設定と、Wi-Fi 6E および 6 の機能が有効かどうかを判断します。



(注) 特定の条件下では、AP プラットフォームの機能に関係なく、Wi-Fi 6E ワイヤレスクライアントの遅延または通信時間効率のデータが、Wi-Fi 6 またはレガシー Wi-Fi よりも最適でない場合があります。たとえば、次の場合、Wi-Fi 6E は最適ではない可能性があります。

- 非 Wi-Fi 6E AP よりも大幅に多くのクライアントが Wi-Fi 6E AP に接続されている。
- 非 Wi-Fi 6E 環境よりも Wi-Fi 6E 環境で、貧弱な RF 設計による干渉が多い。
- Wi-Fi 6E に接続されているクライアントが、信号強度 (RSSI) が弱い場所にいる。

前述のシナリオは、従来の Wi-Fi に対する Wi-Fi 6E にも適用されます。

## Wi-Fi 6E および 6 ネットワークの対応状況の確認

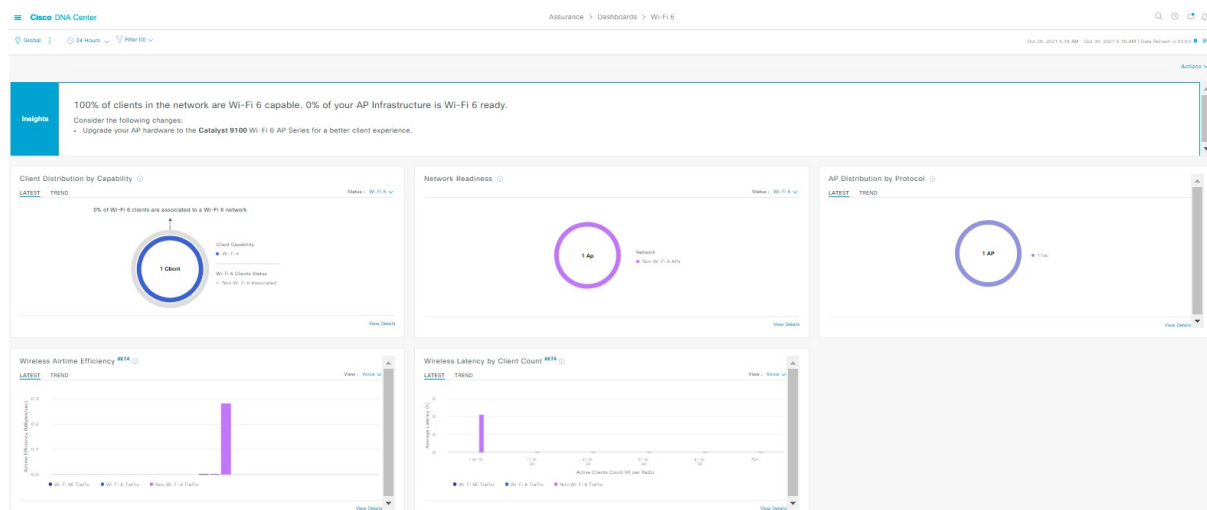
Wi-Fi 6E および Wi-Fi 6 ネットワークの対応状況を確認するには、この手順を使用します。

### 始める前に





アシュアランスを設定します。「[基本的な設定のワークフロー \(15 ページ\)](#)」を参照してください。

**ステップ 1** メニューアイコン (☰) をクリックして、アシュアランス > [Wi-Fi 6] の順に選択します。

[Wi-Fi 6] ダッシュボードが表示されます。



**ステップ 2** 次の機能には、上部のメニューバーを使用します。

| アイテム                                                                                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <br>[Location] ペイン | クリックすると、次のアイコンが表示されます。 <ul style="list-style-type: none"> <li>  : [Hierarchical Site View] テーブルを表示するには、このトグルボタンをクリックします。サイト内のワイヤレスクライアントとワイヤレスネットワークデバイスの割合を示します。特定の建物の情報を表示するには、ドロップダウンリストから [Building View] を選択します。           </li> <li>  : このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、提示されるネットワーク サイトは問題の重大度に従って色分けされています。           </li> </ul> |
| <br>時間範囲の設定        | ダッシュボードで指定された時間範囲内のデータを表示できるようにします。次の手順を実行します。 <ol style="list-style-type: none"> <li>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。</li> <li>[開始日付 (Start Date) ]と時刻、[終了日付 (End Date) ]と時刻を指定します。</li> <li>[Apply] をクリックします。</li> </ol>                                                                                                                                                                                                                                                                                                  |
| [Filter] アイコン                                                                                       | [SSID] および [Band] オプションが含まれます。ドロップダウンリストから SSID と帯域周波数の隣にあるチェックボックスをオンにして選択し、[Apply] をクリックします。選択した内容に応じて、ダッシュボードの情報が更新されます。                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [Actions] ドロップダウンリスト                                                                                | 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。<br><br>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。 <a href="#">ダッシュレットの位置の変更 (340 ページ)</a> および <a href="#">カスタム ダッシュボードの作成 (335 ページ)</a> を参照してください。                                                                                                                                                                                                                                                                                                 |

**ステップ 3** ネットワークに関する情報を取得するには、[Insights] 領域を使用します。次の情報を出力します。

- Wi-Fi 6E および Wi-Fi 6 対応クライアントの割合。
- Wi-Fi 6E および 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 6E および Wi-Fi 6 ネットワークのメリットを最大限に活用するために実行できるアクションについての推奨事項が提供されます。

**ステップ 4** [Client Distribution By Capability] ダッシュレットを使用して、Wi-Fi 6E と Wi-Fi 6 間のクライアントの分布機能を比較し、Wi-Fi 6E または 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します。

クライアントが関連付けられている AP に基づいて、クライアントは Wi-Fi 6 機能で動作する場合もあれば、それより低い機能で動作することもあります。たとえば、11ac AP に関連付けられた Wi-Fi 6 クライアントは、11ac クライアントとして機能します。

#### [Client Distribution By Capability] ダッシュレット

[Wi-Fi 6E] および [Wi-Fi 6] のステータスに基づいて、ワイヤレスネットワークに関連付けられているすべてのクライアントを表示できます。

このダッシュレットには、次のタブが含まれます。

- [Latest] : デフォルトで表示されます。
  - 円の**外側**のセグメントは、Wi-Fi 6E、Wi-Fi 6 および非 Wi-Fi 6 ネットワークに参加している（関連付けられている）Wi-Fi 6E 対応クライアントの数を示します。
  - 円の**外側**のセグメントは、Wi-Fi 6 および非 Wi-Fi 6 ネットワークに参加している（関連付けられている）Wi-Fi 6 対応クライアントの数を示します。
  - **内側**の円は、ネットワーク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機能します。
    - [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は、選択したステータス（[Wi-Fi 6E] または [Wi-Fi 6]）に基づき一定の時間範囲で Wi-Fi 6E、Wi-Fi 6 または非 Wi-Fi 6 プロトコルに関連付けられているクライアントの数を示します。

チャートにカーソルを重ねると、クライアントの合計数と指定された日時におけるクライアントのプロトコルが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



**ステップ 5** [Network Readiness] ダッシュレットを使用して、Wi-Fi 6E および Wi-Fi 6 に対応し、Wi-Fi 6E または Wi-Fi 6 モードで動作するように設定（有効化）されている AP の数を確認します。

#### [Network Readiness] ダッシュレット

[Wi-Fi 6E] または [Wi-Fi 6E] のステータスに基づいて、ワイヤレスネットワークに関連付けられているすべてのクライアントを表示できます。

- 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、次の条件に従って 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 6** [AP Distribution by Protocol] ダッシュレットを使用して、Wi-Fi 標準（Wi-Fi 6E、Wi-Fi 6 および 11 ac/n/a/b/g）をサポートするハードウェア機能をもつ AP の数を確認します。

**[AP Distribution by Protocol] ダッシュレット**

このダッシュレットには、次のタブが含まれます。

- [Latest] : デフォルトで表示されます。Wi-Fi 6E、Wi-Fi 6 (11ax) プロトコルをサポートする AP の数と、非 Wi-Fi 6 (11ac/n/a/b/g) プロトコルをサポートする AP の数を示します。
  - [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は、一定の時間範囲でさまざまなプロトコル (Wi-Fi 6E、Wi-Fi 6 または非 Wi-Fi 6) に関連付けられている AP の数を示します。

チャートにカーソルを重ねると、AP の合計数と指定された日時における AP のプロトコルが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

**ステップ 7** [Wireless Airtime Efficiency] ダッシュレットを使用して、アクセスカテゴリ (音声、ビデオ、ベストエフォート、バックグラウンド) ごとに、Wi-Fi 6E、Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均通信時間効率を比較します。

**[Wireless Airtime Efficiency] ダッシュレット**

[Voice]、[Video]、[Best Effort]、[Background]、および [All] のアクセスカテゴリに従って、ワイヤレス通信時間効率を表示できます。デフォルトは [Voice] です。

このダッシュレットには、次のタブが含まれます。

- [Latest] : デフォルトで表示されます。棒グラフでは、選択したアクセスカテゴリにおける Wi-Fi 6E、Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均通信時間効率（1 ミリ秒あたりのバイト数）を比較できます。

AP の無線が、類似した RF 状態の他のネットワークよりも少ない通信時間（マイクロ秒）でより多くのトラフィック（クライアントに送信されるバイト数）を送信できる場合は、スペクトルが効率的に使用されています。効率的なネットワークでは、より多くのビデオまたは音声コールを処理できる可能性があります。

トラフィックは次のように分類されます。

- Wi-Fi 6E トラフィックは、Wi-Fi 6E の AP から Wi-Fi 6E として関連付けられているクライアントに送信されるトラフィックです。
- Wi-Fi 6 トラフィックは、Wi-Fi 6 の AP から Wi-Fi 6 として関連付けられているクライアントに送信されるトラフィックです。
- 非 Wi-Fi 6 トラフィックは以下を集約したものです。
  - Wi-Fi 6 AP から非 Wi-Fi 6 対応クライアントへのトラフィック。
  - 非 Wi-Fi 6 AP から非 Wi-Fi 6 対応クライアントへのトラフィック。
  - 非 Wi-Fi 6 AP から Wi-Fi 6 対応クライアントへのトラフィック。

(注) Wi-Fi 6 対応クライアントは、非 Wi-Fi 6 AP に接続すると非 Wi-Fi 6 モードで動作します。

- [Trend] : [Trend] タブをクリックすると、トレンドチャートが表示されます。この色分けされたトレンドチャートは、一定の時間範囲でさまざまなワイヤレス ネットワーク モード（Wi-Fi 6E、Wi-Fi 6 または非 Wi-Fi 6）に関連付けられているクライアントの数を示します。

チャートにカーソルを重ねると、クライアントの合計数と指定された日時におけるクライアントのプロトコルが表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

**ステップ 8** [Wireless Latency by Client Count] ダッシュレットを使用して、アクセスカテゴリ（音声、ビデオ、ベストエフォート、バックグラウンド）ごとに、Wi-Fi 6E、Wi-Fi 6 トラフィックと非 Wi-Fi 6 トラフィックの平均ワイヤレス遅延を比較します。

クライアント数が多い AP 無線は、通常、類似した RF 条件下のクライアント数が少ない無線と比べて遅延が多くなります。

**[Wireless Latency by Client Count] ダッシュレット**

[Voice]、[Video]、[Best Effort]、[Background] トラフィックのワイヤレス遅延を表示できます。デフォルトは [Voice] です。

このダッシュレットには、次のタブが含まれます。

- [Latest] : デフォルトで表示されます。同様の数の「アクティブな」クライアントに対応する Wi-Fi 6E、Wi-Fi 6 および非 Wi-Fi 6 AP 無線間の平均ワイヤレス遅延を比較できます。ワイヤレス遅延は、パケットが AP からクライアントに正常に送信されるまでにかかる時間（マイクロ秒）で測定されます。

(注) アクティブなクライアント数には、単に関連付けられたクライアントではなく、特定のアクセスカテゴリのトラフィックをアクティブに送信しているクライアントが含まれます。

- [Trend] : [Trend] タブをクリックすると、トレンドチャートが表示されます。トレンドチャートには、すべてのアクセスカテゴリの平均ワイヤレス遅延が表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。



## 第 15 章

# Power over Ethernet の監視

- [PoE について \(321 ページ\)](#)
- [PoE テレメトリの設定ワークフロー \(321 ページ\)](#)
- [PoE テレメトリに使用するデバイスでの NETCONF の設定 \(323 ページ\)](#)
- [PoE テレメトリのテレメトリ設定の更新 \(325 ページ\)](#)
- [ネットワーク内の PoE 対応デバイスの監視 \(326 ページ\)](#)

## PoE について

Cisco DNA Center Power over Ethernet (PoE) を使用してネットワーク内の PoE 対応デバイスをモニターできます。また、PoE を供給するスイッチの電源の概要がモニターされ、スイッチの電力バジェット、使用済み電力、残り電力、電力使用状況などの情報が提供されるため、スイッチの割り当て済み電力と電力負荷を表示できます。

## PoE テレメトリの設定ワークフロー

アシュアランスで PoE テレメトリと分析を有効にするには、必要な設定タスクを実行する必要があります。基本的な設定ワークフローのタスクは次のとおりです。

1. PoE テレメトリに使用するネットワークデバイスで NETCONF を設定します。  
詳細については、「[PoE テレメトリに使用するデバイスでの NETCONF の設定 \(323 ページ\)](#)」を参照してください。
2. Cisco DNA Center でテレメトリ設定を更新します。  
詳細については、「[PoE テレメトリのテレメトリ設定の更新 \(325 ページ\)](#)」を参照してください。

### 設定ワークフロー

PoE テレメトリの設定ワークフローは、Cisco DNA Center のソフトウェアバージョンと設定、および PoE テレメトリをサポートするネットワークデバイスによって異なります。

Cisco DNA Center の新規インストールの場合は、次の表を参照してください。

| Cisco DNA Center の新規インストール                                                                                                           |                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| ネットワーク デバイス設定                                                                                                                        | 必要な設定タスク                                                                                                                 |
| <ul style="list-style-type: none"> <li>IOS XE のバージョンが 16.12.3s である。</li> <li>NETCONF が無効になっている。</li> </ul>                           | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| <ul style="list-style-type: none"> <li>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。</li> <li>NETCONF が無効になっている。</li> </ul> | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| <ul style="list-style-type: none"> <li>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。</li> <li>NETCONF が有効になっている。</li> </ul> | <ol style="list-style-type: none"> <li>1. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol>                                    |

以前のリリースから Cisco DNA Center にアップグレードする場合は、次の表を参照してください。

| 以前のリリースからのアップグレード                                                                                                                    |                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| ネットワーク デバイス設定                                                                                                                        | 必要な設定タスク                                                                                                                 |
| <ul style="list-style-type: none"> <li>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。</li> <li>NETCONF が無効になっている。</li> </ul> | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| <ul style="list-style-type: none"> <li>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。</li> <li>NETCONF が有効になっている。</li> </ul> | <ol style="list-style-type: none"> <li>1. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol>                                    |
| <ul style="list-style-type: none"> <li>IOS XE のバージョンが 16.12.3s である。</li> <li>NETCONF が無効になっている。</li> </ul>                           | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| <ul style="list-style-type: none"> <li>IOS XE のバージョンが 16.12.3s である。</li> <li>NETCONF が有効になっている。</li> </ul>                           | <ol style="list-style-type: none"> <li>1. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol>                                    |

PoE テレメトリをサポートするネットワークデバイスのインベントリに変更がある場合は、次の表を参照してください。

| ネットワークデバイスのインベントリの変更                     |                                                                                                                          |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| ネットワークデバイスの変更                            | 必要な設定タスク                                                                                                                 |
| インベントリからデバイスを削除して再度追加する。Cisco DNA Center | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| インベントリに新しいデバイスを追加する。Cisco DNA Center     | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |
| インベントリの交換用デバイスを使用する。Cisco DNA Center     | <ol style="list-style-type: none"> <li>1. デバイスで NETCONF を有効にします。</li> <li>2. Cisco DNA Center でテレメトリ設定を更新します。</li> </ol> |

## 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

Cisco DNA Center とネットワークデバイスの設定によっては、PoE テレメトリを設定するためにこの手順を実行する必要がない場合もあります。詳細については、「[PoE テレメトリの設定ワークフロー \(321 ページ\)](#)」を参照してください。

**ステップ 1** 既存のネットワークデバイスの NETCONF ポートを設定します。

- a) メニューアイコン (☰) をクリックして、**[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) メニューアイコン (☰) をクリックして、[Tools] > [Template Editor] の順に選択します。

[Template Editor] ウィンドウが表示されます。


b) 左ペインで  アイコンをクリックし、[Create Project] を選択します。

c) [Name] フィールドに、プロジェクトの名前を入力します。

d) [Add] をクリックします。

プロジェクトが [Template Editor] の左ペインに追加されます。

**ステップ 3** NETCONF 設定のプロジェクトでテンプレートを作成します。

a) 左ペインで、プロジェクトの右にある  アイコンにカーソルを合わせ、[Add Template] を選択します。

b) [Name] フィールドに、テンプレートの名前を入力します。

c) [Device Type (s)] フィールドで、[Edit] をクリックします。

d) スイッチとハブを追加するには、[Switches and Hubs] のチェックボックスをオンにしてテンプレートを適用します。

(注) スイッチの正確なモデルを指定する場合は、[Switches and Hubs] を展開し、特定のスイッチモデルのチェックボックスをオンにします。

e) [Back to Add New Template] をクリックします。

f) [Software Type] ドロップダウンリストをクリックし、[IOS-XE] を選択します。

g) [Add] をクリックします。

テンプレートが作成されて表示されます。

**ステップ 4** テンプレートの内容を追加します。

a) テンプレートで次のように入力します。

```
netconf-yang
```

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

テンプレートの内容が保存されます。

c) [Actions] ドロップダウンリストから、[Commit] を選択します。

d) [Commit Note] テキストボックスに、メモを入力します。

e) [Commit] をクリックします。

**ステップ 5** ネットワークプロファイルを作成してテンプレートを関連付けます。

a) メニューアイコン (☰) をクリックして、[Design] > [Network Profile] の順に選択します。



[Network Profiles] ウィンドウが表示されます。

- b) [+Add Profile] をクリックし、[Switching] を選択します。
- c) [Profile Name] フィールドに、ネットワークプロファイルの名前を入力します。
- d) [Day-N Templates] タブをクリックします。
- e) [Add] をクリックします。
- f) [Device Type] ドロップダウンリストから、[Switches and Hubs] を選択します。
- g) [Template] ドロップダウンリストから、手順 3 で作成したテンプレートを選択します。
- h) [Save] をクリックします。

ネットワークプロファイルが作成され、[Network Profiles] ウィンドウに表示されます。

**ステップ 6** ネットワークプロファイルのサイトを割り当てます。

- a) [Sites] 列で、[Assign Site] をクリックします。
- b) ネットワークデバイスが割り当てられているサイトのチェックボックスをオンにします。
- c) [Save] をクリックします。

**ステップ 7** NETCONF 設定をネットワークデバイスにプロビジョニングします。

- a) メニューアイコン (☰) をクリックして、[Provision] > [Inventory] の順に選択します。  
[Inventory] ウィンドウが表示されます。
- b) PoE テレメトリのネットワークデバイスのチェックボックスをオンにします。
- c) [Actions] ドロップダウンリストから、[Provision] > [Provision Device] の順に選択します。
- d) [Assign Site] ステップで、[Next] をクリックします。
- e) [Advanced Configuration] ステップで、[Provision these templates even if they have been deploy before] チェックボックスをオンにします。
- f) [Next] をクリックします。
- g) [Summary] ステップで、[Deploy] をクリックします。
- h) [Apply] をクリックします。

プロビジョニングが開始され、NETCONF 設定がネットワークデバイスにプッシュされます。

---

## PoE テレメトリのテレメトリ設定の更新

この手順では、Cisco DNA Center でテレメトリ設定を更新する方法を示します。これは、NETCONF ポートを設定し、PoE テレメトリに使用するネットワークデバイスに NETCONF 設定をプッシュした後に必要な手順です。

### 始める前に

PoE テレメトリ用に設定するネットワークデバイスで NETCONF ポートが確立され、NETCONF が適切に設定されていることを確認します。詳細については、「[PoE テレメトリに使用するデバイスでの NETCONF の設定 \(323 ページ\)](#)」を参照してください。

---

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

[Inventory] ウィンドウが表示されます。

**ステップ 2** PoE テレメトリ用に設定されているネットワークデバイスのチェックボックスをオンにします。

**ステップ 3** [Actions] ドロップダウンリストから、**[Telemetry] > [Update Telemetry Settings]** の順に選択します。

**ステップ 4** [Force Configuration Push] チェックボックスをオンにします。

(注) このオプションを選択すると、設定の変更がデバイスにプッシュされます。

**ステップ 5** [Next] をクリックします。

**ステップ 6** 次のオプションボタンをクリックして、テレメトリ設定を更新するスケジュールを設定します。

- [Now] : テレメトリ設定をすぐに更新するには、このオプションを選択します。
- [Later] : タスクを別の時間にスケジュールするには、このオプションを選択します。日付と時刻を指定します。

**ステップ 7** [Apply] をクリックします。

---

## ネットワーク内の PoE 対応デバイスの監視

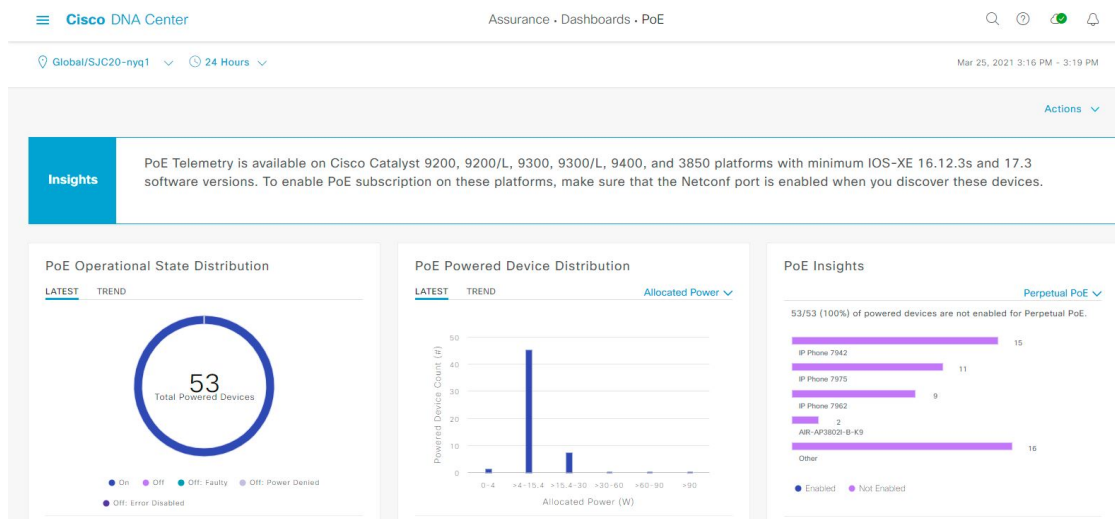
ネットワーク内の PoE 対応デバイスのグローバルビューを取得するには、次の手順を使用します。

---

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



[PoE] ダッシュボードが表示されます。



図 32: [PoE] ダッシュボード



**ステップ 2** 上部のメニューバーにあるロケーションオプション (📍 Global) をクリックして、ロケーションペインを表示します。

ロケーションペインには、次の機能があります。

| ロケーションオプション                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|  トグルボタン<br>[List View] | <p>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。</p> <p>ドロップダウンリストをクリックして、次のオプションを選択できます。</p> <ul style="list-style-type: none"> <li>• [Hierarchical Site View] : リストをサイトレベルで並べ替えます。</li> </ul> <p>[Apply to Page Location] 列で特定のサイトまたはビルディングの [Apply] をクリックすると、そのロケーションのデータのみが [Network] ダッシュボードに表示されます。</p> <ul style="list-style-type: none"> <li>• [Building View] : リストをビルディングレベルで並べ替えます。</li> </ul> <p>[Apply to Page Location] 列で特定のビルディングの [Apply] をクリックすると、そのビルディングのデータのみが [Network] ダッシュボードに表示されます。</p> |
|  トグルボタン<br>[Map View]  | <p>このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、地理的ロケーションに基づいたネットワーク正常性マップで表示されます。デフォルトでは、提示されるネットワークサイトは問題の重大度に従って色分けされています。</p>                                                                                                                                                                                                                                                                                                                                                                                             |

| ロケーションオプション                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <br>[Topology]ツール | <p>このアイコンをクリックすると、[Topology]ツールが開きます[Topology] ウィンドウには次のビューがあります。</p> <ul style="list-style-type: none"> <li>• <b>[Geographical View]</b> : このトグルボタンをクリックすると、ネットワークが地理的マップで表示されます。 </li> </ul> <p>ロケーションにカーソルを合わせると、正常なデバイスの割合が表示されます。</p> <ul style="list-style-type: none"> <li>• <b>[Topology View]</b> : このトグルボタンをクリックすると、ネットワークにおけるコンポーネントの接続状況を示すトポロジが表示されます。</li> </ul> <p>デバイスにカーソルを重ねると、デバイスロール、IP アドレス、ソフトウェアバージョンなどのデバイス情報が表示されます。デバイスの 360 度ビューを取得するには、[View Details 360] をクリックします。</p> |

**ステップ 3** 上部のメニューバーにある時間範囲設定 (🕒) をクリックして、ダッシュボードに表示するデータの時間範囲を指定します。

- 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。
- [開始日付 (Start Date)] と時刻、[終了日付 (End Date)] と時刻を指定します。
- [Apply] をクリックします。

**ステップ 4** 上部のメニューバーにある [Actions] ドロップダウンリストをクリックして、次の機能を実行できます。

- **[Export Dashboard]** : PoE ダッシュボードを PDF 形式にエクスポートできます。[Export Dashboard] をクリックしてプレビュー ページを表示し、[Save] をクリックします。
- **[Edit Dashboard]** : ダッシュボードの表示をカスタマイズできます。 [ダッシュレットの位置の変更 \(340 ページ\)](#) および [カスタム ダッシュボードの作成 \(335 ページ\)](#) を参照してください。

**ステップ 5** 次の機能には、PoE ダッシュレットを使用します。

### PoE AP 電力モードの分布

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 ~ 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 ~ 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

### PoE 動作状態の分布

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 ~ 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 ~ 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

**PoE 受電デバイスの分布**

現在 PoE を使用しているデバイスのうち、特定の基準に当てはまるデバイスの割合が表示されます。ドロップドロップリストを使用して、次の基準を指定します。

- 割り当て済み電力
- 受電デバイスクラス

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で [24 hours] を選択した場合、トレンドチャートには 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

(注) 表示されるデータポイントは、対応する 10 分または 1 時間の開始時刻です。たとえば、10:00 ~ 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 ~ 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

### 電力負荷の分布

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 ~ 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 ~ 11:00 の間に受信されたデータは、10:00 のタイムスタンプで表示されます。このデータポイントは、対応するウィンドウの終了後に使用可能になります。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下に表示されるテーブルのデータを更新できます。

### PoE インサイト

現在 PoE を使用しているデバイスのうち、次の PoE テクノロジーをサポートするように設定されているデバイスや IEEE に準拠しているデバイスの割合が表示されます。

- 無停止型 POE
- 高速 PoE
- IEEE 準拠
- UPOE+

ドロップダウンリストを使用して、特性を選択します。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、チャートの下のテーブルに表示されるデータを更新できます。

**PoE 電力割り当て**

現在 PoE を使用しているデバイスの合計電力使用量が表示されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。円グラフには、合計電力使用量の [Consumed Power] と [Remaining Power] がワット単位で表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で 24 時間を選択した場合、トレンドチャートには電力使用の 24 時間の範囲全体で 10 分のデータポイントが表示されます。
- 時間範囲の設定で 24 時間を超える時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの色付きセグメントまたは対応する凡例をクリックすると、一定期間におけるデバイスの電力使用量の状況を表示できます。

水平バーとして表示されるデータを選択して、電力使用量、デバイスロール、および場所に基づいて進行中のテーブルをフィルタ処理できます。

**PoE ポートの可用性**

PoE の電力負荷に基づいてポートの可用性が表示されます。

[Latest] タブには、10 分間のスナップショットビューが表示されます。

[Trend] タブには、次の情報が表示されます。

- 時間範囲の設定で 24 時間以下の時間を選択した場合、トレンドチャートには、時間範囲全体に対して 1 時間のデータポイント（10 分のデータから集約）が表示されます。
- 時間範囲の設定で 7 日間を選択した場合、トレンドチャートには、時間範囲全体に対して 12 時間のデータポイント（1 時間のデータから集約）が表示されます。

[View Details] をクリックすると、追加の詳細情報を記載したスライドインペインが開きます。スライドインペインからチャートの 1 時間のデータポイントをクリックすると、チャートの下に表示されるテーブルのデータを更新できます。





## 第 16 章

# 不正管理ダッシュボードの監視

---

- ・ネットワークのセキュリティ脅威の管理 (333 ページ)

## ネットワークのセキュリティ脅威の管理

Cisco DNA Center の不正管理アプリケーションを使用すると、不正アクセスポイントからのネットワーク上の脅威をモニターできます。最も優先度の高い脅威を迅速に特定し、アシュアランス ダッシュボードからそうした脅威をモニターできます。

Cisco DNA Center の不正管理アプリケーションの詳細については、『[Cisco DNA Center Rogue Management Application Quick Start Guide \[英語\]](#)』を参照してください。





## 第 17 章

# Manage Dashboards

- [ダッシュボードについて \(335 ページ\)](#)
- [カスタム ダッシュボードの作成 \(335 ページ\)](#)
- [テンプレートからのダッシュボードの作成 \(336 ページ\)](#)
- [ダッシュボードの表示 \(338 ページ\)](#)
- [ダッシュボードの編集または削除 \(338 ページ\)](#)
- [ダッシュボードの複製 \(339 ページ\)](#)
- [ダッシュボードをお気に入りにする \(339 ページ\)](#)
- [ダッシュレットの位置の変更 \(340 ページ\)](#)

## 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

- ステップ 1** メニューアイコン (☰) をクリックして、**[Assurance] > [Dashboard Library]** の順に選択します。  
[ダッシュボードライブラリ (Dashboard Library)] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。
- ステップ 2** [+ Create a Dashboard] をクリックします。
- ステップ 3** [ダッシュボードの作成 (Create a Dashboard)] ダイアログ ボックスで、ダッシュボードのタイトルを入力します。
- ステップ 4** [保存 (Save)] をクリックします。  
空白のダッシュボードが表示されます。
- ステップ 5** ダッシュボードでは、次の操作を実行できます。

- a) [+ Add 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** [保存 (Save) ] をクリックしてダッシュボードを保存します。

## テンプレートからのダッシュボードの作成

テンプレートからダッシュボードを作成すると、範囲を使用してダッシュボードデータをフィルタ処理できます。範囲は、場所、デバイスタイプ、およびその他のオプションでデバイスをフィルタ処理します。

- ステップ 1** メニューアイコン (☰) をクリックして、[Assurance] > [Dashboard Library] の順に選択します。[Dashboard Library] ウィンドウが表示され、すべての定義されたダッシュボードとテンプレートを (下に) リスト表示します。
- ステップ 2** [Templates] エリアで、ダッシュボードテンプレートをクリックします。
- ステップ 3** [ダッシュボードの作成 (Create a Dashboard) ] ダイアログボックスで、ダッシュボードのタイトルを入力します。
- ステップ 4** [保存 (Save) ] をクリックします。
- ステップ 5** 既存の範囲を使用する場合は、既存の範囲を選択して [Select Scope] をクリックします。  
既存の範囲を選択した場合は、手順 [ステップ 15](#) に進みます。新しい範囲を作成する場合は次の手順を続けます。
- ステップ 6** 新しい範囲を作成する場合は、[Create New Scope] をクリックします。  
最初のステップ [Create New Scope] が表示されます。
- ステップ 7** 範囲名を入力し、[Next] をクリックします。範囲名にスペースを入力すると、スペースは下線に変換されます。  
2 番目のステップ [Select Location (s) ] が表示されます。
- ステップ 8** 範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含まれる 1 つ以上の場所を選択します。  
(注) 場所をフィルタリングするには検索フィールドを使用します。

- ステップ 9** [Next] をクリックします。  
3 番目のステップ [Select Filters] が表示されます。
- ステップ 10** [Client Health] テンプレートを使用している場合は、次のフィルタを使用できます。
- [Client Type] : 範囲の隣にあるチェックボックスをオンまたはオフにして有線またはワイヤレスを選択し、これらのタイプのデバイスを範囲に含めます。
  - [SSID] : 範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に SSID を含めます。検索フィールドに入力して SSID をフィルタリングします。このフィルタはワイヤレスデバイスにのみ適用されます。
  - [Host Name] : 範囲に含めるホスト名を入力します。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
  - [Device Type] : デバイスの OS の種類 (iOS、Android など) を入力して範囲に含めます。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
  - [MAC Address] : 範囲に含める MAC アドレスを入力します。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
  - [IP Address] : 範囲に含める IP アドレスを入力します。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- ステップ 11** [Network Health] テンプレートを使用している場合は、次のフィルタを使用できます。
- [Network Device Type] : 範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含まれる 1 つ以上のデバイスタイプを選択します。検索フィールドに入力してデバイスをフィルタリングします。
  - [Network OS] : 範囲の隣にあるチェックボックスをオンまたはオフにして、範囲に含めるネットワークの OS バージョンを選択します。検索フィールドに入力してバージョンをフィルタリングします。
  - [IP Address] : 範囲に含める IP アドレスを入力します。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
  - [Host Name] : 範囲に含めるホスト名を入力します。パーセント記号 (%) をワイルドカードとして使用し、それぞれの入力後に Enter キーを押します。
- ステップ 12** [Next] をクリックします。  
4 番目のステップの [Preview] が表示されます。
- ステップ 13** 選択したフィルタに基づいて更新されるクライアントのダイナミックリストを有効または無効にするには、[Dynamic list] トグルをクリックします。
- ステップ 14** [Save] をクリックして範囲を保存します。  
確認のダイアログが表示されます。
- ステップ 15** (任意) ダッシュレットをドラッグアンドドロップすると、ダッシュボード上でのダッシュレットの場所を変更できます。
- ステップ 16** ダッシュボードからダッシュレットを削除するには、次の手順を実行します。
- a) ダッシュレットの右上隅にあるゴミ箱アイコンをクリックします。
  - b) ダイアログボックスで、[Delete] をクリックします。
- ステップ 17** [Save] をクリックしてダッシュボードを保存します。

(注) 新しい範囲の場合は、ダッシュボードにデータが表示されるまで最大 15 分かかります。

## ダッシュボードの表示

- ステップ 1** メニューアイコン (☰) をクリックして、**[Assurance] > [Dashboard Library]** の順に選択します。**[Dashboard Library]** ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。**[並べ替え (Sort By)]** コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、**[検索 (Find)]** フィールドにその名前を入力して検索することができます。
- (注) ダッシュボードを **[Date Modified]** で並べ替えると、ダッシュボードに変更が加えられていない場合でも、ダッシュボードを最後に開いた日時で並べ替えられます。
- ステップ 2** お気に入りとしてマークされているダッシュボードを表示するには、**[Favorite Dashboards]** タブをクリックします。
- ステップ 3** 表示するダッシュボードをクリックします。
- ステップ 4** ダッシュボードのコントロールで、**[Show]** または **[Hide]** をクリックし、必要に応じてマップを表示または非表示にします。
- ステップ 5** (任意) フィルタから適切な値を選択して、期間、サイト、またはドメイン別にダッシュボードデータをフィルタ処理します。

## ダッシュボードの編集または削除

- ステップ 1** メニューアイコン (☰) をクリックして、**[Assurance] > [Dashboard Library]** の順に選択します。**[Dashboard Library]** ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。**[並べ替え (Sort By)]** コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、**[検索 (Find)]** フィールドにその名前を入力して検索することができます。
- ステップ 2** 編集または削除するダッシュボードをクリックします。
- ステップ 3** 次のいずれかを実行します。
- 変更するには、**[Actions]** メニューで **[Edit Dashboard]** を選択します。ダッシュレットを追加または削除し、ダッシュレットをダッシュボード内の別の位置にドラッグできます。設定が終了したら、**[Save]** をクリックします。

- ダッシュボードを削除するには、[Actions] メニューで [Delete Dashboard] を選択します。確認ダイアログで [Delete] をクリックします。

---


## ダッシュボードの複製

---

- ステップ 1** メニューアイコン (☰) をクリックして、[Assurance] > [Dashboard Library] の順に選択します。  
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[並べ替え (Sort By)] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[検索 (Find)] フィールドにその名前を入力して検索することができます。
- ステップ 2** ダッシュボードの複製アイコン (スターアイコンの隣) をクリックします。
- ステップ 3** [Duplicate a Dashboard] ダイアログボックスで、ダッシュボードコピーのタイトルを入力します。
- ステップ 4** [Save] をクリックします。
- ステップ 5** コピーしたこのダッシュボードは、ダッシュレットを追加、削除、または再配置することで変更できます。
- ステップ 6** [Save] をクリックしてダッシュボードを保存します。  
確認のダイアログが表示されます。
- ステップ 7** [OK] をクリックします。
- 

## ダッシュボードをお気に入りにする

---

- ステップ 1** メニューアイコン (☰) をクリックして、[Assurance] > [Dashboard Library] の順に選択します。  
[Dashboard Library] ウィンドウが表示され、定義されているすべてのダッシュボードの一覧が表示されます。[並べ替え (Sort By)] コントロールを使用すると、日付または名前でダッシュボードを並べ替えることができます。ダッシュボードは、[検索 (Find)] フィールドにその名前を入力して検索することができます。
- ステップ 2** ダッシュレット名の横にある  をクリックすると、お気に入りとして登録されます。
- (注) [Favorite Dashboards] タブをクリックすると、お気に入りにしたダッシュボードにアクセスできます。
-

# ダッシュレットの位置の変更

アシュアランスのダッシュボード（デフォルト）で、ダッシュレットの位置を変更できます。

---

**ステップ 1** 次のいずれかを実行します。

- [Health]メニューアイコン（☰）をクリックして、**アシュアランス** > [Overall Health] ダッシュボードが表示されます。
- メニューアイコン（☰）をクリックして、**アシュアランス** > [Health] > [Network Health]。 [Network Health] ダッシュボードが表示されます。
- メニューアイコン（☰）をクリックして、**アシュアランス** > [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。
- メニューアイコン（☰）をクリックして、**アシュアランス** > [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。

---





## 第 18 章

# ネットワークのトレンドを観察し洞察を得る

- ネットワークのトレンドとインサイトについて (341 ページ)
- ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する (342 ページ)
- ネットワークトレンドの表示とインサイトの取得 (346 ページ)
- ネットワークヒートマップ内アクセスポイントの比較 (351 ページ)
- KPI 値をネットワーク内のピアと比較 (355 ページ)
- 建物、APモデルファミリー、およびワイヤレスエンドポイントタイプの比較 (357 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 (360 ページ)
- 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 (363 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 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 駆動型 AP 比較**：ヒートマップ内の特定の月について、ネットワーク内のすべての AP を比較してトレンドを把握し、洞察を得ます。
  - **AI 駆動型のピア比較**：選択した主要業績評価指標（KPI）について、ピアネットワークと比較してネットワークのパフォーマンスを判断します。
  - **AI 駆動型のネットワークの比較**：選択した KPI 全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリー、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

# ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する

Cisco AI Network Analytics は、機械学習アルゴリズムを使用して、潜在的にクライアントエクスペリエンスが低いワイヤレス AP を特定します。AP は長期間にわたって継続的に分析され、最適ではないクライアントエクスペリエンスを提供していると疑われる AP は、根本的な原因と提案される改善点によってグループ化されます。修正可能な根本的な問題を診断するために使用できる一連の無線およびネットワーク機能で構成されるインサイトが生成されます。インサイトには次の主要なコンポーネントがあります。

- さまざまなクライアントエクスペリエンス KPI によってパフォーマンスの低い AP を検出します。
- 根本原因分析 (RCA) の基礎として、重要であり、顧客によって実行可能な、不十分なクライアントエクスペリエンスまたは優れたクライアントエクスペリエンスを持つ AP を区別できる適切な機能を見つけます。

AP は、2.4 GHz、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。

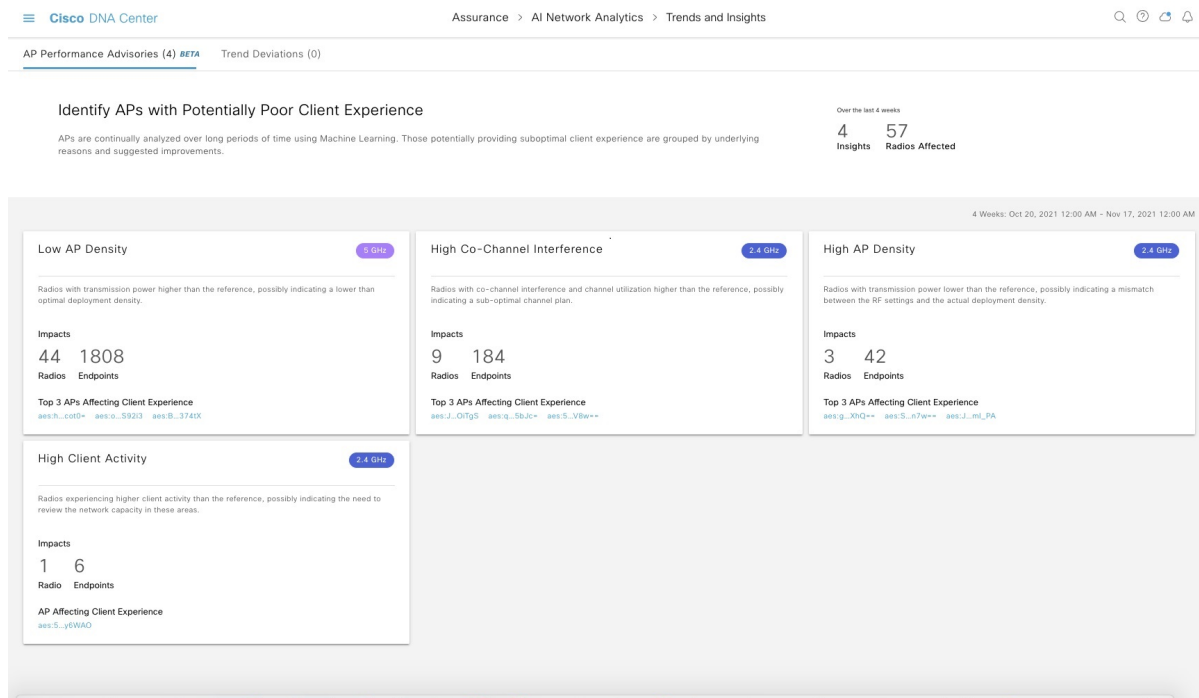
この手順を使用して、AP パフォーマンスアドバイザリを表示し、4 週間のデータの分析に基づいてクライアントエクスペリエンスが低い最もアクティブな AP を強調表示します。

---

**ステップ 1** メニューアイコン (☰) をクリックして、[Assurance] > [Trends and Insights] > [AP Performance Advisories] の順に選択します。

**ステップ 2** [AP Performance Advisories] タブをクリックすると、一般的な根本原因分析カテゴリと影響を受ける無線に関するさまざまなタイプのインサイトの概要が表示されます。

図 33: アクセス ポイント パフォーマンス アドバイザリ



一般的な根本原因分析で発生する可能性のあるインサイトを以下に示します。

- 外部 RF 負荷
- クライアントアクティビティが多い外部 RF 負荷
- 頻繁なチャネル変更
- 高 RF 負荷
- 高いチャネル使用率
- 高いクライアントアクティビティ
- 高いクライアントの負荷
- 高い AP 展開密度
- 低い AP 展開密度
- 低い AP 展開密度および外部干渉
- 低い AP 展開密度および高負荷

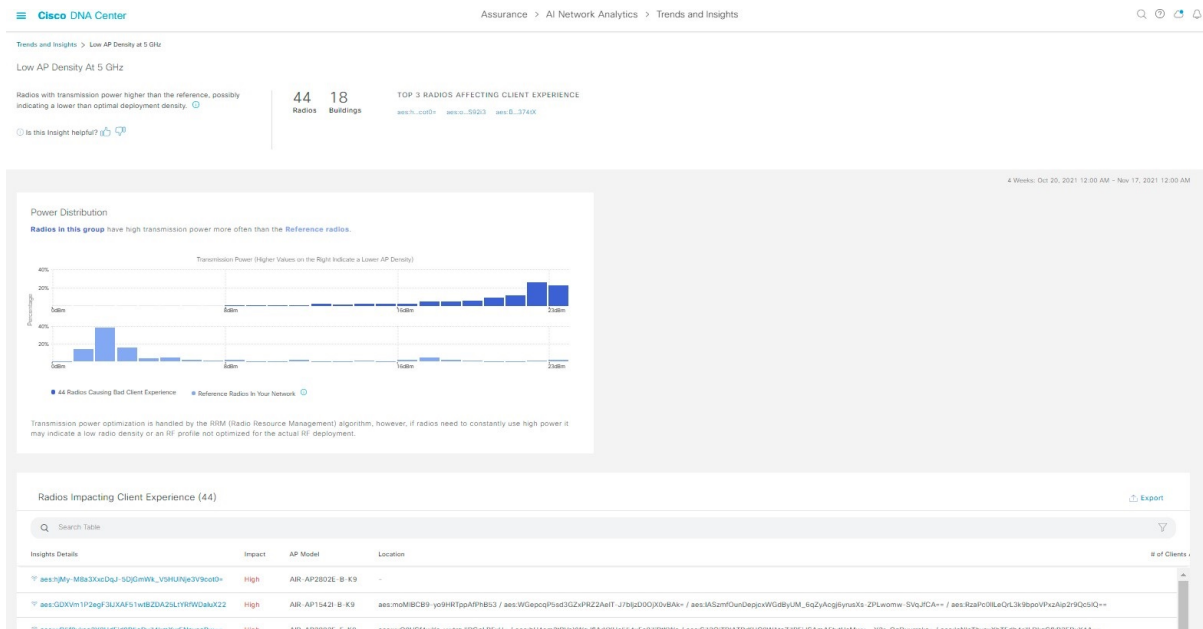
**ステップ 3** [AP Performance Advisories] ダッシュボードを使用して、次のインサイトの概要を確認します。

ワイヤレスアクセスポイントのパフォーマンスアドバイザリを表示する

| [Network Overview] ウィンドウ      |                                                                |
|-------------------------------|----------------------------------------------------------------|
| アイテム                          | 説明                                                             |
| インサイトサマリー                     | 特定の周波数帯に関するインサイト（低 AP 密度、高クライアントアクティビティなど）の名前と問題定義を表示します。      |
| 影響                            | インサイトごとに影響を受ける [Radios] と [Endpoints] の数を表示します。                |
| クライアントエクスペリエンスに影響する上位 3 つの AP | 特定の周波数帯で影響を受ける上位 3 つの AP を表示します。これらは、手順 5 に示す詳細ページへのハイパーリンクです。 |

**ステップ 4** 次の情報について各インサイトダッシュレットをクリックすると、一般的な根本原因分析と、このカテゴリのすべての無線に対する推奨アクションが表示されます。

図 34: 影響を受ける無線のインサイト サマリー ダッシュボード



| インサイトダッシュボード |                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
| アイテム         | 説明                                                                                                                                  |
| 概要           | 4 週間にわたって分析された無線の総数、建物の数、影響を受けた上位 3 つの AP を表示します。                                                                                   |
| [KPI] チャート   | すべての無線での KPI の分布を示す RCA カテゴリに応じて、複数の KPI チャートを表示します。チャートを使用して、この一般的な RCA を使用した無線のパフォーマンスを、クライアントエクスペリエンスの問題が検出されていない参照の無線と比較対照できます。 |

| インサイトダッシュボード                              |                                                                                      |
|-------------------------------------------|--------------------------------------------------------------------------------------|
| アイテム                                      | 説明                                                                                   |
| [Radios Impacting Client Experience] テーブル | インサイトの詳細、影響（低、中、または重大）、AP モデル、場所、影響を受けるクライアントの数、およびクライアントエクスペリエンスに影響を与える KPI が含まれます。 |
| [Export]                                  | CSV ファイルにテーブルデータをエクスポートするには、[Export] をクリックします。                                       |

**ステップ 5** [Radios Impacting Client Experience] テーブルで、ハイパーリンクされた AP をクリックして、特定の AP に関する次の詳細なインサイトサマリーを表示します。

図 35: アクセスポイントのインサイトサマリー



| インサイトダッシュボード |                                                                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム         | 説明                                                                                                                                                  |
| 上部バー         | AP モデル、場所、影響を受けるクライアント、および [Assurance Device] ウィンドウにハイパーリンクされた追加の AP の詳細などの情報を表示します。また、クライアントエクスペリエンスを向上させるために、特定された根本原因と異常な KPI に固有の推奨アクションも提供します。 |

| インサイトダッシュボード                        |                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                | 説明                                                                                                                                                                                                                                                                                                                                             |
| [Client Experience KPIs]            | <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul> |
| [Radio Specific Root-Cause Context] | <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> </ul>                                                                |

## ネットワークトレンドの表示とインサイトの取得

トレンドは、一定期間にわたって観察されたネットワーク内の動作の長期的な進化です。次のトレンドは、ネットワークのパフォーマンス（蜂群グラフで表現）に関するインサイトを提供します。以下のタイプのインサイトがあります。



- [Intra-Site] : Cisco AI Network Analytics は、単一のサイトまたはビルを検索し、そのビル内だけの外れ値デバイスを強調表示します。この場合、蜂群グラフ内のエンティティは無線であり、円で表されます。
- [Inter-Site] : Cisco AI Network Analytics は、グローバルネットワークを調べ、選択したKPIに関して外れ値となっているビルを特定します。この場合、蜂群グラフ内のエンティティはビルであり、多角形で表されます。

ネットワークのトレンドを表示するには、次の手順を実行します。

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

[Network Insights] ウィンドウに、[Capacity]、[Coverage]、[Throughput] のフィルタが表示されます。テーブルのデータを更新するには、該当するフィルタをクリックします。デフォルトでは、[Capacity] フィルタが選択されています。

(注) フィルタは動的です。フィルタに使用可能なインサイトがない場合、そのフィルタは表示されません。

| インサイトテーブル                                                                                |                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                     | 説明                                                                                                                                                                                                                                     |
| <b>Occurrence</b>                                                                        | このトレンドが観測された期間 ([May 27 - June 03 2019] など)。                                                                                                                                                                                           |
| [Insight Type]                                                                           | [Daily] および [Weekly] という名前のインサイトタイプをリストします                                                                                                                                                                                             |
| <b>Insight</b>                                                                           | 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。                                                                                                                                                                                                      |
| <b>カテゴリ</b>                                                                              | インサイトが観測されたカテゴリ。インサイトの KPI は次のカテゴリにグループ化されます。 <ul style="list-style-type: none"> <li>• [Capacity] : 無線クライアント数、チャンネル変更数</li> <li>• [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</li> <li>• [Throughput] : 総無線スループット</li> </ul> |
| 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。<br>値は [2.4 GHz]、[5 GHz]、[6GHz] またはすべての周波数帯です。                                                                                                                                                             |
| <b>KPI</b>                                                                               | 特定のインサイトに関する重要業績評価指標 (KPI)。                                                                                                                                                                                                            |
|  アイコン | インサイトテーブルに表示する列をカスタマイズできます。  アイコンをクリックし、表示しない列のチェックボックスをオフにして、[Apply] をクリックします。                                                                   |

ステップ 2 [insights] 列でインサイトをクリックするとスライドインペインが開き、次の情報が表示されます。

| [Insight Details] スライドインペイン |                                                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------|
| アイテム                        | 説明                                                                                            |
| <b>Cisco AI</b>             | インサイトの計算方法に関する情報が表示されます。<br>人工知能の概要については、 <a href="#">こちら</a> を参照してください。                      |
| <b>Insight Summary</b>      | 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。 |
| <b>Weekly Client Load</b>   | 週あたりのクライアント負荷。                                                                                |

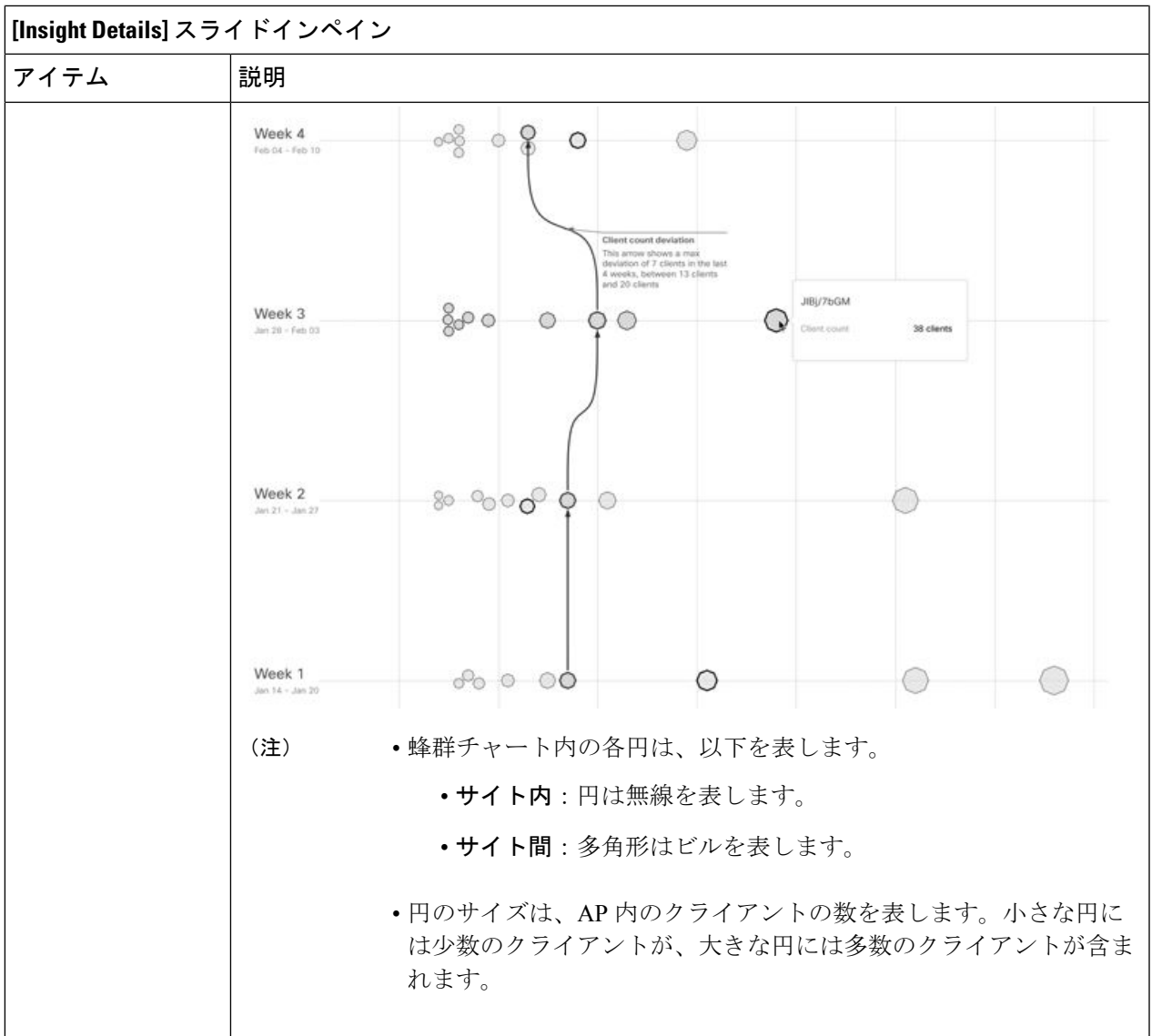
| [Insight Details] スライドインペイン |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| トラブルシューティング                 | <p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> </ul> <p>• 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。</p> |
| 問題数                         | 問題数のグラデーション。                                                                                                                                                                                                                                                                                                                                                                                                                        |



| [Insight Details] スライドインペイン |    |
|-----------------------------|----|
| アイテム                        | 説明 |
| チャート (Chart)                |    |

[Insight Details] スライドインペイン

| アイテム | 説明                                                                                                                                                                                                                     |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>蜂群グラフには、次の図に示すように、ネットワーク内のクライアントデバイスのパフォーマンスが4日（日次インサイト）および週（週次インサイト）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が体系的に乖離している場合、その傾向はチャート内の矢印によって表示されます。</p> <p>図 36: 蜂群チャート</p> <p>[Daily Insights]</p> <p>[Weekly Insights]</p> |



**ステップ 3** チャート内の円の上にカーソルを置くと、APの名前と MAC アドレス、帯域周波数、AP グループ、AP の場所、問題の数、クライアント数、および KPI 値などの情報が表示されます。

(注) グローバルサイトでは、チャート内の円の上にカーソルを置くと、トレンドが観測されたビルやクライアント数に関する情報が表示されます。

## ネットワークヒートマップ内アクセスポイントの比較

ネットワークヒートマップを使用して、特定の月に関してネットワーク内のすべての AP を視覚的に比較し、トレンドを把握し、インサイトを取得します。異なる KPI と帯域周波数で AP

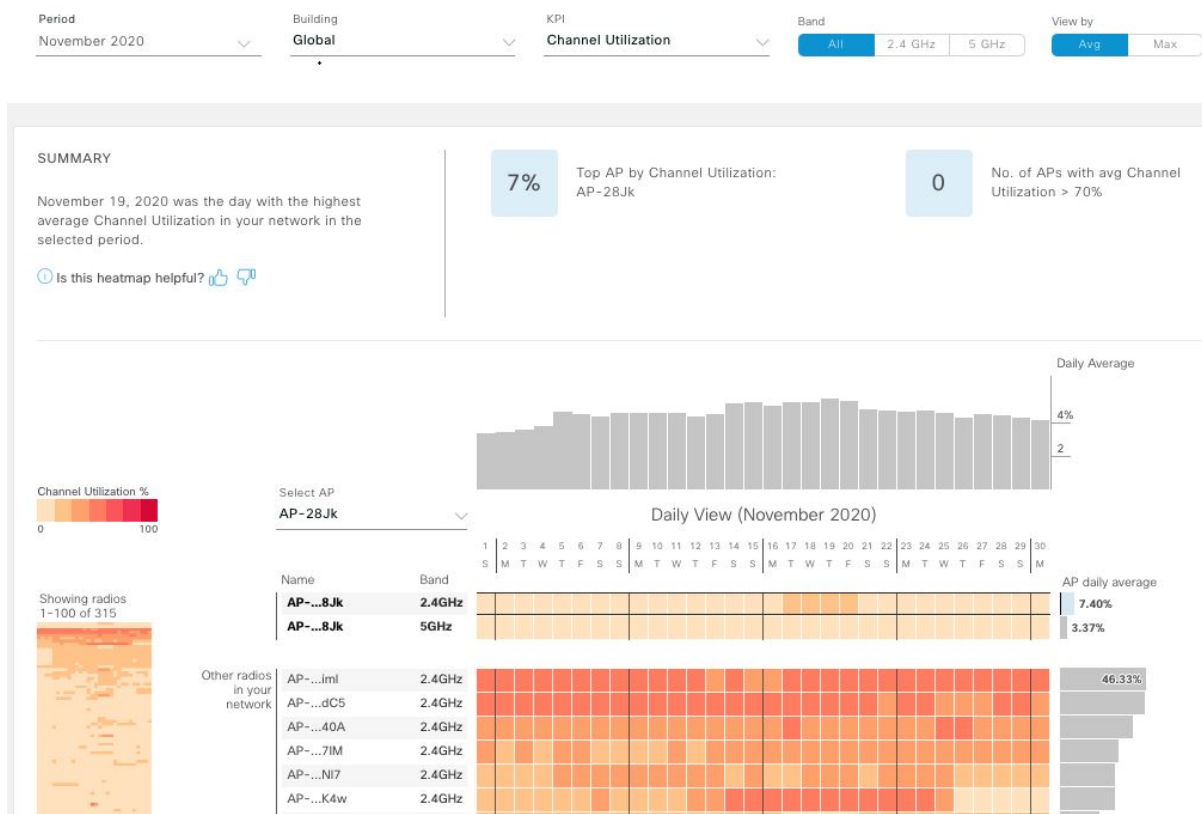
ネットワークヒートマップ内アクセスポイントの比較

を比較することを選択できます。取得したインサイトにより、最も輻輳が多いKPI、最も輻輳のあるAP、およびそれらのAPのうち使用中のAPに関する情報が得られます。この情報により、トレンドが観察されたサイトまたはビルにさらにドリルダウンすることができます。APまたはAPのグループを特定したら、それらのAPの動作履歴（1日、1週間、および月全体）を判断できます。


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

[Network Heatmap] ウィンドウに次の情報が表示されます。


図 37: [Network Heatmap] ウィンドウ



| [Network Heatmap] ウィンドウ |                                                                                    |
|-------------------------|------------------------------------------------------------------------------------|
| アイテム                    | 説明                                                                                 |
| [Period]                | ドロップダウンリストから選択した月の情報がヒートマップに表示されます。                                                |
| [Building]              | グローバルネットワーク全体またはドロップダウンリストから選択した特定のサイトとビルディングの情報がヒートマップに表示されます。デフォルトは [Global] です。 |
| [KPI] ドロップダウンリスト        | ドロップダウンリストから選択したKPIのヒートマップに情報を表示します。デフォルトは [Client Count] です。                      |

| [Network Heatmap] ウィンドウ |                                                                                                                                                                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                    | 説明                                                                                                                                                                                                                                        |
| [Band]                  | 選択した帯域周波数のヒートマップに情報を表示します。[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を表示できます。<br>[View By] のリストに表示されるオプションは、選択した KPI に応じて異なります。<br>KPI に応じて、[Avg]、[Min]、または [Max] を並べ替えのオプションとして選択できる場合、[Avg] または [Max] を選択できる場合のほか、いずれのオプションも提供されない場合もあります。                                            |
| [Summary] 領域            | ヒートマップ分析から得られたインサイトの概要が表示されます。次のタイプの情報が表示されます。 <ul style="list-style-type: none"> <li>• 最もビジーだった日。</li> <li>• 無線あたりのクライアント数がゼロの AP の数。</li> <li>• 無線あたりのクライアント数が 50 を超える AP の数。</li> </ul>                                                |
| [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。                                                                                      |
| <b>KPI</b> のグラデーション     | このエリアには、[KPI] ドロップダウンリストから選択した KPI に応じて、KPI のパフォーマンスに関する情報が色のグラデーションで表示されます。濃い色のブロックは、有意な KPI スコアを示します。たとえば、低い RSSI スコアは、高い RSSI スコアよりも有意になります。クライアント数が多いスコアは、クライアント数の少ないスコアよりも有意になります。                                                   |
| [Search AP] ドロップダウンリスト  | AP を検索および選択できます。次の手順を実行します。 <ol style="list-style-type: none"> <li>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。<br/>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。</li> <li>2. 強調表示された AP をクリックして選択します。<br/>AP の個々の無線が、ヒートマップに個別に表示されます。</li> </ol> |

| [Network Heatmap] ウィンドウ                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| [Network Daily Avg]、[Network Daily Min]、または [Network Daily Max] グラフ | <p>選択した [View By] オプションに応じて、該当するグラフが表示されます。</p> <ul style="list-style-type: none"> <li>• [Avg] を選択した場合、日単位の平均値が表示され、最も高い平均値がグラフ内で強調表示されます。</li> <li>• [Min] または [Max] を選択した場合、日単位の最小値または最大値が表示され、それらの値がグラフ内でそれぞれ強調表示されます。</li> </ul> <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| [Showing Radios] ヒートマップ                                             | <p>ヒートマップの圧縮ビューが表示されます。</p> <p>デフォルトでは、この領域には、最初の 100 個の無線のヒートマップが表示されます。追加の無線のヒートマップデータを表示するには、圧縮されたヒートマップの下部までスクロールして、ドロップダウンリストから適切なオプションを選択します。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| [AP Heatmap] エリア                                                    | <p>次が含まれます。</p> <ul style="list-style-type: none"> <li>• [Radios in Your Network] : AP の名前とクライアントによって使用された帯域周波数が表示されます。AP の横にあるアイコンをクリックすると、その AP の [Device 360] ページが開きます。</li> </ul> <p>この領域には、[Band] のオプションから選択した帯域周波数に応じて、対応する帯域の AP が一覧表示されます。</p> <ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>[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。</p> <ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>[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。</p> |

| [Network Heatmap] ウィンドウ                                                                  |                                                                                                                                                  |
|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                     | 説明                                                                                                                                               |
|  Export | CSV ファイルにヒートマップデータをエクスポートするには、[Export] をクリックします。<br><br>ヒートマップに適用されている AP とフィルタは、エクスポート対象のデータに適用されます。エクスポートは、日単位のビューでのみ有効になり、時間単位のビューでは有効になりません。 |

**ステップ 2** 追加の無線のヒートマップデータを表示するには、ウィンドウの下部までスクロールして、ドロップダウンリストから適切なオプションを選択します。


## KPI 値をネットワーク内のピアと比較

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



(注) 比較に使用されるピアネットワークは、同様の規模のネットワークです。

ピアの比較では、計算のために、オンボーディングの日付から数カ月のデータが使用されません。

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

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

| [Peer Comparison] ウィンドウ |                                                                                                                                                                                                                           |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                    | 説明                                                                                                                                                                                                                        |
| [KPI] ドロップダウンリスト        | ドロップダウンリストから KPI を選択します。[Radio Throughput]、[Cloud Apps Throughput]、[Radio Resets]、[Packet Failure Rate]、[Interference]、[Onboarding Error Source]、[Roaming Error Source]、[RSSI] のいずれかを選択できます。デフォルトは [Radio Throughput] です。 |
| Show                    | 自ネットワークとピアネットワークの間の KPI 値を比較する曜日を選択します。デフォルトは [All] です。                                                                                                                                                                   |

| [Peer Comparison] ウィンドウ  |                                                                                                                                                                                                                                                                                                     |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                     | 説明                                                                                                                                                                                                                                                                                                  |
| 要約                       | <p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> </ul>                                                                                                |
| [Highlight Peers] トグルボタン | <p>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。</p>                                                                                                                                                                                                                                                           |
| ピア比較棒グラフ                 | <p>デフォルトでは、次の図に示すように、[Band 2.4 GHz] および [Band 5 GHz] グラフのネットワークの KPI 値が強調表示されます。</p> <p>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。</p> <p><b>図 38: ピア比較棒グラフ</b></p> <p>グラフの色は、以下を表します。</p> <ul style="list-style-type: none"> <li>• 青 : 自ネットワーク。</li> <li>• ピンク : ピアネットワーク。</li> </ul> |

**ステップ 2** 特定の日について、自ネットワークとピアネットワークの KPI 値を表示するには、[Show] エリアで該当する日を選択します。



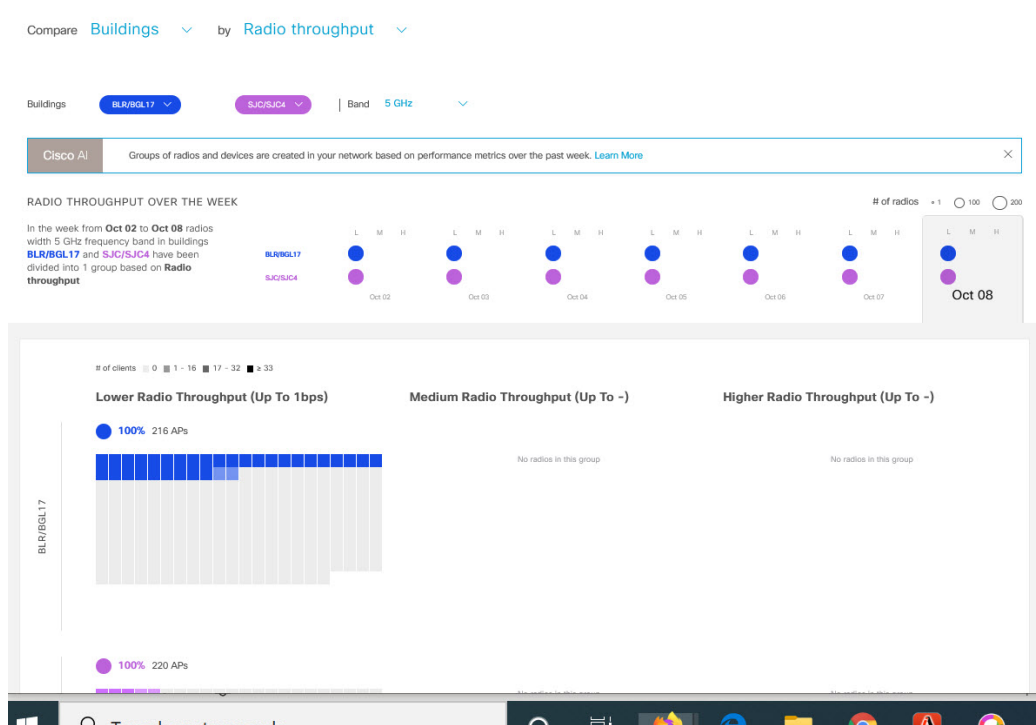
# 建物、AP モデルファミリー、およびワイヤレス エンドポイントタイプの比較

この手順を使用して、選択した重要業績評価指標（KPI）全体で、ネットワーク内のオブジェクト（建物、AP モデルファミリー、ワイヤレスエンドポイント）のパフォーマンス改善の機会を表示、比較、および特定します。

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

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

図 39: [Network Object Comparison] ウィンドウ



## [Network Object Comparison] ウィンドウ

| アイテム                     | 説明                                                                                                                                                           |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Compare] ドロップ<br>ダウンリスト | 比較するネットワーク内のオブジェクトを選択します。オプションは、[Buildings]（サイト）、[AP Model Families]、または [Wireless Endpoints]（Android デバイス、Android 携帯、IOS タブレット、IOS 携帯、Linux ワークステーションなど）です。 |

| [Network Object Comparison] ウィンドウ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| [By KPI] ドロップダウンリスト               | <p>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。</p> <p>[Buildings] の場合、オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• [Radio Throughput]</li> <li>• [Channel Utilization]</li> <li>• [Average Client RSSI]</li> <li>• [Average Client SNR]</li> <li>• [Average Onboarding Time]</li> <li>• [Average Authorization Time]</li> <li>• [Average DHCP Time]</li> <li>• [Cloud Throughput]</li> <li>• [Media Throughput]</li> <li>• [Social Throughput]</li> <li>• [Interference]</li> </ul> <p>[AP Model Families] の場合、オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• [Radio Throughput]</li> <li>• [Interference]</li> <li>• [Media Apps Throughput]</li> <li>• [Average Client RSSI]</li> <li>• [Channel Utilization]</li> <li>• [Average Client SNR]</li> <li>• [Cloud Throughput]</li> <li>• [Social Throughput]</li> </ul> <p>[Wireless Endpoints] の場合、オプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• [Average AAA Time]</li> <li>• [Average Onboarding Time]</li> <li>• [Average DHCP Time]</li> </ul> |

| [Network Object Comparison] ウィンドウ                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                            | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| [Buildings]<br>[AP Model Families]<br>または<br>[Wireless Endpoints]<br>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 モデルファミリー、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。<br><br>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/紫色で表示されません。                                                                                                                                                                                                                                                                                                                                                                                          |
| [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<br>デーション<br><br>または<br>[Device Count]<br>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。<br><br>[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。<br><br>ブロックの色の濃さでクライアント数またはデバイス数が示されます。濃い色のブロックには、薄い色のブロックよりも多くのクライアントやデバイスが存在します。                                                                                                                                                                                                                                                                                                                                         |
| [AP Clusters]<br>または<br>[Device Type<br>Clusters]                               | この領域には、各ネットワークオブジェクトに 1 つずつ、2 つのクラスタのセットが表示されます。この領域では、2 つのネットワークオブジェクトのパフォーマンスを視覚的に比較できます。次の情報を出力します。 <ul style="list-style-type: none"> <li>• KPI のパフォーマンス（パーセンテージ）。</li> <li>• 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。</li> <li>• KPI 値が低、中、高のネットワーク内のオブジェクト。</li> </ul> <p>[Onboarding Time] や [Authorization Time] などの KPI については、この領域に次のような情報が表示されます。</p> <ul style="list-style-type: none"> <li>• クライアントが各サイトでオンボーディングするデバイスのタイプ。たとえば、Windows ワークステーション、OS X ワークステーション、Linux ワークステーション、Android 電話機、IOS デバイスなどです。</li> <li>• 各デバイスタイプの数。</li> <li>• KPI の時間が低、中、高のデバイスの数。</li> </ul> |

**ステップ 2** クラスタ内の色付きブロックにカーソルを合わせると、日付、AP が存在する建物、AP のモデル番号、無線プロトコル、無線クライアント数など、AP に関する情報が表示されます。濃い色のブロックには、薄い色のブロックよりも多くのクライアントが存在します。

# ベースラインを使用したネットワークパフォーマンスの表示と監視

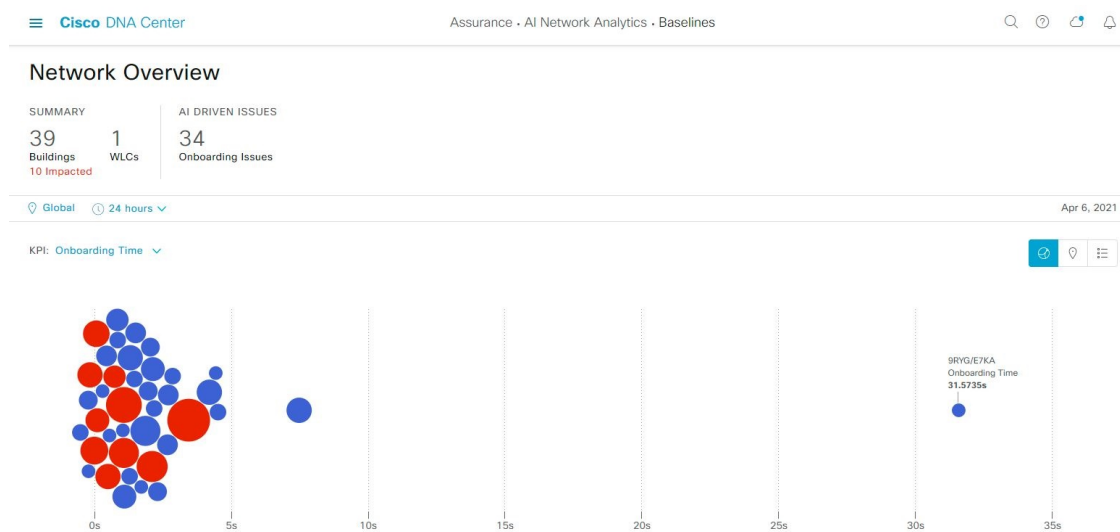
Cisco AI Network Analytics は最先端の機械学習技術を使用して、特定のネットワークとサイトに関するベースラインを定義します。Cisco AI Network Analytics は、この情報に基づいて特定の時点における各ネットワークとサイトの正常な動作を定義し、最も重要な問題を特定できます。

機械学習アルゴリズムから派生したベースラインを使用してネットワークパフォーマンスを調査および監視するには、次の手順を実行します。

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





[Baselines] ダッシュボードが表示されます。


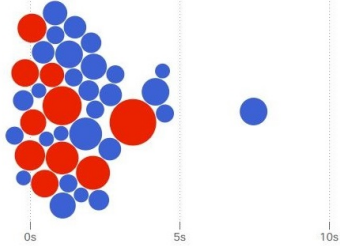
図 40: [Baselines] ダッシュボード



**ステップ 2** [Network Overview] ウィンドウを使用して、次の情報が表示されます。

| [Network Overview] ウィンドウ |                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------|
| アイテム                     | 説明                                                                                   |
| 概要                       | 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総数、およびワイヤレスコントローラ の総数が表示されます。                              |
| [AI Driven Issues]       | 特定のネットワーク環境の予測ベースラインからの乖離度に基づいてトリガーされ、Cisco AI Network Analytics によって検出された問題が表示されます。 |

| [Network Overview] ウィンドウ                                                                                            |                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                                                                                                                | 説明                                                                                                                                                                                                          |
|  Global ▾<br>[Location] ドロップダウンリスト | ロケーションアイコンをクリックしてペインのスライドを開き、サイトまたは建物を選択します。ダッシュボード上の情報が、選択に応じて更新されます。                                                                                                                                      |
| <br>[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。 <ul style="list-style-type: none"> <li>• ドロップダウンメニューで、範囲の長さ ([24 Hours]、またはカスタム範囲) を選択します。</li> <li>• 開始日と終了日を指定します。</li> <li>• [Apply] をクリックします。</li> </ul> |
| [KPI] ドロップダウンリスト                                                                                                    | ドロップダウンリストから KPI を選択します。オプションは、[Onboarding Time]、[Onboarding Failures]、[DHCP Time]、[Authentication Time]、および [Association Failures] です。デフォルトは [Onboarding Time] です。                                         |
| <br>[Map View]                    | このトグルボタンをクリックすると、すべてのネットワークサイトの正常性が、ネットワークの地理的ロケーションに基づいたマップビューに表示されます。                                                                                                                                     |
| <br>[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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|  <p>[Beeswarm Chart]</p> | <p>このトグルボタンをクリックすると、選択した KPI に関するネットワークのクライアントデバイスのパフォーマンスに関するインサイトを提供する蜂群チャートが表示されます。</p> <p>KPI: Onboarding Time ▼</p>  <p>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。</p> <p>蜂群チャート内の各円は、以下を表します。</p> <ul style="list-style-type: none"> <li>青色：円は建物を表します。チャート内の円の上にカーソルを合わせると、ロケーション、KPI、SSID、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。</li> <li>赤色：円は問題の影響を受けた建物を表します。チャート内の円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。</li> <li>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。</li> </ul> |

**ステップ 3** 蜂群チャートから円をクリックして、次の情報の建物ビューを表示します。

### 建物ビュー

サイトまたは建物の特定の情報が表示されます。それぞれのドロップダウンリストから KPI、SSID、および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。

より詳細な時間範囲を指定するには、タイムラインスライダを使用します。時間範囲を指定するには、タイムライン境界線をクリックしてドラッグします。

タイムラインスライダの下に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。

カラーコードは次のことを表します。

- 赤は AI に起因する問題を表します
- 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、追加の詳細情報を記載したスライドインペインが開きます。この内容は、KPI チャートから選択した KPI によって異なります。スライドインペインに、平均 KPI 期間 ([Onboarding Time]、[DHCP Time]、[Onboarding Failures]、[Authentication Time] など) と固有のクライアントの色分けされたチャートが表示されます。

サンキョーグラフは、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の平均です。

## 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

- 拡張 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 DNA Center ユーザーガイド](#)』の「[Assign Location to an Existing AI RF Profile](#)」[英語]を参照してください。

## 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

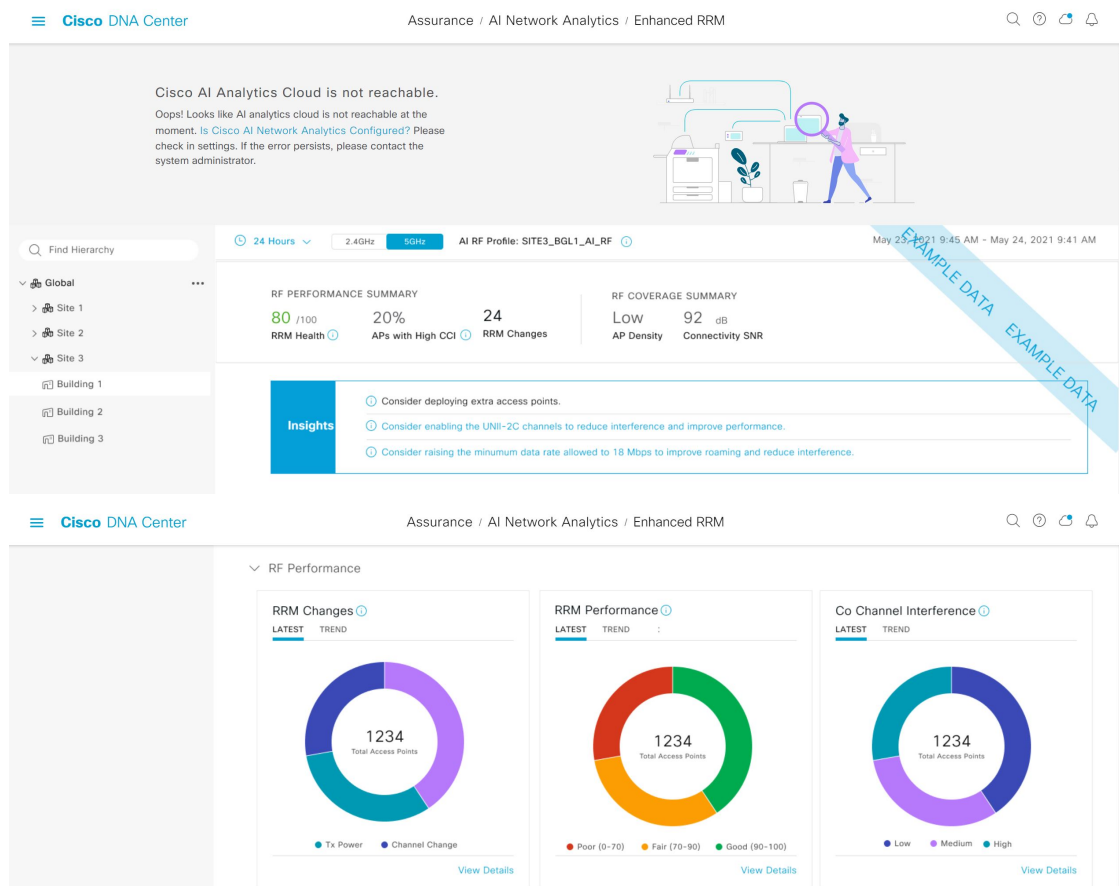
- AI 拡張 RRM インサイトにアクセスするには、AI RF プロファイルに割り当てられた場所全体にデバイスをプロビジョニングする必要があります。詳細については、『[Cisco DNA Center ユーザーガイド](#)』の「[Provision Wireless Devices](#)」[英語]を参照してください。
- Cisco AI 拡張 RRM は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco IOS-XE 17.7.1 以降でのみサポートされています。
- 次のタスクを実行するには、**スーパー管理者**または**ネットワーク管理者**である必要があります。

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

**[Enhanced RRM]** ダッシュボードが表示されます。

図 41: 機能強化された RRM ダッシュボード



**ステップ 3** 次の機能には、**[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。 |
| [Band]          | [2.4GHz] 帯域と [5GHz] 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** [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。

- [Channel List] チェックボックスをオンにして、現在 AI RF プロファイルリストにあるチャンネルリストを選択します。
- [Channel Width] チェックボックスをオンにし、[Apply] をクリックして、推奨される動的帯域幅選択を設定します。
- [Now] または [Later] をクリックして、推奨事項をいつ適用するかを指定します。
- [Run Simulation] をクリックして、シミュレーション結果を表示します。

**ステップ 5** [RF PERFORMANCE SUMMARY] エリアを使用して、次の詳細を表示します。

- [RRM Performance] : 同一チャンネル干渉、ノイズ、SNR、無線使用率など、多数の KPI に基づいた複合メトリックを表示します。
- [APs with High CCI] : AP とネイバーによって提供されるワイヤレス ネットワークのパフォーマンスが低いことを示します。
- [RRM Changes] : RRM チャンネル変更、チャンネル帯域幅変更、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。

**ステップ 6** [RF COVERAGE SUMMARY] エリアを使用して、次の詳細を表示します。

- [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 7** [Insights] ダッシュレットを使用して、AI 拡張 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]
- TPC しきい値
- [Channel Width]
- [Enable FRA]

- ステップ 8** [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、新しい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、拡張 RRM ダッシュボードに対して予測される結果を視覚化できます。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。
  - b) 必要に応じて [5 GHz] の下で属性を変更して、メトリックを表示できます。  
(注) ピーク時間、データレート、クライアント制限、RX SOP 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。  
[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、5 GHz 無線帯域の AI 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。詳細を編集するには、ウィンドウの対応する領域に表示される [Edit] オプションをクリックします。
    - [Simulation Name]
    - [Profile Details]
    - [RF Performance]
    - [RF Coverage]
  - f) [Upgrade AI RF Profile] をクリックします。  
[Upgrading AI RF Profile] ダイアログボックスが表示されます。
  - g) [Upgrading AI RF Profile] ダイアログボックスで、プロファイル名を編集できます。  
[Now] または [Later] をクリックして、推奨事項をいつ適用するかを指定し、[Apply] をクリックします。
  - h) [Review Cisco AI Recommendations for RRM] 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、[Apply] をクリックします。
  - i) [AI RF Profile Successfully Updated] ダイアログボックスで [OK] をクリックします。
  - j) [Simulation Result] ウィンドウで、構成された AI サポート RF プロファイルのシミュレーション結果を確認します。
- ステップ 9** 次の機能のために [RF Performance] を展開します。

| アイテム                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[RRM Changes] ダッシュレット</p> | <p>次のタブが含まれます。</p> <ul style="list-style-type: none"> <li>• [LATEST] : 過去 30 分間の RRM チャンネル変更、チャンネル帯域幅変更、および Tx 電力変更イベントの合計数を表示します。</li> <li>• [TREND] : 時間範囲内のイベントと選択した時間の AP のチャンネル変更、チャンネル帯域幅変更、および Tx 電力変更を表示します。</li> </ul> <p>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] スライドインペインを開きます。</p> <ol style="list-style-type: none"> <li>1. グラフの色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。</li> <li>2. グラフの色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。             <ul style="list-style-type: none"> <li>• Access Point</li> <li>• [Change Category]</li> </ul> </li> <li>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。             <p>(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。</p> </li> <li>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。</li> </ol> |

| アイテム                | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [RRMHealth] ダッシュレット | <p>次のタブが含まれます。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> </ul> <p>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] スライドインペインを開きます。</p> <ol style="list-style-type: none"> <li>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。</li> <li>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] テーブルの次のデバイスデータを表示します。 <ul style="list-style-type: none"> <li>• Access Point</li> <li>• ヘルス スコア</li> <li>• 同一チャンネルの重複</li> <li>• 同一チャンネルネイバー利用</li> <li>• RSSI クライアントスコアが低い</li> <li>• 同じチャンネルのノイズ</li> <li>• 同じチャンネルの干渉</li> </ul> <p>(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。</p> </li> <li>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。</li> </ol> |

| アイテム                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[Co-Channel Interference]<br/>ダッシュレット</p> | <p>次のタブが含まれます。</p> <ul style="list-style-type: none"> <li>• [LATEST] : 過去 30 分間に [Low]、[Medium]、[High] の同一チャンネル干渉が発生している AP の総数を表示します。</li> <li>• [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] の同一チャンネル干渉の割合を示します。</li> </ul> <p>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] スライドインペインを開きます。</p> <ol style="list-style-type: none"> <li>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] の同一チャンネル干渉が表示されます。</li> <li>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] テーブルの次のデバイスデータを表示します。 <ul style="list-style-type: none"> <li>• Access Point</li> <li>• チャンネル</li> <li>• 影響スコア</li> <li>• CCI (dBm)</li> <li>• Duty Cycle</li> </ul> <p>(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。</p> </li> <li>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。</li> </ol> |
| <p>[Utilization Per Channel]<br/>ダッシュレット</p> | <p>[LATEST] タブには、過去 30 分間に [Low]、[Medium]、[High] の同一チャンネル干渉が発生している AP の総数が表示されます。</p> <p>次の詳細を表示するには、チャートにカーソルを合わせます。</p> <ul style="list-style-type: none"> <li>• チャンネルの数</li> <li>• Tx/Rx の使用率</li> <li>• Interference</li> </ul> <p>[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ンネルごとの使用率の詳細が表示されます。</p> <p>(注) [Select Channel] ドロップダウンリストでは、名前を入力してチャンネルを検索するか、リストからチャンネルを選択して詳細を表示できます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| アイテム                               | 説明                                                                                                                                                                                                                                                                                                                  |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [AP and Radar per Channel] ダッシュレット | <p>[LATEST] タブには、過去 30 分間の AP およびチャンネルのチャートに、チャンネルごとの AP およびレーダーの詳細が表示されます。</p> <p>次の詳細を表示するには、チャートにカーソルを合わせます。</p> <ul style="list-style-type: none"> <li>• チャンネルの数</li> <li>• Tx/Rx の使用率</li> <li>• Interference</li> </ul> <p>[TREND] タブには、時間範囲内の AP またはレーダーと選択された時間のチャートに、チャンネルごとの AP、不正、およびレーダーの詳細が表示されます。</p> |

**ステップ 10** 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <p>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、チャンネル、チャンネル幅、および Tx 電力の最適な実効値に影響します。</p> <ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>以下を表示するには、チャートにカーソルを合わせます。</p> <ul style="list-style-type: none"> <li>• AP ネイバー密度</li> <li>• AP Count</li> <li>• エンドポイントカウント</li> </ul> <ul style="list-style-type: none"> <li>• [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 AP 数を表示します。</li> </ul> <p>平均隣接密度範囲は、 [&lt;5]、 [5-10]、 [10-15]、 [15-20]、 [20-25]、 および [&gt;=25] です。</p> <p>[LATEST] タブで、グラフの色セグメントまたは [View Details] リンクをクリックして、[AP Spatial Density Details] スライドインペインを開きます。</p> <ol style="list-style-type: none"> <li>1. チャートにカーソルを合わせると、選択した建物の [AP Neighbor Density]、[AP Count]、および [Clients Count] が表示されます。</li> <li>2. 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。 <ul style="list-style-type: none"> <li>• アクセスポイント</li> <li>• ネイバー密度メトリック</li> <li>• 合計 Rx ネイバー</li> <li>• チャンネルネイバー RSSI で最高</li> <li>• チャンネルネイバーの合計</li> </ul> <p>(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。</p> </li> <li>3. [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。</li> <li>4. [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。</li> </ol> |



| アイテム | 説明                                                |
|------|---------------------------------------------------|
|      | 5. [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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>[Power Distribution] ダッシュレット</p> | <p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>以下を表示するには、チャートにカーソルを合わせます。</p> <ul style="list-style-type: none"> <li>• 動作電力レベル</li> <li>• 無線数</li> <li>• Neighbor Count</li> </ul> <ul style="list-style-type: none"> <li>• [TREND] : 時間範囲内のさまざまな電力レベルで動作している AP の数と、無線数の割合と選択された時間が表示されます。</li> </ul> <p>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。</p> <p>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。</p> <p>[LATEST] タブで、グラフの色セグメントまたは [View Details] リンクをクリックして、[Power Distribution Details] スライドイン ペインを開きます。</p> <ol style="list-style-type: none"> <li>1. グラフにカーソルを合わせると、選択した建物の [Operating Power Level]、[Radio Count]、および [Neighbor Count] が表示されます。</li> <li>2. 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。 <ul style="list-style-type: none"> <li>• アクセスポイント</li> <li>• カバレッジホール数</li> <li>• 送信電力 (dBm)</li> <li>• 送信電力レベル</li> <li>• ネイバー密度メトリック</li> <li>• デルタ平均ネイバー送信電力 (dB)</li> </ul> </li> </ol> <p>(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。</p> <ol style="list-style-type: none"> <li>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。</li> </ol> |

- ステップ 11** [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 12** [Service Bundle] エリアで、[Request a Latest Service Bundle] リンクをクリックして、選択した建物のサービスバンドルをダウンロードします。
- ステップ 13** 過去 1 時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] を指定します。
- ステップ 14** [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を使用して、建物の RF 環境のトラブルシューティングと分析を行い、より優れた RRM サービスを実現できます。

---





## 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 \(377 ページ\)](#)
- [インテリジェントキャプチャ対応デバイス \(378 ページ\)](#)
- [インテリジェントキャプチャのベストプラクティス \(379 ページ\)](#)
- [クライアントデバイス向けのライブおよびスケジュール済みキャプチャセッション \(380 ページ\)](#)
- [クライアントデバイス向けデータパケットキャプチャ \(388 ページ\)](#)
- [アクセスポイント向けインテリジェントキャプチャ \(395 ページ\)](#)
- [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 \(406 ページ\)](#)

## インテリジェントキャプチャについて

Cisco DNA Center では、デバイスやクライアントの正常性に関するすべての情報は、通常シスコワイヤレスコントローラから入手できます。インテリジェントキャプチャ機能は Cisco DNA Center とアクセスポイント (AP) 間の直接通信リンクをサポートしているため、各 AP は Cisco DNA Center と直接通信できます。Cisco DNA Center はこのチャンネルを使用して、パケットキャプチャデータ、AP とクライアントの統計情報、およびスペクトルデータを受信できます。インテリジェントキャプチャ機能は、Cisco DNA Center と AP 間の直接通信リンクを利用することで、ワイヤレスコントローラからはアクセスできないデータに AP からアクセスできるようにします。



- (注)
- インテリジェントキャプチャは、ローカルモードまたは FlexConnect モードの AP でのみサポートされます。
  - インテリジェントキャプチャは、SDA 展開ではサポートされていません。

## インテリジェントキャプチャ対応デバイス

インテリジェントキャプチャをサポートするシスコ ワイヤレス コントローラを次の表に示します。

| サポート対象の Cisco Catalyst ワイヤレスコントローラ |                      |
|------------------------------------|----------------------|
| デバイス                               | サポート対象の最小ソフトウェアバージョン |
| Cisco 3504 ワイヤレス コントローラ            | AireOS 8.8.125.0     |
| Cisco 5520 ワイヤレス コントローラ            | AireOS 8.8.125.0     |
| Cisco 8540 ワイヤレス コントローラ            | AireOS 8.8.125.0     |

インテリジェントキャプチャをサポートする Cisco Catalyst ワイヤレスコントローラを次の表に示します。

| サポート対象の Cisco Catalyst ワイヤレスコントローラ    |                            |
|---------------------------------------|----------------------------|
| デバイス                                  | サポート対象の最小ソフトウェアバージョン       |
| Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ | IOS-XE Gibraltar 16.12.1.s |

インテリジェントキャプチャをサポートする Cisco AP を次の表に示します。

| サポート対象の Cisco AP                  |                              |                              |
|-----------------------------------|------------------------------|------------------------------|
| デバイス                              | サポート対象 AireOS ソフトウェアの最小バージョン | サポート対象 IOS-XE ソフトウェアの最小バージョン |
| Aironet 1540 AP <sup>3</sup>      | 8.10.105.0                   | 16.12.1.s                    |
| Aironet 1560 AP                   | 8.10.105.0                   | 16.12.1 s                    |
| Aironet 1815 AP <sup>1</sup>      | 8.10.105.0                   | 16.12.1 s                    |
| Aironet 1830 AP <sup>1</sup>      | 8.10.105.0                   | 16.12.1 s                    |
| Aironet 1840 AP <sup>1</sup>      | 8.10.105.0                   | 16.12.1 s                    |
| Aironet 1850 AP <sup>1</sup>      | 8.10.105.0                   | 16.12.1 s                    |
| Aironet 2800 シリーズ AP              | 8.8.125.0 または 8.10           | 16.12.1s                     |
| Aironet 3800 シリーズ AP              | 8.8.125.0 または 8.10           | 16.12.1s                     |
| Aironet 4800 シリーズ AP <sup>4</sup> | 8.8.125.0 または 8.10           | 16.12.1s                     |
| Catalyst 9105 AP <sup>1</sup>     | 8.10 MR3                     | 17.3.1                       |
| Catalyst 9115 AP <sup>1</sup>     | 8.10.105.0                   | 16.12.1 s                    |

| サポート対象の Cisco AP                   |                                      |                                |
|------------------------------------|--------------------------------------|--------------------------------|
| デバイス                               | サポート対象 AireOS ソフトウェアの最小バージョン         | サポート対象 IOS-XE ソフトウェアの最小バージョン   |
| Catalyst 9120 AP                   | 8.10.105.0<br>8.10.112.0 (スペクトル解析向け) | 16.12.1s<br>17.2.1 (スペクトル解析向け) |
| Catalyst 9130 AP <sup>2</sup>      | 8.10 MR3                             | 17.3.1                         |
| Catalyst IW6300 Heavy Duty シリーズ AP | 8.10.105.0                           | 17.1.1s                        |
| Catalyst ESW6300 組み込みサービス AP       | 8.10.105.0                           | 17.1.1s                        |

<sup>3</sup> スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、Catalyst 9105 AP、および Catalyst 9115 AP ではサポートされていません。

<sup>4</sup> データパケットキャプチャは、Aironet 4800 AP および Catalyst 9130 AP のみでサポートされます。

## インテリジェントキャプチャのベストプラクティス

インテリジェントキャプチャ機能を Cisco DNA Center で確実に最適化するためのベストプラクティスを以下で紹介します。

- 新しいワイヤレスコントローラデバイスを Cisco DNA Center に追加したら、インテリジェントキャプチャのグローバル設定を無効にしてから、設定を再度有効にします。これで、新しいワイヤレスコントローラにインテリジェントキャプチャが設定されます。
- Cisco DNA Center からワイヤレスコントローラデバイスを削除する前に、すべてのインテリジェントキャプチャ設定を無効にします。
- 管理対象のワイヤレスコントローラのアップグレードや Cisco DNA Center の再イメージ化の前に、すべてのインテリジェントキャプチャ設定を無効にします。アップグレード完了後に設定を再度有効にします。

# クライアントデバイス向けのライブおよびスケジュール済みキャプチャセッション

## クライアントデバイス向けのキャプチャセッションについて

クライアントデバイスに対して、次の種類のキャプチャセッションを実行できます。

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。このデータは [Client 360] > [Intelligent Capture] ページに表示されます。セッションは、すぐに開始することも ([Run Now])、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 時間に設定されています。デフォルトでは、最後にクライアントに接続されたワイヤレスコントローラでキャプチャが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。

### オンボーディング キャプチャ セッションの制限事項

オンボーディング キャプチャ セッションの制限事項は次のとおりです。

- キャプチャセッション（ライブおよびスケジュール済み）には合計 16 個のタイムスロットが割り当てられています。セッション内の各クライアントは 1 つのタイムスロットを使用します。

ライブキャプチャセッションの最大数は 16 であるため、16 のライブキャプチャセッションが同時に実行されている場合は、スケジュール済みキャプチャセッションに使用できるスロットはありません。

同時に実行可能なスケジュール済みキャプチャセッションは、最大 12 です。このため、常に 4 個（16 - 12）のスロットがライブキャプチャセッション用に確保されています。

たとえば、17 個目のライブキャプチャセッションを開始しようとする、この最大値を超えるため、次のエラーメッセージが表示されます。エラーメッセージのダイアログボックスで [Yes] をクリックし、次に終了するライブキャプチャセッションを選択します。



(注) 16 個のタイムスロット制限は、ワイヤレスコントローラによって適用されます。

キャプチャセッションが Cisco DNA Center で設定されている場合、Cisco DNA Center が認識していないライブキャプチャセッションやスケジュール済みのキャプチャセッションはすべて削除されます（ワイヤレスコントローラで直接設定された部分的なパケットキャプチャセッションなど）。



- オンボーディングイベント期間中は、オンボーディングイベントに関連した最大 100 パケットのキャプチャが可能です。
- Cisco DNA Center に格納するすべてのスケジュール済みオンボーディング パケット ファイルの合計サイズには、3.5GB の制限があります。制限を超えると、合計サイズが 3.5GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

## クライアント統計情報について

グローバル設定のオンボーディング 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。

収集されたクライアント統計情報は、[Client 360] > [Intelligent Capture] ウィンドウの 4 つの RF 統計情報チャートに表示されます。

## クライアントデバイスのライブキャプチャセッションの有効化

以下の手順により、特定のクライアントデバイスに対してライブキャプチャセッションを有効にし、オンボーディングイベントと RF 統計情報のデータパケットを表示できます。

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

[Overall health] ダッシュボードが表示されます。

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

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

**ステップ 3** 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- [クライアントデバイス (Client Devices)] 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索 (Search)] フィールド (右上端) に次のいずれかを入力します。ユーザ ID (Cisco ISE により認証済み)、IP アドレス、MAC アドレス。

クライアントデバイスの 360 度ビューが表示されます。

**ステップ 4** [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

**注目** [GRPC link is not ready (CONNECTING)] というメッセージ付きの ▲ アイコンがクライアント名の横に表示される場合は、クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center (406 ページ) で詳細を確認してください。

図 42: 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          | <p>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。</p> <p>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 [&lt;] ボタンと [&gt;] ボタンをクリックします。</p> <p>(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。</p> <p>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。</p> |


ステップ 6 ライブキャプチャセッションを実行するには、次の手順を実行します。

- a) ライブキャプチャセッションを開始するには、右上隅にある [Start Live Capture] をクリックします。ライブキャプチャセッション中、[Onboarding Events] と [RF Statistics] ダッシュレットのデータパケットが収集されます。

- b) ライブキャプチャセッションを停止するには、[Stop Capturing] ボタンをクリックします。  
 (注) ライブキャプチャセッションは3時間実行されます。3時間が経過すると、セッションを延長するためのダイアログボックスが表示されます。
- c) 実行中のライブキャプチャセッションは、クライアントの [Intelligent Capture Settings] ウィンドウで確認できます。

**ステップ7** ネットワーク接続の確立に関連付けられているイベントを表示するには、[Onboarding Events ダッシュレット]を使用します。

| [Onboarding Events] ダッシュレット |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [All]および Anomaly PCAP フィルタ  | <p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• Anomaly PCAP : 異常イベントのみをフィルタ処理します。</li> </ul> <p>(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。</p> <p>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。</p>                                                                                                             |
| Export PCAP                 | <p>指定されたイベントの範囲の packets をダウンロードできます。</p> <ol style="list-style-type: none"> <li>1. [Export PCAP] をクリックします。</li> <li>2. PCAP に含める最初と最後のイベントを指定します。</li> <li>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。</li> </ol> <p>(注) ヒューリスティックを使用してイベントに属する packets 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 packets 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 packets がダウンロードされた PCAP に含まれるようになります。</p> <p>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 packets までに制限されます。</p> |

| [Onboarding Events] ダッシュレット |                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                         |
| オンボーディング、不完全、および異常イベントのリスト  | <p>オンボーディング、不完全、および異常イベントのリストを時系列順に表示します。イベントは、以下を示すために色分けされています。</p> <ul style="list-style-type: none"><li>● : 正常なオンボーディングイベント。</li><li>● : 不完全なイベント。</li><li>● : 異常イベント。</li></ul> <p>(注)  アイコン付きのイベントは、このイベントのデータパッケージ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。</p> <p>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。</p> |

| [Onboarding Events] ダッシュレット |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                        | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Event Details               | <p>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。</p> <p>[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。</p> <p>[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 packets をキャプチャした場合に表示されます。イベントの横に表示される  アイコンは、イベントによって packets がキャプチャされたことを示します。</p> <p>[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。</p> <ul style="list-style-type: none"> <li>• イベントを囲む packets (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 packets 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 packets を示します。</li> </ul> <p>認証解除 packets と予期しない packets 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 packets です。</p> <p>[Download Packets] をクリックすると詳細分析のために packets をダウンロードできます。</p> <ul style="list-style-type: none"> <li>• packets (クライアントまたは AP からの packets)</li> <li>• オンボード packets のステージ識別子</li> <li>• packets 間ギャップ (ms)</li> <li>• packets ごとの RSSI (dBm)</li> <li>• 関連付けられている AP</li> </ul> <p>[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。</p> <p>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 packets と Rx packets、および Tx packets の再試行で構成されます。</p> <p>(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 packets はキャプチャされます。</p> |

ステップ 8 [Client Location] ダッシュレットでは、フロアマップを表示して次の情報を確認できます。

- フロア上のクライアントと AP の場所。
- 色の強度でカバレッジの強度を表すヒートマップ。
- フロアマップ上のクライアントのリアルタイムロケーション。クライアントが別の場所に移動すると、その移動が表示されます。
- RF 統計情報 (RSSI、SNR、データレート、スループット、およびパケットドロップレート) を使用して接続が色分け表示されたクライアント証跡トラッキング。  
マップ上の色は、クライアントの正常性を示します。  
● : 良い ● : 平均 ● : 悪い
- 選択したオンボーディングイベントの時間を含む 1 分間のクライアントのトラッキング。
- マップの下のリプレイおよび停止/開始のコントロールを使用すると表示をコントロールできます。


(注) クライアントロケーション機能を使用するには、CMX が Cisco DNA Center と統合されている必要があります。詳細については、「[ワイヤレスマップ向け Cisco CMX の統合 \(415 ページ\)](#)」の章を参照してください。

**ステップ 9** [RF Statistics] ダッシュレットでは、RF 情報の詳細を確認できます。

クライアントの AP クライアント統計情報は、4 つのチャートに表示されます。[クライアント統計情報について \(381 ページ\)](#) を参照してください。データは色分けされていて、次の情報が含まれています。

- RSSI および SNR の測定値 (デシベル単位)。
- Rx 平均データレート (直近の 5 秒間) および Rx 最新データレート。
- Tx パケットおよび Rx パケット。
- Tx パケットの再試行。

チャートでは、次の操作を実行できます。

- チャートにカーソルを重ねると、特定の時点の統計を表示できます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルト表示に変更するには、 アイコンをクリックします。

**ステップ 10** クライアントデバイスのデータパケットキャプチャを実行するには、「[クライアントデバイスのデータパケットキャプチャの実行 \(390 ページ\)](#)」を参照してください。

## クライアントデバイス向けキャプチャセッションのスケジュールと管理

スケジュール済みのキャプチャセッションを停止、編集、削除するには、次の手順を実行します。

クライアントキャプチャセッションは、次のデータを収集します。

- オンボーディングイベントのデータパケットおよび **[Client 360] > [Intelligent Capture]** ウィンドウに表示される **[RF Statistics]** チャートデータ（5秒のサンプル）。[クライアントデバイスのライブキャプチャセッションの有効化（381 ページ）](#) を参照してください。
- **[Device 360] > [Intelligent Capture]** ウィンドウに表示されるチャートおよび表のデータ。[RF 統計情報の表示とアクセスポイントのスペクトル解析データの管理（400 ページ）](#) を参照してください。

**ステップ 1** メニューアイコン（☰）をクリックして、**[Assurance] > [Intelligent Capture Settings]**。

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

**ステップ 2** クライアント キャプチャ セッションをスケジュールするには、**[+ Schedule Client Capture]** をクリックします。

**[Schedule Client Capture]** スライドインペインで、次の設定を行います。

- a) **[Start Time]** エリアで、キャプチャセッションを開始するタイミングを指定します。**[Run Now]**、**[Run Later]** のどちらかを選択できます。
- b) **[Duration]** ドロップダウンリストをクリックして期間を指定します。
- c) **[Select Client Devices]** ドロップダウンリストをクリックすると、カテゴリの一致を返す検索文字列を入力できます（クライアント ユーザー ID、ホスト名、MAC アドレス）。

（注） 検索では、カテゴリごとに最大 10 個の一致が返されるため、エントリが見つからない場合は検索文字列を再調整します。

（注） キャプチャセッションの詳細については、[クライアントデバイス向けのキャプチャセッションについて（380 ページ）](#) を参照してください。

d) **[Save]** をクリックします。

**ステップ 3** 実行中のキャプチャセッションを停止するには、次の手順を実行します。

- a) **[In-progress Captures]** タブをクリックします。
- b) テーブルからクライアントを選択します。
- c) **[Stop Capture]** をクリックします。

**ステップ 4** 将来の時間にスケジュールされたキャプチャセッションを編集するには、次の手順を実行します。

- a) **[Scheduled Captures]** タブをクリックします。
- b) テーブルからクライアントを選択します。

- c) [Edit Schedule] をクリックします。

**ステップ 5** 完了したキャプチャセッションを削除するには、次の手順を実行します。

- a) [Completed Captures] タブをクリックします。
- b) テーブルからクライアントを選択します。
- c) [Delete Schedule] をクリックします。

## クライアントデバイス向けデータパケットキャプチャ

### クライアントデバイス向けデータパケットキャプチャについて

データパケットキャプチャを使用すると、ネットワークデータをPCAPファイルにキャプチャできます。このファイルは Wireshark でダウンロードして表示できます。さらに、Network Analysis Module (NAM) と統合すれば、クライアントデバイスに関する情報（アクセスされたアプリケーションとポート、QoS データ、パケット損失、ワイヤレス遅延、ジッター）をキャプチャできます。詳細については、[NAM 統合について \(388 ページ\)](#) および [クライアントデバイスのデータパケットキャプチャの実行 \(390 ページ\)](#) を参照してください。

#### データパケットキャプチャの制限事項

データパケットキャプチャには、次の制限事項があります。

- データパケットキャプチャは、Cisco Aironet 4800 AP および Cisco Catalyst 9130 AP でのみサポートされます。データパケットキャプチャが有効になっていて、クライアントがパケットキャプチャに対応していない AP にローミングした場合、クライアントがパケットキャプチャ対応の AP に再接続するまで、パケットキャプチャは停止します。
- 一度に実行できるデータパケットキャプチャセッションは1つだけです。
- すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Center とシスコワイヤレスコントローラの間でクロックを同期させる必要があります。ワイヤレスコントローラが Network Time Protocol (NTP) サーバーに接続されていることを確認します。
- 各データパケットキャプチャセッションで最大 1 GB のローリングデータをキャプチャできます。ダウンロードを高速化するために、1 GB のデータが 10 個の 100 MB のファイルに分割されます。

### NAM 統合について

ソフトウェアバージョン 6.4(2)以降を実行中の Network Analysis Module (NAM) または vNAM サーバーをご使用の場合は、お使いの NAM サーバーを Cisco DNA Center と統合できます。イ



インストールと設定の詳細については、[Cisco Prime 仮想ネットワーク解析モジュール \(vNAM\) インストールおよびコンフィギュレーションガイド \[英語\]](#) を参照してください。

クライアントに対して NAM 統合とフルパケットキャプチャを有効にすると、[Client 360] > [Intelligent Capture] ウィンドウの [Wireless Packet Application Analysis] チャートにデータが提供されます。このテーブルとチャートには、クライアントが使用するアプリケーション、その QoS 設定、パケット損失、ワイヤレス遅延、およびジッターに関する情報が表示されます。

NAM サーバーを Cisco DNA Center と統合するには、次の手順を実行します。

1. NAM データポートで IP アドレスを設定します。
2. gRPC コレクタを設定します。



(注) NAM 統合は、IPv6 アドレスを使用する Cisco DNA Center クラスタではサポートされません。

## NAM データポートでの IP アドレス設定

NAM や vNAM のデータポートに有効な IP アドレスを設定するには、次の手順を実行します。この手順は、NAM と統合するために必要です。



(注) データポートはパケットを受信するためだけのもので、要求には応答しません。したがって、IP アドレスを正しく設定していても、データポートに ping を実行するとタイムアウトになります。IP アドレスが有効で、Cisco DNA Center から到達可能であることを確認します。

**ステップ 1** NAM サーバーの CLI にログインします。

**ステップ 2** コマンド **show data-port ip-addresses** を入力します。  
コマンドにより、ポート番号と IP アドレスが表示されます。

```
Device# show data-port ip-addresses
Port number: 1
IPv4 address: 172.20.125.125
```

**ステップ 3** **show data-port ip-addresses** コマンドで何も表示されない場合、コマンド **data-port 1 ip-address ip-address** を入力して、IP アドレスをポート 1 に割り当てます。

**ステップ 4** **show data-port ip-addresses** コマンドを再度実行し、そのデータポート 1 が IP アドレスに割り当てられたことを確認します。

**ステップ 5** データポート 1 またはその他の表示されているポートの IP アドレスの 1 つを記録します。

**ステップ 6** **cdb-export** が Cisco DNA Center で有効であることを確認します。そのためには、**show cdb-export all** コマンドを入力します。何も表示されない場合は、コマンド **cdb-export collector 1 ip-address IP-address-of-Cisco-DNA-Center** を入力します。

**ステップ 7** コマンド **autocreate-data-source erspan** を入力して、Cisco DNA Center からのデータパケットが処理されていることを確認します。

**ステップ 8** NAM や vNAM サーバーと Cisco DNA Center で時間が同期していることを確認します。NAM ユーザーインターフェイスから **[Administration] > [System] > [System Time]** の順に選択することにより、時刻を同期できます。

---

## gRPC コレクタの設定

この手順を gRPC コレクタに対して実行して NAM を統合します。gRPC は、オープンソースの高パフォーマンス RPC (リモートプロシージャコール) フレームワークです。

### 始める前に

NAM データポートで IP アドレスを設定します。[NAM データポートでの IP アドレス設定 \(389 ページ\)](#) を参照してください。

---

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

[Data Centers] ウィンドウが表示されます。

**ステップ 2** [Collectors] タブをクリックします。

[Collectors] ウィンドウが表示されます。

**ステップ 3** [GRPC-COLLECTOR] をクリックします。

[GRPC-COLLECTOR] ウィンドウが表示されます。

**ステップ 4** [+ Add] をクリックします。

[gRPC Collector Configuration] ウィンドウが表示されます。

**ステップ 5** [GRPC-COLLECTOR] 設定を 1 つだけ追加します。次の手順を実行します。

- [ConfigData] エリアで [Agent Export] チェックボックスをオンにして、ネットワークパケットデータの NAM へのエクスポートを有効にします。
- [Agent IP Address] フィールドに、記録したデータポートの IP アドレスを入力します ([NAM データポートでの IP アドレス設定 \(389 ページ\)](#) の [ステップ 5 \(389 ページ\)](#) を参照してください)。
- [Configuration Name] フィールドに、GRPC-コレクタ設定の一意の名前を入力します。
- [Save Configuration] をクリックします。

---

## クライアントデバイスのデータパケットキャプチャの実行

この手順では、クライアントデバイスのデータパケットキャプチャを実行する方法を示します。

### 始める前に

アクセスされたアプリケーションとポート、QoSデータ、パケット損失、ワイヤレス遅延、およびジッターに関する情報を取得するには、NAM 統合を有効にする必要があります。詳細については、「[NAM 統合について \(388 ページ\)](#)」を参照してください。

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

[Overall health] ダッシュボードが表示されます。

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

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

**ステップ 3** 次のいずれかを実行して、特定のクライアントの [Client 360] ウィンドウを開きます。

- [クライアントデバイス (Client Devices) ] 表で、ハイパーリンク付きの識別子またはデバイスの MAC アドレスをクリックします。
- [検索 (Search) ] フィールド (右上端) に次のいずれかを入力します。ユーザ ID (Cisco ISE により認証済み)、IP アドレス、MAC アドレス。

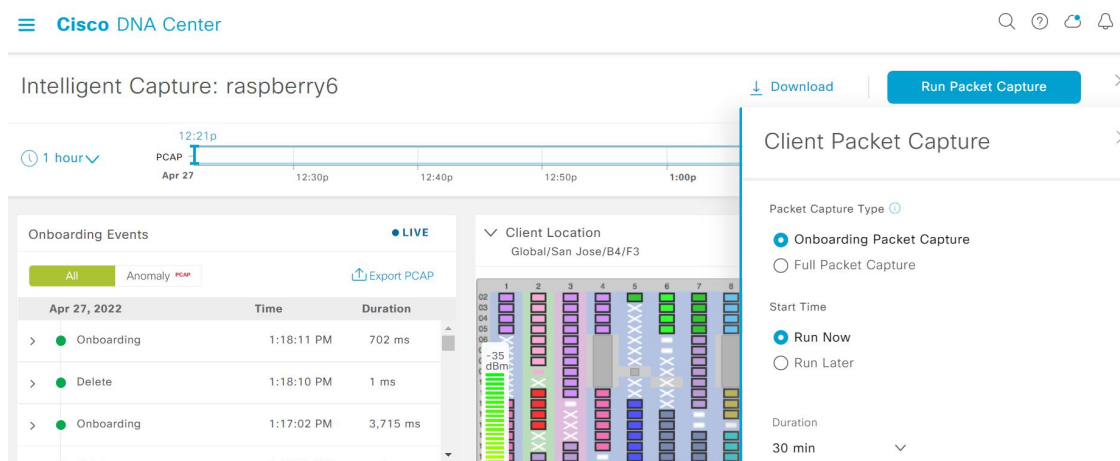
クライアント デバイスの 360 度ビューが表示されます。

**ステップ 4** [Client 360] ウィンドウで、[Intelligent Capture] をクリックします。

[Intelligent Capture: Client Device] ウィンドウに次の情報が表示されます。

**注目** [GRPC link is not ready (CONNECTING)] というメッセージ付きの ▲ アイコンがクライアント名の横に表示される場合は、[クライアントまたはアクセスポイントがインテリジェントキャプチャ データを送信できない Cisco DNA Center \(406 ページ\)](#) を参照してください。

図 43: 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          | <p>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 [&lt;] ボタンと [&gt;] ボタンをクリックします。</p> <p>(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。</p> <p>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。</p> |

**ステップ 6** データパケットキャプチャを実行するには、[Data Packet Capture] エリア（右上隅）で次の機能を使用します。

| [Data Packet Capture] エリア |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| [Run Packet Capture] ボタン  | <p>[Run Packet Capture] をクリックして、[Client Packet Capture] スライドインペインを開き、次の手順を実行します。</p> <ol style="list-style-type: none"> <li>[Onboarding Packet Capture] または [Full Packet Capture] オプションボタンをクリックして、[Packet Capture Type] を選択します。</li> <li>[Start Time] を選択します。[Run Now]、[Run Later] のどちらかを選択できます。</li> <li>[Duration] ドロップダウンリストから、パケットキャプチャの期間を選択します。デフォルトは 30 分です。</li> <li>パケットキャプチャを有効にする必要がある [Wireless Controllers] を選択します。ワイヤレスコントローラは最大 3 つまで選択できます。</li> <li>[Save] をクリックします。</li> </ol> <p>(注) 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は、<b>アシュアランス &gt; [Intelligent Capture Settings] &gt; [Client Schedule Capture]</b> の下に表示されます。</p> <p>データパケットキャプチャセッションが Cisco DNA Center で設定されている場合、Cisco DNA Center が認識していないデータパケットキャプチャセッションはすべて削除されます (ワイヤレスコントローラで直接設定されたフルパケットキャプチャセッションなど)。</p> <p>(注) すべてのインテリジェントキャプチャ機能に共通するように、データパケットキャプチャを機能させるためには、Cisco DNA Center とシスコ ワイヤレス コントローラの間でタイムゾーンを同期させる必要があります。ワイヤレスコントローラが Network Time Protocol (NTP) サーバーに接続されていることを確認します。</p> <p>(注) 新しいキャプチャセッションが開始されるたびに、新しい一連の PCAP ファイルが開始されます。</p> |

| [Data Packet Capture] エリア |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                      | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| [Download] ボタン            | <p>フルパケット PCAP ファイルがセッションからキャプチャされたら、このボタンをクリックして PCAP ファイルをダウンロードします。データパケットファイルをダウンロードするには、[Download] 列にあるアイコンをクリックします。次のいずれかのファイルをダウンロードできます。</p> <ul style="list-style-type: none"> <li>• ワイヤレスデータ：AP とクライアント間のパケットの 802.11 ファイル。</li> <li>• 有線データ：AP とスイッチまたはワイヤレスコントローラ間のパケットのイーサネットファイル。</li> </ul> <p>(注) データパケットキャプチャファイルには、100 MB の制限があります。すべてのデータパケットキャプチャファイルの合計は、3.5 GB を超えることはできません。</p> <p>(注) 過去 7 日間の PCAP ファイルのみダウンロードできます。</p> |

**ステップ 1** [Wireless Packet Application Analysis] ダッシュレットでは、データパケットキャプチャの詳細を確認できません。

データパケットキャプチャが実行されている場合、このダッシュレットには、アクセスされたアプリケーションとポート、QoS データ、パケット損失、ワイヤレス遅延、およびジッターなど、分析されたパケットに関する詳細が表示されます。

(注) このダッシュレットにデータを表示するには、NAM の統合を設定する必要があります。[NAM 統合について \(388 ページ\)](#) を参照してください。

## クライアントのデータパケットキャプチャ履歴の表示

クライアントのデータパケットキャプチャセッションの履歴（最初のパケットと最後のデータパケットがキャプチャされた時刻、キャプチャされたデータパケットの合計サイズ、パケットのタイプなど）を表示するには、以下の手順を実行します。

**ステップ 1** メニューアイコン (☰) をクリックして、[Assurance] > [Intelligent Capture Settings]。

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

**ステップ 2** [Client Data Packet Capture] タブをクリックします。

[Client Data Packet Control] ウィンドウが表示されます。

**ステップ 3** [Intelligent Capture Settings - Client Data Packet Capture] ウィンドウには、次の情報が表示されます。

| オプション               | 説明                                                                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------|
| [Identifier]        | クライアントのユーザー ID またはホスト名が表示されます。ユーザー ID またはホスト名をクリックすると、[Intelligent Capture: Client Device] ウィンドウが開きます。 |
| [MAC Address]       | クライアントデバイスの MAC アドレスが表示されます。                                                                           |
| [First Packet Time] | 最初のデータパケットがキャプチャされた時刻が表示されます。                                                                          |
| [Last Packet Time]  | 最後のデータパケットがキャプチャされた時刻が表示されます。                                                                          |
| [Total Size]        | キャプチャされたデータの合計サイズが表示されます。                                                                              |
| [Currently Running] | データパケットキャプチャが実行中かどうかを表示します。                                                                            |
| [Type of Packet]    | パケットのタイプ ([Wired]、[Wireless] など) が表示されます。                                                              |

## アクセスポイント向けインテリジェントキャプチャ

### アクセスポイントのインテリジェントキャプチャについて

AP インテリジェントキャプチャ機能を使用すると、1 つ以上の AP で次のデータをキャプチャできます。

- **AP 統計情報キャプチャ**には、次の情報が含まれます。
  - **[Device 360] > [Intelligent Capture]** ウィンドウの **[RF Statistics]** タブに表示される AP 無線および WLAN 統計情報。
  - 選択した AP に関連付けられているすべてのクライアントの **[Client 360] > [Intelligent Capture]** ウィンドウで **[RF Statistics]** エリアに表示される AP クライアントの統計情報 (サンプリング時間は 30 秒)。
- **異常キャプチャ**は、選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント (グローバルまたは選択した AP に関連付けられているすべてのクライアント) をキャプチャして、ダウンロードまたは表示できます。

#### キャプチャの制限事項

Cisco DNA Center に格納する異常をトリガーしたパケットファイルの合計サイズには、1.05 GB の制限があります。制限を超えると、合計サイズが 1.05 GB の制限を下回るまで、最も古いパケットファイルから順番に削除されます。

## アクセスポイントのインテリジェントキャプチャの有効化と管理

1つまたは複数のアクセスポイント（AP）を有効にして次のデータをキャプチャするには、以下の手順を実行します。

- **AP 統計情報**：AP 無線の統計情報、WLAN 統計情報、および AP クライアントの統計情報が含まれます。
- **異常キャプチャ**：選択した 1 つ以上の AP に関連付けられているすべてのクライアントの異常なオンボーディングイベントに関する情報です。異常キャプチャを有効にすると、すべての異常なオンボーディングイベント（グローバルまたは選択した AP に関連付けられているすべてのクライアント）をキャプチャして、ダウンロードまたは表示できます。

**ステップ 1** メニューアイコン（☰）をクリックして、**[Assurance] > [Intelligent Capture Settings]**。

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

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

[Access Point] ウィンドウが表示されます。

**ステップ 3** AP 統計情報キャプチャを有効または無効にするには、次のいずれかを実行します。

- 有効な AP がない場合は、[Configure AP Enablement] エリアが表示されます。[Specific] または [Global] のいずれかのオプションを選択し、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[AP Stats Capture] ウィンドウが表示されます。[AP Stats Capture] ウィンドウで、次のいずれかのオプションを選択します。

| オプション                         | 説明                                                                                               |
|-------------------------------|--------------------------------------------------------------------------------------------------|
| <b>None - disable all APs</b> | 1 つ以上の AP が有効になっている場合は、「None - disable all APs」と表示されます。<br>現在有効になっているすべての AP で統計情報キャプチャを無効にできます。 |



| オプション                                                   | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Specific - select specific APs and enable</b></p> | <p>選択した AP の 統計情報キャプチャを有効にできます。次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [Specific - select specific APs and enable] オプションボタンをクリックします。</li> <li>2. 左側のペインで、[Global] を展開し、サイト &gt; ビルディング &gt; フロア の順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。</li> <li>3. 選択した AP の統計情報キャプチャを有効にするには、次の手順を実行します。 <ul style="list-style-type: none"> <li>• [Disabled APs] タブをクリックします。統計情報キャプチャが現在無効になっている AP のリストが表示されます。</li> <li>• 統計情報キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。</li> </ul> </li> <li>4. 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 <p>(注) 互換性のない AP の条件は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 動作モードが [local] または [FlexConnect] に設定されていない。</li> <li>• AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。</li> </ul> </li> </ol> |
| <p><b>Global - enable all capable APs</b></p>           | <p>すべての対応 AP で統計情報キャプチャを有効にできます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**ステップ 4** 異常キャプチャを有効または無効にするには、[Anomaly Capture] タブをクリックして、次のいずれかを実行します。

- 有効になっている AP がない場合は、[Configure AP Enablement] エリアが表示されます。次のいずれかのオプションを選択してから、[Get Started] をクリックします。
- 1 つ以上の AP が有効になっている場合は、[Anomaly Capture] ウィンドウが表示されます。[Anomaly Capture] ウィンドウで、次のいずれかのオプションを選択します。

| オプション                         | 説明                                                                                        |
|-------------------------------|-------------------------------------------------------------------------------------------|
| <b>None - disable all APs</b> | 1つ以上のAPが有効になっている場合は、「None - disable all APs」と表示されます。<br>現在有効になっているすべてのAPで異常キャプチャを無効にできます。 |

| オプション                                                              | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Specific - select specific APs and enable or disable</b></p> | <p>選択した AP の異常キャプチャを有効または無効にできます。次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. [Specific - select specific APs and enable or disable] オプションボタンをクリックします。</li> <li>2. 左側のペインで、[Global] を展開し、サイト &gt; ビルディング &gt; フロアの順にドリルダウンします。右側のペインには、そのフロアにある AP のリストが表示されます。[Enabled APs]、[Disabled APs]、[Not-Ready APs] の 3 つのタブがあります。</li> <li>3. 選択した AP の異常キャプチャを有効にするには、次の手順を実行します。 <ul style="list-style-type: none"> <li>• [Disabled APs] タブをクリックします。異常キャプチャが現在無効になっている AP のリストが表示されます。</li> <li>(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。</li> <li>• 異常キャプチャを有効にする AP の横にあるチェックボックスをオンにして、[Enable] をクリックします。</li> </ul> </li> <li>4. 選択した AP の異常キャプチャを無効にするには、次の手順を実行します。 <ul style="list-style-type: none"> <li>• [Enabled APs] タブをクリックします。異常キャプチャが現在有効になっている AP のリストが表示されます。</li> <li>• 異常キャプチャを無効にする AP の横にあるチェックボックスをオンにして、[Disable] をクリックします。</li> </ul> </li> <li>5. 互換性のない AP を表示するには、[Not-Ready APs] タブをクリックします。 <ul style="list-style-type: none"> <li>(注) 互換性のない AP の条件は次のとおりです。 <ul style="list-style-type: none"> <li>• 動作モードが [local] または [FlexConnect] に設定されていない。</li> <li>• AP にインストールされている OS リリースには互換性がありません。OS リリースは MR1 以降である必要があります。</li> </ul> </li> </ul> </li> <li>6. インテリジェントキャプチャをサポートしている AP のリストを表示するには、[Not-Ready APs] タブの横にある情報 (I) アイコンをクリックします。</li> </ol> |

| オプション                           | 説明                          |
|---------------------------------|-----------------------------|
| Global - enable all capable APs | すべての対応 AP の異常キャプチャを有効にできます。 |

## RF統計情報の表示とアクセスポイントのスペクトル解析データの管理

RF 統計情報を表示し、特定のアクセスポイントのスペクトル解析データを開始および管理するには、次の手順を実行します。

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

[Overall health] ダッシュボードが表示されます。

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

[Network Health] ウィンドウが表示されます。

**ステップ 3** 次のいずれかを実行します。

- [Network Devices] ダッシュレットで、AP のデバイス名 (ハイパーリンクされた識別子) をクリックし、AP の詳細を表示します。
- [Search] フィールド (右上隅にあります) で、デバイス名、IP アドレス、または MAC アドレスを入力します。

AP の 360 度ビューが表示されます。

**ステップ 4** [Client 360] ウィンドウで、右上隅にある [Intelligent Capture] をクリックします。

[Intelligent Capture: AP Name] ウィンドウが表示されます。

**注目** AP 名の横にメッセージ「**GRPC リンクはまだ利用できません (接続中) (GRPC link is not ready (CONNECTING))**」付きの ▲ アイコンが表示された場合、詳細については [クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center \(406 ページ\)](#) を参照してください。

**ステップ 5** [RF Statistics] タブをクリックすると、RF 統計情報の詳細が表示されます。

(注) [AP Stats Capture] が有効になっていない場合は、有効にします。 [アクセスポイントのインテリジェントキャプチャの有効化と管理 \(396 ページ\)](#) を参照してください。


**ステップ 6** [RF Statistics] タブでは、次の操作を実行できます。

- a) タイムラインを使用すると、指定された時間の RF 統計情報を表示し、データの範囲を指定できます。

| タイムラインスライダ          |                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム                | 説明                                                                                                                                                                                                                                                                |
| [1 hour] ドロップダウンリスト | ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。                                                                                                                                                            |
| タイムラインスライダ          | <p>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。</p> <p>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 [&lt;] ボタンと [&gt;] ボタンをクリックします。</p> <p>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。</p> |

- b) タイムラインの下にある無線周波数セレクトアを使用すると、周波数帯域に基づいてダッシュレットに表示されるデータをフィルタ処理できます。ドロップダウンリストをクリックして、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。
- c) このダッシュレットで、RF 統計情報の詳細を確認できます。

(注) ダッシュレットに表示されるチャートでは、次の操作を実行できます。

- 詳細を表示するには、チャートにカーソルを合わせます。
- チャート内をクリックしてドラッグすると、特定の期間を拡大表示できます。ビューをデフォルトに変更するには、 をクリックします。
- チャートの下の色分けされたデータタイプをクリックすると、チャートに表示されているそのデータタイプを無効化または有効化できます。

| ダッシュレット                                              | 説明                                                                                                                                                            |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Clients] ダッシュレット                                    | この AP を使用しているクライアントの数が表示されます。データソースは AP WLAN 統計情報からのものです。                                                                                                     |
| [Top Clients with Tx Failed Packets by SSID] ダッシュレット | <p>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。</p> <p>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。</p> |
| [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ンネル使用率が表示されます。棒グラフのデータソースは、AP 無線統計情報からのものです。                                                                          |

| ダッシュレット                                     | 説明                                                                                                                                                                |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Channel Utilization by this Radio] ダッシュレット | AP によって使用されている現在のチャンネル使用率、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。<br><br>テーブルのデータソースは、AP WLAN 統計情報からのものです。円グラフのデータソースは、AP 無線統計情報からのものです。 |
| [Frame Count] ダッシュレット                       | 管理フレームとデータフレームの数が表示されます。データソースは AP 無線統計情報からのものです。                                                                                                                 |
| [Frame Errors] ダッシュレット                      | 送受信エラーの数が表示されます。データソースは AP 無線統計情報からのものです。                                                                                                                         |
| [Tx Power and Noise Floor] ダッシュレット          | 送信電力とノイズフロアが表示されます。データソースは AP 無線統計情報からのものです。                                                                                                                      |
| [Multicast/Broadcast Counter] ダッシュレット       | 各 SSID のマルチキャストおよびブロードキャストの数が表示されます。データソースは AP WLAN 統計情報からのものです。                                                                                                  |

**ステップ 7** [Spectrum Analysis] タブをクリックします。

**ステップ 8** [Start Spectrum Analysis] タブをクリックし、スペクトル解析セッションを開始します。

- (注)
- スペクトル解析期間は 10 分です。
  - 同時スペクトル解析セッションの最大数は 20 です。

**ステップ 9** [Spectrum Analysis] タブでは、次の操作を実行できます。

- タイムラインを使用すると、指定された時間のスペクトル解析データを、データの範囲を指定して表示できます。

| タイムラインスライダ          |                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------|
| アイテム                | 説明                                                                                                     |
| [1 hour] ドロップダウンリスト | ドロップダウンリストをクリックして期間を選択し、タイムラインの範囲を設定します。オプションは、[1 hour]、[3 hours]、および [5 hours] です。デフォルトは [1 hour] です。 |

| タイムラインスライダ |                                                                                                                                                                                                                                                                                                                                     |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム       | 説明                                                                                                                                                                                                                                                                                                                                  |
| タイムラインスライダ | <p>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。</p> <p>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。</p> <p>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 [&lt;] ボタンと [&gt;] ボタンをクリックします。</p> <p>(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。</p> <p>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。</p> |

- b) タイムラインの下にある無線周波数セクタを使用すると、周波数帯域に基づいてチャートに表示されるデータをフィルタ処理できます。[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 \(405 ページ\)](#) を参照してください。

- c) [Spectrum Analysis] チャートには、次の機能が用意されています。

| スペクトル解析チャート        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| アイテム               | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 上位チャート（パーシステンス）    | <p>このチャートは、RF環境で検知された各信号の振幅（電力）とチャン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軸はチャンネル周波数を表します。</p> <p>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ンネル周波数で検知される信号の数を表します。</p> <ul style="list-style-type: none"> <li>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。</li> <li>赤色は、オーバーラップする信号の数が多ことを示します。</li> </ul> <p>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 &gt; 緑色 &gt; 黄色 &gt; オレンジ色 &gt; 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。</p> <p>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。</p> <p>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。</p> <p>特定の範囲のチャン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ンネルのデータが表示されます。</p> <p>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。</p> |
| ボトムチャート（ウォーターフォール） | <p>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軸はチャン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ティングすることができます。</p> <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

d) [Interference and Duty Cycle] チャートには、次の情報が表示されます。

- 検出された干渉とその重大度：
  - 干渉は、半径が干渉の帯域幅を表す円としてプロットされます。X軸は干渉が検出された周波数を表し、Y軸は重大度を表します。



- [Severity] は、干渉と範囲の影響を測定します。範囲は 0（影響がないことを示す）から 100（大きな影響を示す）です。
- 干渉タイプは RF 署名から決定され、Cisco CleanAir テクノロジーによって識別されます。
- 各チャネルのデューティサイクル。

## スペクトル解析時の Cisco AP 機能について

Cisco Aironet 2800 シリーズ、3800 シリーズ、および 4800 シリーズ アクセスポイント (AP) には、フレキシブル ラジオ アサインメント (FRA) を備えたデュアルバンド無線がスロット 0 に搭載されています。この FRA 無線は 2.4 GHz で動作しますが、5 GHz で動作するように割り当てることができます。このモードは、AP の動作モードとは異なるように変更できます。AP の FRA 無線を 5 GHz で動作するように設定すると、クライアント無線は 2.4 GHz 帯域で動作できなくなります。



- (注) スペクトル解析は、Aironet 1540 AP、Aironet 1800 シリーズ AP、および Catalyst 9115 AP ではサポートされていません。



- (注) AP に正しいソフトウェアバージョンがインストールされていることを確認します。[インテリジェントキャプチャ対応デバイス \(378 ページ\)](#) に記載された「サポート対象の Cisco AP」の表を参照してください。

スペクトル解析のための無線スロットの割り当ては次のとおりです。

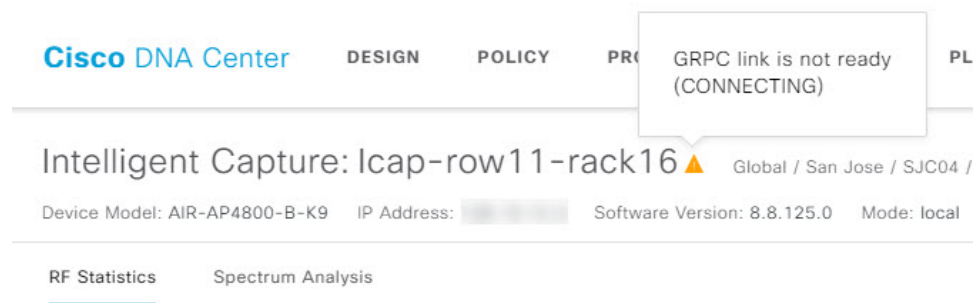
| デバイス モデル                           | スペクトル解析の無線スロットの割り当て        |
|------------------------------------|----------------------------|
| Aironet 2800 シリーズ AP               | 無線スロット 0 および 1 が有効になっています。 |
| Aironet 3800 シリーズ AP               |                            |
| Aironet 1560 AP                    |                            |
| Catalyst IW6300 Heavy Duty シリーズ AP |                            |
| Catalyst IW6300 Heavy Duty シリーズ AP |                            |

| デバイス モデル                                                     | スペクトル解析の無線スロットの割り当て                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aironet 4800 シリーズ AP<br>Catalyst 9120 AP<br>Catalyst 9130 AP | <p>これらの AP には、3 つの無線スロットがあります。</p> <p>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。</p> <p>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。</p> <p>(注) AP スペクトル解析データは、2.4 GHz チャネル帯域では表示されません。また、2.4 GHz 帯域を提供する AP 無線がない場合、[Radio Mode] フィールドと [Channel] フィールドは空になります。こうした状況になるのは、FRA 無線が 5 GHz で動作するように設定され、パケットキャプチャが有効になっている場合です。</p> |

## インテリジェントキャプチャのトラブルシューティング

### クライアントまたはアクセスポイントがインテリジェントキャプチャデータを送信できない Cisco DNA Center

**問題：**クライアントまたはアクセスポイントがインテリジェントキャプチャデータを Cisco DNA Center に送信できません。警告 (▲) アイコンが「**GRPC link is not ready (CONNECTING)**」というメッセージと共に表示されます。



**バックグラウンド：**AP がインテリジェントキャプチャデータを Cisco DNA Center に送信するためには、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 Cisco DNA Center によって検出されると、ポート番号は自動的に 32626 に設定されます。

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

**解決策：**この問題を解決するには、次の作業を実行します。

1. 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。

クライアントまたはアクセスポイントがインテリジェントキャプチャ データを送信できない Cisco DNA Center



## 第 20 章

# デバイスのパスをトレース

- [パス トレースについて \(409 ページ\)](#)
- [パス トレースの既知の制限事項 \(409 ページ\)](#)
- [パス トレースの実行 \(411 ページ\)](#)

## 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実行できます。2つのノードは、有線または無線ホスト、レイヤ3インターフェイスの組み合わせ、あるいは両方で構成できます。さらに、Cisco DNA Center コントローラがパストレース接続（TCP または UDP）を確立する際に使用するプロトコルを指定できます。

パストレースを開始すると、Cisco DNA Center コントローラは、検出されたデバイスのネットワークトポロジおよびルーティングデータを確認して収集します。Cisco DNA Center コントローラはこのデータを使用して、2つのホストまたはレイヤ3 インターフェイス間のパスを計算し、パストレーストポロジにパスを表示します。このトポロジには、パスの方向とパスに沿ったデバイスが含まれ、デバイスの IP アドレスも表示されます。ディスプレイには、パスに沿ったデバイスのプロトコル（**Switched**、**STP**、**ECMP**、**Routed**、**Trace Route**）や、その他のソース タイプも表示されます。

## パス トレースの既知の制限事項

パストレースには次の制限事項および制約があります。

- ファブリッククライアントと非ファブリッククライアントの間のパストレースは、サポートされていません。
- 複数の Virtual Routing Forwarding (VRF) 仮想ネットワーク (VN) 上にある2つのファブリッククライアント間のパストレースは、サポートされていません。
- 複数のサイト (ドメイン) 上にある2つのファブリッククライアント間のパストレースは、サポートされていません。

- いずれかのエッジスイッチがファブリックに含まれていない、同じファブリックの同じサイト内に接続されているクライアントは、サポートされていません。
- ルータのループバック インターフェイスからのパストレースは、サポートされていません。
- 重複する IP アドレスは、ファブリックの有無にかかわらずサポートされていません。
- パストレースを Locator/ID Separation Protocol (LISP) ファブリックで機能させるには、トラフィックが実行されていて、エッジスイッチでキャッシュを利用できることを確認します。
- Cisco 適応型セキュリティアプライアンス (ASA) は CDP をサポートしていないため、Cisco ASA のパストレースはサポートされていません。Cisco ASA アプライアンスを通るパスを識別することはできません。
- タグなしモードのワイヤレスコントローラの管理インターフェイスでは、パストレースはサポートされていません。
- 集中管理型ワイヤレス モビリティ モードの非対称モビリティ トンネリングに対するパストレースは、サポートされていません。
- 仮想スイッチング システム (VSS) 、マルチリンク集約制御プロトコル (MLACP) 、または仮想 PortChannel (vPC) のパストレースはサポートされていません。
- スイッチ仮想インターフェイス (SVI) 上の等コスト マルチパスルーティング (ECMP) のパストレースは、サポートされていません。
- NAT またはファイアウォールを使用するデバイスでのパストレースはサポートされていません。
- Cisco Performance Routing (PfR) は DMVPN トンネルでサポートされていません。
- VLAN ACL (VACL) が有効になっているパストレースは、サポートされていません。
- 非周期的な更新 (NPR) パスシナリオでは、アップグレード後にコントローラでパスは更新されません。また、統計収集が停止します。統計収集を続行するには、新しいパス要求を開始する必要があります。
- Hot Standby Router Protocol (HSRP) VLAN のホストから任意の HSRP ルータに接続されている 非 HSRP VLAN のホストへのパストレースは、サポートされていません。
- オブジェクト グループは ACL トレーシングでサポートされていません。
- ポートチャネルのポート集約プロトコル (PAgP) モードは、サポートされていません。LACP モードのみがサポートされています。
- インターフェイスに異なるパフォーマンス モニター ポリシーが設定されている場合は、Cisco DNA Center を使用したパフォーマンスモニター設定の適用が失敗します。インターフェイスのパフォーマンスモニター設定を削除して、パストレース要求を再送信します。
- パフォーマンスモニター統計情報のパストレースは、Cisco ASR 1000 シリーズルータ (Cisco IOS XE 16.3.1) ではサポートされていません。

- パフォーマンスモニター統計情報のパストレースは、Cisco Catalyst 3850 スイッチ（Cisco IOS XE 16.2.x および 16.3.1）ではサポートされていません。
- Cisco Mobility Express（ME）ワイヤレスコントローラのパストレースはサポートされていません。
- Cisco SD-Access ファブリックで OTT を使用するワイヤレスクライアントのパストレースはサポートされていません。
- レイヤ 2 スイッチからのパストレースはサポートされていません。
- シスコの産業用イーサネット（IE）スイッチは、SD-Access ソリューションの一部として拡張されたノードです。現在、パストレースは拡張ノードを認識していないため、トポロジに拡張ノードが含まれている場合は、エラーメッセージが表示されます。
- デバイス用に IPv4 アドレスと IPv6 アドレスの両方を使用するデュアルスタックはサポートされていません。この状況になると、指定されたアドレスが不明であることを示すエラーメッセージが表示されます。
- シスコ ワイヤレス コントローラは SNMP モビリティトラップを送信しないため、次の点に注意してください。
  - パストレース要求の場合、Cisco DNA Centerの外部ワイヤレスコントローラでは、右側の出力仮想インターフェイスは強調表示されません。
  - パストレース要求では、外部ワイヤレスコントローラに適用されている ACL は強調表示されません。



---

(注) 回避策は、インベントリサイクルが完了するまで待機することです。

---

## パス トレースの実行

パス トレース機能は、すべてのデバイスで同様の方法で動作します。[クライアント 360 (Client 360)] または [デバイス 360 (Device 360)] ウィンドウからパス トレースを実行できます。

### 始める前に

- パス トレースの既知の制限事項を確認してください。パス トレースの既知の制限事項 (409 ページ) を参照してください。
- デバイス (ルータ、スイッチ、ワイヤレス コントローラ、およびアクセス ポイント) が検出されたことを確認します。IP アドレス範囲を使用したネットワークの検出 (29 ページ)、CDP を使用したネットワークの検出 (21 ページ)、または LLDP を使用したネットワークの検出 (37 ページ) を参照してください。

- デバイスで CDP が有効であることを確認してください。

**ステップ 1** [Client 360] または [Device 360] ウィンドウの [Path Trace] カテゴリで、[Run New Path Trace] をクリックします。

[Set up Path Trace] スライドインペインが表示されます。

**ステップ 2** 送信元の IP アドレス、インターフェイス、およびポート番号、宛先の IP アドレス、インターフェイス、およびポート番号を入力します。

| フィールド                         | アクション                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Source] フィールド                | [Source] フィールドの IP アドレスは事前に入力されていますが、次の操作を実行して別の送信元 IP アドレスを入力できます。 <ul style="list-style-type: none"> <li>• 送信元 IP アドレスを入力します。</li> <li>• [Source] フィールドをクリックして、使用可能なオプションから IP アドレスを選択します。</li> </ul> |
| [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。<br>(注) 送信元 IP アドレスがネットワーク デバイスの場合は、このフィールドが表示されます。                                                                                                                          |
| [Port (optional) ] フィールド      | トレースを開始するホストのポート番号を入力します。                                                                                                                                                                               |
| [Destination] フィールド           | 次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• [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。</li> </ul>                     |
| [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。<br>(注) [Destination] フィールドで選択した IP アドレスがネットワーク デバイスの場合、このフィールドが表示されます。                                                                                                      |
| [Port (optional) ] フィールド      | トレースを終了するホストのポート番号を入力します。                                                                                                                                                                               |

**ステップ 3** [Options] エリアで、必要に応じて次の操作を実行します。

| フィールド                 | アクション                           |
|-----------------------|---------------------------------|
| [Protocol] ドロップダウンリスト | (オプション) [tcp] または [udp] を選択します。 |



| フィールド                 | アクション                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [Live Traffic]        | <p>[On] に切り替えて有効にすると、選択したデバイスを通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。</p> <p>[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。</p> <p>(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。</p>                                                                                                          |
| [Refresh Every 30sec] | <p>(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。</p>                                                                                                                                                                                                                                                                                            |
| [ACL Trace]           | <p>(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。</p>                                                                                                                                                                                                                                                                              |
| [Include Stats] オプション | <p>(オプション) 追加の統計を収集するようにパス トレースを設定するには、必要に応じて次のチェック ボックスをチェックします。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> </ul> |

**ステップ 4** [Start] をクリックします。

パス トレース トポロジが表示されます。IP アドレス、プロトコル、およびパス トレースの最終更新日時を示すタイムスタンプが、トポロジの上に表示されます。

**ステップ 5** パストレーストポロジでは、次の操作を実行できます。

a) デバイスにカーソルを合わせると、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。

次の 5 タプル値（送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、使用されているプロトコル）が指定されている場合、表示されている ACL トレースは 100% 正確です。情報が部分的に

指定されている場合、表示されている ACL トレースはベストエフォートに基づきます。このような場合、ACL 結果に許可と拒否の両方が表示される可能性があります。

特定のトラフィックフローで一致した ACL は、色付きのアイコンで表示されます。緑は許可を示します。赤は拒否を示します。入力 ACL の場合、アイコンはデバイスの左側に表示されます。出力 ACL の場合、アイコンはデバイスの右側に表示されます。

- b) デバイスをクリックすると、デバイスの詳細情報を含むスライドインペインが開きます。
  - c) レイヤ 2 または レイヤ 3 ポート チャネル インターフェイスの上にカーソルを重ねると、使用された VLAN や出力ドロップなどの情報が表示されます。[More Details] をクリックすると、追加情報を含むスライドインペインが開きます。
  - d) パスの上にカーソルを重ねると、パスに沿ったデバイスのプロトコル (Switched、STP、ECMP、Routed、Trace Route) や、その他のソース タイプも表示されます。
-



## 第 21 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 \(415 ページ\)](#)
- [Cisco CMX API サーバーへのユーザーの追加 \(415 ページ\)](#)
- [Cisco CMX 設定の作成 \(416 ページ\)](#)
- [Cisco CMX のトラブルシューティング \(418 ページ\)](#)

## Cisco Connected Mobile Experiences の統合について

Cisco DNA Center は、ワイヤレスマップのためのオンプレミス コネクテッド モバイル エクスペリエンス (CMX) の統合をサポートしています。CMX を統合すると、Cisco DNA Center ユーザーインターフェイス内で、フロアマップ上でのワイヤレスクライアント、不正アクセスポイントおよび干渉源の正確な場所を把握できます。

CMX の設定は、ユーザーの要件に応じて、グローバルレベルで、あるいはサイト、ビルディング、またはフロアレベルで作成できます。小企業の場合はグローバルレベル (親ノード) で CMX を割り当てることができます。すべての子ノードが親ノードから設定を継承します。中企業の場合はビルディングレベルで、小企業の場合はフロアレベルで CMX を割り当てることができます。



(注) セキュリティ上の理由から、CMX は匿名にする必要があります。

## Cisco CMX API サーバーへのユーザーの追加

Cisco CMX インスタンスを Cisco DNA Center ネットワーク設定に追加する前に、Cisco CMX API サーバーにユーザーを追加する必要があります。

**ステップ 1** cmxadmin アカウントを使用して Cisco CMX に SSH 接続します。次のコマンドを入力します。

```
ssh -l cmxadmin (cmx-ip-address)
```

**ステップ 2** Cisco CMX API サーバーを起動します。次のコマンドを入力します。

```
cmxos apiserver start
```

**Example**

The following example shows how to start the Cisco CMX API server:

```
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

**ステップ 3** Cisco CMX API サーバーへのユーザーの追加次のコマンドを入力します。

```
cmxos apiserver user add
```

パスワードプロンプトが表示されたら、Cisco CMX Web 管理画面のユーザー パスワードと同じパスワードを入力します。

**Example**

The following example shows how to add a user for the Cisco CMX API server:

```
[root@server]# cmxos apiserver user add
Please enter the userid for the CMX API Server: user1
Please enter the password for the CMX API Server: password
Please re-enter the password for the CMX API Server: password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

### 次のタスク

Cisco DNA Center で Cisco CMX の設定を作成します。[Cisco CMX 設定の作成 \(416 ページ\)](#) を参照してください。

## Cisco CMX 設定の作成

### 始める前に

Cisco CMX API ユーザーを追加します。[Cisco CMX API サーバーへのユーザーの追加 \(415 ページ\)](#) を参照してください。

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

**ステップ 2** [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。

[DNA Spaces/CMX Servers] ウィンドウが表示されます。

**ステップ 3** [CMX Servers] テーブルから、[Add] をクリックします。

**ステップ 4** [Add CMX Server] スライドインペインで、次のフィールドに入力します。

- [IP Address] : CMX Web GUI の有効な IP アドレスを入力します。
- [User Name] : CMX Web GUI のユーザー名を入力します。
- [Password] : パスワードログイン情報を入力します。

- [SSH User Name] : CMX 管理者のユーザー名を入力します。
- [SSH Password] : CMX 管理者のパスワードログイン情報を入力します。

(注) CMX が到達可能であることを確認してください。

**ステップ 5** [Add] をクリックします。

CMX サーバーが正常に追加されました。

**ステップ 6** CMX サーバーをサイト、建物、またはフロアに割り当てるには、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** 左側の [Tree View] メニューで、[Global] か、興味のあるエリア、ビルディング、フロアを選択します。

**ステップ 9** [DNA Spaces/CMX Servers] セクションで、ドロップダウンリストを使用して、CMX サーバーを選択します。

**ステップ 10** [Save] をクリックします。

[Create CMX Settings] ページが表示されます。

CMX の追加後に [Network Hierarchy] ページのフロアに変更を加えた場合、その変更は自動的に CMX と同期されます。

CMX が同期されると、Cisco DNA Center はクライアントロケーションを CMX に照会し、その場所がフロアマップに表示されます。

**ステップ 11** フロアマップでは、次のことを実行できます。

- クライアントの場所を表示します。これは青色のドットとして表示されます。
- AP 上にカーソルを移動します。ダイアログボックスは、[Info]、[Rx Neighbor]、[Clients] タブで表示されます。詳細については、各タブをクリックしてください。[Device 360] をクリックして、デバイス 360 ウィンドウを開き、問題を表示します。問題をクリックして、問題の場所とクライアントデバイスの場所を表示します。
- AP をクリックして、AP に関する詳細を含むサイドバーを開きます。
- Intelligent Capture と CMX を統合するときにリアルタイムでクライアント トラッキングを実行します。

**ステップ 12** 変更を加えたときに CMX がダウンした場合は、手動で同期する必要があります。同期するには、[Network Hierarchy] ページで、左側のツリーペインで変更を加えた建物やフロアの隣にある省略記号 **...** の上にカーソルを置き、[Sync: DNA Spaces/CMX] を選択して、変更を手動でプッシュします。

**ステップ 13** CMX サーバーの詳細を編集する場合や CMX サーバーを削除する場合は、次の手順を実行します。

- a) メニューアイコン (**☰**) をクリックして、**[System] > [Settings]** の順に選択します。
- b) [External Services] セクションで、[DNA Spaces/CMX Servers] をクリックします。
- c) 編集する CMX サーバーを選択して変更を加え、[Update] をクリックします。
- d) 削除する CMX サーバーを選択し、[Delete] をクリックします。

- e) [OK] をクリックして削除を実行します。
- 

## Cisco CMX のトラブルシューティング

### CMX 認証に失敗した場合

- Cisco DNA Center で CMX 設定の作成時に指定したログイン情報で、CMX Web UI にログインできるかどうかを確認します。
- SSH を使用して CMX コンソールにログインできるかどうかを確認します。
- CMX UI の API ドキュメンテーションリンクを使用して CMX REST API を使用できるかどうかを確認します。

### クライアントがフロアマップに表示されない場合

- 特定のフロアのシスコ ワイヤレス コントローラが CMX で設定されており、アクティブであるかどうか確認します。
- CMX UI がフロア マップにクライアントを表示するかどうか確認します。
- Cisco DNA Center マップ API を使用して、フロアにクライアントをリスト表示します。

```
curl -k -u <user>:<password> -X GET
/api/v1/dna-maps-service/domains/<floor group
id>/clients?associated=true
```



## 第 22 章

# レポート

---

- [レポートの概要 \(419 ページ\)](#)

## レポートの概要

レポート機能のデータを使用すると、ネットワークとその動作に関する洞察を得ることができます。このデータがいくつかの形式でレポートされることと、柔軟なスケジューリングおよび設定オプションが提供されることにより、データとレポートの両方を運用上のニーズに合わせて容易にカスタマイズできます。

Cisco DNA Center レポートの詳細については、『[Cisco DNA Center Platform User Guide](#)』を参照してください。







## 第 23 章

# アシュアランス監査ログの表示

- ・ [監査ログの表示 アシュアランス \(421 ページ\)](#)

## 監査ログの表示 アシュアランス

監査ログは、設定の変更が要求されたとき、設定の変更が実行されたとき、設定中にエラーが発生したかどうかなどの重要なアクティビティを記録するために作成されます。アシュアランスでは、インテリジェントキャプチャ、問題のしきい値、センサー、および AI ネットワーク分析の設定が変更されると、監査ログが提供されます。

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 DNA Center 管理者ガイド](#)の「監査ログの表示」を参照してください。

アシュアランスでは、次のデータが監査ログにキャプチャされます。

表 20: 監査ログ

| アイテム                 | 説明                |
|----------------------|-------------------|
| <b>Date and Time</b> | ログが受信または実行された日時。  |
| <b>Description</b>   | 監査ログについて簡単な説明。    |
| <b>User</b>          | 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。

#### センサー監査ログ

センサーについては、次の設定要求をキャプチャするために監査ログが提供されます。

- テストスイートの追加要求を受信。
- テストスイートの更新要求を受信。
- テストスイートの削除要求を受信。
- 証明書バンドルに関するテストの更新要求を受信。
- テストステータスの追加要求を受信。

#### AI 分析の監査ログ

AI 分析については、次の AI エージェントの設定変更をキャプチャするために監査ログが提供されます。

- エージェントのオンボード。
- エージェントの復元。
- エージェントの再設定。



## 第 24 章

### 関連資料

- [関連資料 \(423 ページ\)](#)

### 関連資料

Cisco DNA Center の参照ドキュメントとして以下をお勧めします。

| 情報のタイプについては、                                        | このドキュメントを参照してください...                                       |
|-----------------------------------------------------|------------------------------------------------------------|
| リリース情報（新機能、制限事項、未解決および解決済みのバグなど）。                   | <a href="#">Cisco DNA Center リリースノート</a>                   |
| Cisco DNA Center のインストールと設定（設置作業を含む）について。           | <a href="#">Cisco DNA Center 設置ガイド</a>                     |
| Cisco DNA Center の最新リリースに関するアップグレード情報。              | <a href="#">Cisco DNA Center アップグレードガイド</a>                |
| Cisco DNA Center GUI とアプリケーションの使用について。              | <a href="#">Cisco DNA Center ユーザガイド</a>                    |
| ユーザアカウント、セキュリティ証明書、認証およびパスワードポリシー、バックアップと復元の設定について。 | <a href="#">Cisco DNA Center 管理者ガイド</a>                    |
| セキュリティの機能、強化、ベストプラクティスを通じて安全に展開する方法について。            | <a href="#">Cisco DNA Center セキュリティのベストプラクティスガイド</a>       |
| サポートされているデバイスについて（ルータ、スイッチ、ワイヤレス AP、ソフトウェアリリースなど）。  | <a href="#">Cisco DNA Center Compatibility Matrix [英語]</a> |
| Cisco SD-Access 向けハードウェアおよびソフトウェアのサポートについて。         | <a href="#">Cisco SD-Access 互換性マトリクス</a>                   |
| Cisco DNA アシュアランス GUI の使用について。                      | <a href="#">Cisco DNA Assurance ユーザガイド</a>                 |
| Cisco DNA Center プラットフォーム GUI とアプリケーションの使用について。     | <a href="#">Cisco DNA Center プラットフォーム ユーザガイド</a>           |

| 情報のタイプについては、                                                            | このドキュメントを参照してください...                                         |
|-------------------------------------------------------------------------|--------------------------------------------------------------|
| Cisco DNA Center プラットフォーム リリース情報（新機能、展開、バグなど）。                          | <a href="#">Cisco DNA Center プラットフォーム リリース ノート</a>           |
| Cisco Wide Area Bonjour アプリケーション GUI の使用について。                           | <a href="#">Cisco Wide Area Bonjour アプリケーション ユーザーガイド</a>     |
| Cisco DNA Center での Stealthwatch Security Analytics Service の使用について。    | <a href="#">Cisco Stealthwatch Analytics Service ユーザーガイド</a> |
| Cisco DNA Center GUI の Cisco DNA アシュアランス 内のダッシュボードとして不正管理機能を利用する方法について。 | <a href="#">Cisco DNA Center の不正管理アプリケーション クイック スタート ガイド</a> |

## 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。